UNIVERSIDADE FEDERAL DE SÃO CARLOS
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE PRODUÇÃO

FERNANDA MOREIRA DE SOUZA BERRETTA

ATAQUES CIBERNÉTICOS E O RISCO AOS SISTEMAS DE PRODUÇÃO E SERVIÇOS - UMA ANÁLISE NA PERSPECTIVA DA GESTÃO DA QUALIDADE

SÃO CARLOS – SP
2025

FERNANDA MOREIRA DE SOUZA BERRETTA

ATAQUES CIBERNÉTICOS E O RISCO AOS SISTEMAS DE PRODUÇÃO E SERVIÇOS - UMA ANÁLISE NA PERSPECTIVA DA GESTÃO DA QUALIDADE

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia de Produção da Universidade Federal de São Carlos, como parte dos requisitos para obtenção do título de mestre em Engenharia de Produção.

Orientador: Prof. Dr. Pedro Carlos Oprime.

SÃO CARLOS – SP
2025

UNIVERSIDADE FEDERAL DE SÃO CARLOS

Centro de Ciências Exatas e de Tecnologia
Programa de Pós-Graduação em Engenharia de Produção

Folha de Aprovação

Defesa de Dissertação de Mestrado da candidata Fernanda Moreira de Souza Berretta, realizada em 25/02/2025.

Comissão Julgadora:

Documento assinado digitalmente
gov.br PEDRO CARLOS OPRIME
Verifique em https://validar.iti.gov.br

Prof. Dr. Juliano Endrigo Sordan (FATEC)

Prof. Dr. Ricardo Pires de Souza (UFRN)

O Relatório de Defesa assinado pelos membros da Comissão Julgadora encontra-se arquivado junto ao Programa de Pós-Graduação em Engenharia de Produção.

DEDICATÓRIA

Dedico este trabalho aos meus pais, pelo amor e apoio incondicional em cada etapa desta jornada. À comunidade científica, cuja dedicação e paixão pelo conhecimento inspiram a busca contínua pela excelência. E a todos que se empenham em aprofundar o entendimento sobre Qualidade 4.0, com a esperança de que este trabalho possa contribuir para o avanço deste campo fascinante.

AGRADECIMENTO

A realização da minha dissertação só foi possível graças ao apoio e incentivo de várias pessoas, às quais gostaria de expressar minha sincera gratidão.

Aos meus familiares, que sempre estiveram ao meu lado, oferecendo suporte, amor e compreensão incondicional, meu profundo agradecimento. Vocês são a base que me sustenta em cada passo desta jornada.

Aos colegas de curso, pela parceria, troca de ideias e pelo companheirismo ao longo desse percurso, minha gratidão. Suas contribuições e amizade foram fundamentais até aqui.

Aos membros da banca examinadora, agradeço pela disposição em avaliar este trabalho e pelas valiosas contribuições que certamente enriqueceram esta dissertação.

Ao meu orientador, minha sincera gratidão pela orientação cuidadosa, paciência e incentivo constante. Sua experiência e compromisso têm sido essenciais para a conclusão deste projeto.

Por fim, agradeço à Universidade Federal de São Carlos (UFSCar) por proporcionar um ambiente acadêmico rico em recursos e oportunidades, que tem sido fundamental para o desenvolvimento desta pesquisa.

A todos, meu muito obrigada.

RESUMO

A Indústria 4.0 é caracterizada pela integração de tecnologias digitais nos processos de manufatura. Destacam-se os sistemas ciber-físicos (CPS), que combinam componentes físicos e digitais para criar ambientes de produção conectados, automatizados e inteligentes. No entanto, esses sistemas são vulneráveis a ciberataques. Esses ataques podem ter consequências devastadoras, desde interrupções na produção até danos físicos às instalações e equipamentos. Para mitigar esses riscos, as indústrias têm adotado uma série de práticas e protocolos, entretanto pouco se tem explorado o papel dos sistemas de gestão da qualidade no contexto da cibersegurança. A gestão da qualidade pode desempenhar um papel crucial na prevenção e detecção de problemas de cibersegurança enfrentados pela Indústria 4.0, ao garantir que os processos e sistemas estejam em conformidade com padrões e melhores práticas de segurança. O objetivo desta dissertação é analisar e indicar como a gestão da qualidade pode contribuir para a prevenção e detecção de ataques hackers, destacando suas práticas e ferramentas que fortalecem os sistemas de segurança cibernética. Para isso, foi utilizada a abordagem metodológica do programa de pesquisa de Lakatos, a partir da revisão da literatura. Essa revisão foi dividida em duas etapas: a primeira consistiu em uma análise descritiva, e a segunda, em um mapeamento científico, realizado por meio de uma técnica conhecida como *text mining*. Além disso, realizou-se uma pesquisa de campo com especialistas na área. Os resultados da pesquisa indicaram que o tema é emergente e relevante, pois a Gestão da Qualidade possibilita a mitigação de vulnerabilidades dos sistemas conectados a ataques cibernéticos. A pesquisa indica que os gráficos de controle multivariados são uma das principais técnicas estatísticas recomendadas para a detecção de anomalias em sistemas hiperconectados. Verificou-se também o papel estratégico dos sistemas de gestão da qualidade, que, quando integrados aos sistemas de cibersegurança, melhoram a capacidade de detecção e prevenção, com destaque para as normas da Série ISO 9000 e para o TQM.

Palavras-chave: Ciberataques. Cibersegurança. Sistemas de Gestão da Qualidade. Métodos estatísticos.

ABSTRACT

Industry 4.0 is characterized by the integration of digital technologies into manufacturing processes. Cyber-physical systems (CPS) stand out, combining physical and digital components to create connected, automated, and intelligent production environments. However, these systems are vulnerable to cyberattacks, which can have devastating consequences, ranging from production disruptions to physical damage to facilities and equipment. To mitigate these risks, industries have adopted various practices and protocols; however, the role of quality management systems in the context of cybersecurity has been little explored. Quality management can play a crucial role in preventing and detecting cybersecurity issues faced by Industry 4.0 by ensuring that processes and systems comply with security standards and best practices. This dissertation aims to analyze and indicate how quality management can contribute to the prevention and detection of hacker attacks, highlighting its practices and tools that strengthen cybersecurity systems. To achieve this, the methodological approach of Lakatos' research program was used, based on a literature review. This review was divided into two stages: the first consisted of a descriptive analysis, and the second involved scientific mapping using a technique known as text mining. Additionally, a field study was conducted with experts in the field. The research results indicated that the topic is both emerging and relevant, as quality management enables the mitigation of vulnerabilities in systems connected to cyberattacks. The study suggests that multivariate control charts are among the main statistical techniques recommended for detecting anomalies in hyperconnected systems. Furthermore, the strategic role of quality management systems was highlighted. When integrated with cybersecurity systems, they enhance detection and prevention capabilities, with particular emphasis on the ISO 9000 series standards and Total Quality Management (TQM).

Keyword: Cyberattacks. Cybersecurity. Quality Management Systems. Statistical Methods.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE GRÁFICOS

LISTA DE QUADROS

LISTA DE SIGLAS

ATP - *Advanced Persistent Threat*

BIC - *Bayesian Inference Criterion*

CAM - *Computer Aided Manufaturing*

CAD - *Computer Aided Design*

CPS – *Cyber-Physical System*

CRSTIP - *Compliance, Risk Assessment, and Security Testing Improvement Profiling*

CUSUM - *Cumulative Sum Control Chart*

CWQC - *Company Wild Quality Control*

DoS – *Denial of Service*

ES – Engenharia Social

EWMA - *Exponentially Weighted Moving Average*

FCS – Fatores Críticos de Sucesso

GQ – Gestão da Qualidade

IA – Inteligência Artificial

ICS - *Industrial Control System*

IoT – *Internet of Things*

ISO - *International Organization for Standardization*

LGPD – Lei Geral de Proteção de Dados Pessoais

OT - Tecnologia Operacional

PDCA – *Plan, Do, Check, Act*

SGQ – Sistemas de Gestão da Qualidade

SGSI - Sistema de Gestão de Segurança da Informação

SPM – *Statistical Process Monitoring*

TI – Tecnologia da Informação

TIC - Tecnologias de Informação e Comunicação

TQC – *Total Quality Control*

TQM – *Total Quality Management*

TTPs - *Tatics, Techniques, Procedures*

SUMÁRIO

1 INTRODUÇÃO

Nesta seção, contextualiza-se o problema da vulnerabilidade dos sistemas ciber-físicos (em inglês: *cyber-physical systems* - CPS) diante de ciberataques e o papel do gerenciamento da qualidade frente a essa questão. São delineados os problemas e objetivos de pesquisa que orientam a construção desta dissertação, assim como a justificativa e a relevância do estudo. Por fim, apresenta-se a estrutura do trabalho.

1.1 CONTEXTUALIZAÇÃO

Para as operações de serviço e manufatura, o século XXI é, substancialmente, impactado pela transformação digital, que tem seus alicerces na conexão entre empresas e indivíduos por meio de *internet*, computadores, *smartphones*, *tablets* e armazenamento de dados na nuvem. Tais influências afetam mercados e empresas, moldando novas estruturas organizacionais (NEUMANN *et al.*, 2021; SACOMANO *et al.*, 2018; XU; XU; LI, 2018). Esse ambiente foi profícuo para o surgimento de empresas inovadoras, como a *Uber* e *AirBnB*.

Pode-se afirmar que a integração das tecnologias de informação e comunicação é o grande evento do século XXI, que permitiu as organizações alcançarem novos patamares de produtividade, qualidade e flexibilidade. O principal efeito desses eventos é a geração de novas estratégias e modelos de negócio (NEUMANN *et al.*, 2021; SACOMANO *et al.*, 2018; XU *et al.*, 2018).

Outro conceito emergente no século XXI, no arrastro da Quarta Revolução Industrial, é Qualidade 4.0 (Q4.0). Incorporando novas tecnologias, como inteligência artificial, IoT e análises de *big data* aos sistemas de gestão da qualidade, a Q4.0 revolucionou o controle e melhoria de processos e produtos. Esse movimento transformou as práticas tradicionais de qualidade, possibilitando a identificação e diagnósticos em tempo real de problemas durante o processo de fabricação (ANTONY *et al.,* 2021). Isso foi possível porque as plantas industriais que operam com as tecnologias da I4.0 passaram a ter seus sistemas de produção controlados de modo remoto *online,* sendo possível fazer ensaios virtuais para simular a produção e verificar potenciais riscos à sua integridade (MAHMOUD *et al.,* 2019; SACOMANO *et al.,* 2018). Entretanto, esses sistemas conectados tornaram-se mais suscetíveis a ataques cibernéticos (ELHABASHY *et al.*, 2019; MAHMOUD *et al.*, 2019), o que podem pôr em risco toda a cadeia produtiva. Segundo de Mahmoud *et al.*, (2019), ataques cibernéticos é qualquer ato malicioso

que pode pôr em risco a segurança dos sistemas produtivos, com impactos na qualidade da fabricação e dos serviços prestados.

Os perigos dos ataques ciberfisicos também são alertados por Deuerlein *et al.* (2012), Elhabashy *et al.* (2019), Antony *et al.* (2021) e Rahman e Shafae (2022). Esses autores apontam que organizações que utilizam das tecnologias conectadas à *internet* são mais suscetíveis a ataques *hackers*. Elhabashy *et al.* (2019) destacam as graves consequências e riscos para as empresas decorrentes de ataques *hackers*, que podem afetar o mundo físico e causar danos reais aos sistemas de produção, como a destruição de equipamentos ou a alteração das características dos produtos.

Os alertas aos riscos dos sistemas produtivos conectados à *internet* são evidenciados por inúmeros casos de ataques cibernéticos às organizações. Em março de 2023, o sistema do Hospital Universitário, da Universidade de São Paulo, foi invadido. A paralisação dos sistemas informatizados do hospital obrigou a unidade a restringir os atendimentos aos casos de urgência e emergência, assim mais de 700 pacientes foram prejudicadas (fonte: https://g1.globo.com/sp/sao-paulo/noticia/2023/03/30/hospital-universitario-da-usp-sofre-ataque-de-hackers-e-deixa-de-atender-ao-menos-700-pacientes-em-uma-semana.ghtml, acessado em 24 maio 2023).

Em outubro de 2023, empresas multinacionais proeminentes, incluindo Amazon, Google e Cloudware, foram vítimas do que é agora considerado o mais significativo ataque cibernético já registrado. Este ataque, documentado como um marco na história da segurança digital, tinha como propósito deliberado a indução de lentidão nos sistemas dessas corporações, buscando obstruir suas operações comerciais (fonte: https://www.cnnbrasil.com.br/economia/google-amazon-e-cloudware-confirmam-ter-sofrido-maior-ataque-cibernetico-da-historia/, acessado em 04 de dezembro de 2023). A JBS, importante empresa do setor alimentício do Brasil, sofreu em 2021 um ataque malicioso nas suas unidades dos EUA, Canadá e Austrália e teve seus dados sequestrados. A empresa optou pagar pelo resgate para garantir a integridade dos dados e da produção (fonte: https://g1.globo.com/economia/noticia/2021/06/09/jbs-diz-que-pagou-11-milhoes-em-resposta-a-ataque-hacker-em-operacoes-nos-eua.ghtml, acessado em 4 de dezembro de 2023). A Honda também foi alvo de um ataque cibernético, que ocasionou a interrupção de suas unidades fabris, em razão dos ciberataques terem afetatado os sistemas de controle de qualidade (fonte: https://autoesporte.globo.com/videos/noticia/2020/06/honda-e-alvo-de-ataque-hacker-e-suspende-parte-da-producao-incluindo-no-brasil.ghtml, acessado em 4 de dezembro de 2023).

Estes exemplos ilustram a vulnerabilidade das organizações que operam com tecnologias da Indústria 4.0, em razão da conectividade dos sistemas ciber-físicos, fazendo com que os riscos de ataques *hackers* aumentem (ZONNESHAIN; KENETT, 2020; ASIF, 2020; XU *et al.*, 2018; MAHMOUD *et al.*, 2019; ELHABASHY *et al.*, 2021).

Apesar desses eventos danosos à integridade dos sistemas produtivos, a I4.0 é um processo em curso irreversível. Ela engloba a integração de diversas tecnologias, como as tecnologias da informação, a inteligência artificial (IA), o armazenamento dados em nuvem e a robótica. Quando essas tecnologias são organizadamente implementadas aos sistemas produtivos, tornam-se fatores impulsionadores da competitividade das indústrias modernas (ANTONY *et al.*, 2021; ASIF, 2020; XU *et al.*, 2018).

A questão posta é como os sistemas de gestão da qualidade (SGQ) podem contribuir para a prevenção e detecção de ataques hakers. A resposta pode estar nos procedimentos e planos de controle da qualidade se esses considerarem os riscos de ataques maliciosos. Essa diretriz é reforçada por Zonnenshain e Kenett (2020), que enfatizam a importância dos sistemas de gestão da qualidade no novo paradigma de operações de produção conectadas. Na mesma direção, Elhabashy *et al.* (2021) reforçam o novo papel dos SGQ no contexto da I4.0. Esses autores consideram a possibilidade do uso dos SGQs para identificar e evitar ataques maliciosos. Porém, essa é uma questão ainda pouco explorada pelos pesquisadores e pelas organizações em geral. No momento atual, os sistemas de gestão da qualidade ainda não são plenamente integrados ao ambiente da I4.0, quando se trata a mitigar as ameaças à integridade de sistemas cibernéticos.

A gestão da qualidade (GQ) é um campo de estudo amplo, com seus sistemas, filosofias, abordagens, métodos, técnicas e ferramentas. Estão no seu escopo conceitos e abordagens da qualidade, os sistemas de qualidade, normas e padrões de controle. Se integrados às certificações e práticas no âmbito da tecnologia da informação e comunicação, a GQ pode fortalecer a resiliência dos sistemas ciber-físicos, proporcionando camadas adicionais de defesa contra ataques maliciosos. Porém, isso não está definidamente claro na literatura. Há uma lacuna entre SGQ e cibersegurança que precisa ser trabalhada com novos estudos, e um dos caminhos está em explorar a aplicação de normas internacionais, como ISO 9001 e ISO 27001. Há também espaço para o uso de métodos e técnicas, como os gráficos de controle, para estabelecer um ambiente organizacional que promova a segurança cibernética. A habilidade das organizações em incorporar essas práticas, não apenas refletiria o compromisso com a excelência de seus produtos e serviços, mas também como um indicador claro de

responsabilidade dessas organizações perante seus usuários e clientes decorrentes de ameaças de ataques *hackers* (ANTONY *et al.*, 2021; ASIF, 2020).

1.2 OBJETIVOS DA PESQUISA

Nos últimos anos autores têm se dedicado a entender como os ciberataques podem afetar os CPS (COLOSIMO *et al.*, 2024; ALSULAMI *et al.*, 2022; ALEKSANDROVA *et al.*, 2020; MAHAN; MENOLD, 2020; ELHABASHY *et al.*, 2019; SHAFAE *et al.*, 2019; WELLS *et al.*, 2014), bem como entender as vulnerabilidades inerentes à eles (CHAN *et al.*, 2020; ELHABASHY *et al.*, 2020; MAHAN; MENOLD, 2020).

De acordo com Alshaibi *et al.* (2022) e Humayed *et al.* (2017), as formas de detecção de ataques maliciosos tradicionais já não suprem mais as atuais necessidades das organizações. Novos sistemas e métodos devem ser continuamente desenvolvidos. Estudos do uso de gráficos de controle multivariados na detecção de intrusão em CPS é um exemplo de técnica da qualidade tradicional que pode ser utilizada nesse contexto dos sistemas ciber físicos (CPS) (RODRÍGUEZ-MARTÍNZES *et al.*, 2023; SHAOHUI *et al.*, 2022; ELHABASHY *et al.*, 2021; MASHURI *et al.*, 2021; CHEN; WANG, 2020; AHSAN *et al.*, 2018; BOUYEDDOU *et al.*, 2017).

Nesta dissertação será investigado como as normas, sistemas, métodos e ferramentas da GQ podem auxiliar na proteção dos sistemas produtivos conectados dos ataques cibernéticos (COLOSIMO *et al.*, 2024; ALEKSANDROVA *et al.*, 2020; ELHABASHY *et al.*, 2020; ELHABASHY *et al.*, 2019). Assume-se que GQ desempenha um papel relevante na prevenção e detecção de ataques *hackers*.

Ao **investigar a relação entre GQ e sistemas de proteção à ataques maliciosos, esta dissertação tem como objetivo analisar e indicar como a gestão da qualidade pode contribuir para a prevenção e detecção de ataques *hackers*, destacando práticas e ferramentas que fortaleçam os sistemas de segurança cibernéticos.**

Para esse propósito, estabeleceram-se objetivos específicos, que nortearão o desenvolvimento desta dissertação, a saber:

i) Identificar na literatura possíveis pontos de integração entre GQ, com seus sistemas, e a segurança dos CPS. O resultado esperado é identificar os pontos de convergência entre os dois campos, suas especificidades e os resultados provenientes dessa integração.

ii) Validar com especialistas na área os pontos de integração levantados. O resultado esperado é identificar possíveis *gaps* entre o que está na literatura é a prática atual dos cientistas de dados. Além disso, explorar os diversos aspectos relacionados à gestão da segurança cibernética em organizações.

iii) Entender quais são as métricas de monitoramento e acompanhamento da eficácia dos CPS, bem como saber de que modo o sistema se atualiza e responde a novas ameaças.

1.3 JUSTIFICATIVA E RELEVÂNCIA

Por meio da literatura, observa-se que a gestão da qualidade tem capacidade para ampliar seus horizontes de atuação no âmbito da Indústria 4.0. Broday (2022) e Zonneshein e Kennett (2020) enfatizam que a área da qualidade está estagnada no atual contexto industrial, devido à diversas barreiras. Contudo, pesquisas como Colosimo *et al.* (2024), Elhabashy *et al.* (2019) e Wells *et al.* (2014), detalham que a gestão da qualidade possui diversos campos de atuação, dentre eles, o da cibersegurança.

Pesquisas apontam que a integração entre o gerenciamento da qualidade e a cibersegurança é ainda um campo pouco explorado (COLOSIMO *et al.*, 2024; ALEKSANDROVA *et al.*, 2020; ELHABASHY *et al.*, 2020; ELHABASHY *et al.*, 2019; WELLS *et al.*, 2014). A área de segurança da informação tem sido estudada há mais tempo, estudos como Emran e Ye (2002) e Ye *et al.* (2003), pesquisam métodos de detecção de intrusão em sistemas de informações. Além disso, existe uma norma para gerir essa área de sistemas de informação, conhecida como a série ISO 27000 (DISTERER, 2013).

O que se entende hoje como segurança de sistemas ciber-físicos está amplamente ligado à detectar ataques, por meio de sistemas de detecção de intrusão, baseados em assinaturas e anomalias, neste segundo caso, os gráficos de controle multivariados estão sendo explorados (RODRÍGUEZ-MARTÍNZES *et al.*, 2023; SHAOHUI *et al.*, 2022; ELHABASHY *et al.*, 2021; MASHURI *et al.*, 2021; CHEN; WANG, 2020; AHSAN *et al.*, 2018; BOUYEDDOU *et al.*, 2017). Há uma carência de estudos voltadas para a cibersegurança no ramo da manufatura, principalmente na área de gestão. Como contribuição teórica da pesquisa busca-se explorar como a gestão da qualidade, como um todo, pode colaborar na área da cibersegurança voltada para a manufatura.

1.4 ESTRUTURA DO TRABALHO

Este trabalho é composto por 7 capítulos, a Figura 1 apresenta um esquema da estrutura deste trabalho. O primeiro é dedicado a introdução, o qual é composto por contextualização sobre a problemática dos ciberataques, de modo a conectar o assunto com a gestão da qualidade. Além disso, consta também os objetivos do trabalho, questões de pesquisa, relevância e justificativa.

O Capítulo 2 trata-se da revisão da teórica sobre os temas que circundam o tema desta dissertação: indústria (2.1), ciberataques (2.2), gestão da qualidade (2.3) e perguntas e hipóteses (2.4). A parte metodológica é abordada no Capítulo 3, a qual conta com uma caracterização da pesquisa, o método, os instrumentos de pesquisa e análise dos dados e informações coletados.

Figura 1 – Estrutura do trabalho

Fonte: Autoria própria (2025)

Os resultados da revisão bibliográfica são encontrados no Capítulo 4. Este capítulo possui 4 sub-capítulos, os quais contam com uma análise descritiva (4.1), mapeamento científico (4.2) e análise comparativa entre os achados da bibliometria e a revisão da teoria (4.3) e a relação entre os achados da revisão bibliográfica e as perguntas e hipóteses levantadas no capiutlo 2 (4.4).

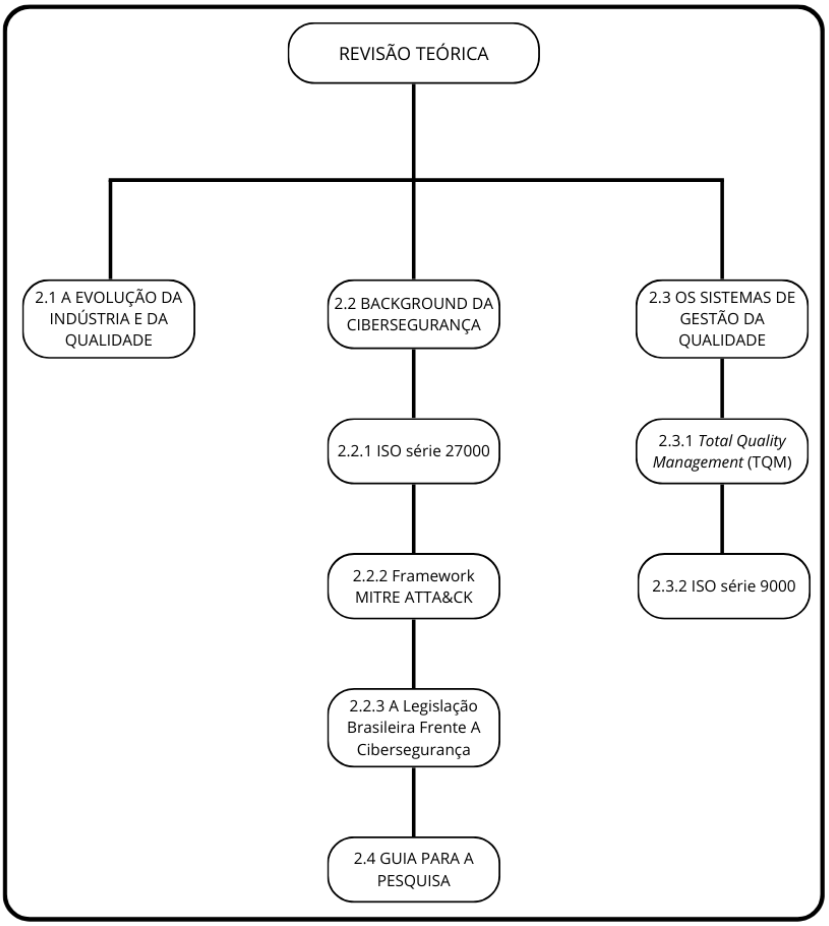
O Capítulo 5 contém os resultados da pesquisa de campo, inicialmente foi apresentada a análise de dados (5.1) e em seguida os principais achados da pesquisa de campo (5.2). Foram feitas discussões e sugestões de integração da área de qualidade com a cibersegurança no

Capítulo 6 baseadas nos resultados. O capítulo 7 trata das conclusões. Por fim, tem-se as referências, apêndices e anexo.

2 REVISÃO TEÓRICA

Este capítulo apresenta uma revisão da teoria sobre a Indústria 4.0, a gestão da qualidade e cibersegurança.

Figura 2 – Estrutura do Capítulo 2



Fonte: Autoria própria (2025)

O subcapítulo 2.1 analisa a evolução da indústria no Brasil e no mundo, bem como o desenvolvimento gerenciamento da qualidade. A sub-seção 2.2 aborda temas de conhecimento geral na área de cibersegurança, incluindo a ISO 27000 (seção 2.2.1) e o *framework* MITRE ATT&CK (seção 2.2.2).

Especificidades da legislação brasileira sobre cibersegurança será apresentada na seção 2.2.3. Aspectos conceituais, filosóficos e metodológicos da gestão da qualidade total, o TQM, são apresentados na seção 2.3. No sub-capítulo 2.4 são apresentadas as perguntas que surgiram

ao longo da revisão teórica, bem como hipóteses que irão guiar o presente trabalho. A Figura 2 ilustra a estrutura do Capítulo 2 deste trabalho.

2.1 A EVOLUÇÃO DA INDÚSTRIA E DA QUALIDADE

A Primeira Revolução Industrial teve início em 1784 e ficou marcada pela introdução de equipamentos de produção mecânica movidos a energia hidráulica e a vapor. Essa inovação tecnológica na produção de bens manufaturados e a organização dos meios de produção, foi um marco na história da humanidade, pois, a partir desse momento, a dinâmica de inovação tecnológica acelerou fortemente (ZONNENSHAIN; KENETT, 2020; XU *et al.*, 2018).

Um século depois, um novo avanço tecnológico deu início à Segunda Revolução Industrial, marcada pelo uso de energia elétrica nas fábricas e pela produção em massa. O fato é que os avanços tecnológicos iniciados no século XIX, associado a novos métodos de produção em escala, institui-se o que se denominou de sociedade moderna, essencialmente industrial, contraponto a sociedade agrículo do século passado. Há um aumento significativo da produtividade com a mecanização dos meios de produção e da ascensão de uma classe média poderosa (ZONNENSHAIN; KENETT, 2020; XU *et al.*, 2018).

O ano 1969 é um marco de um novo avanço tecnológico, caracterizado pela automação dos processos industriais, que deu início a um novo modelo de produção, baseado no uso de eletrônicos e na introdução da produção automatizada, sendo denominado como Terceira Revolução Industrial (ZONNENSHAIN; KENETT, 2020).

Concomitantemente, ao longo das décadas, a gestão da qualidade evoluiu conforme os modelos de produção se modificavam. Na Primeira Revolução Industrial, as atividades de controle de qualidade eram registradas em livros contábeis para fins de contabilidade e planejamento, sendo realizadas exclusivamente pelos artesãos (ZONNENSHAIN; KENETT, 2020).

A Segunda Revolução Industrial é marcada pelo pioneiro trabalho Walter Shewhart, físico, engenheiro e estatístico, que propôs o uso de gráficos de controle para reduzir a necessidade de inspeção, resultando em economia de tempo, dinheiro e melhoria na qualidade. Na era da inspeção da qualidade, a função de qualidade era a apenas para verificar a uniformidade de produtos finais, e era executada pelo departamento de inspeção (COLOSIMO *et al.*, 2024; ZONNENSHAIN; KENETT, 2020).

A partir da década de 1940, na era do controle e da qualidade do processo, a inspeção foi ampliada para todos os processos de produção, tornando-se responsabilidade do

departamento de engenharia e de produção. Tal medida visava reduzir os produtos não conformes ao fim da produção e reduzir a quantidade de produtos inspecionados. A evolução da função qualidade incorporou novas atribuições, que não se restringia somente a inspeção. Um fato relevante sobre isso é a introdução de modelos estatísticos de probabilidade no controle estatístico da qualidade, e do pensamento estatístico na rotina das empresas, sendo que a compreensão da variação aleatória das medições das características de qualidade dos produtos é um elemento tecnológico crucial para o domínio dos processos (COLOSIMO *et al.*, 2024; ZONNENSHAIN; KENETT, 2020; TOLEDO *et al.*, 2012).

A Terceira Revolução Industrial representa a era da garantia da qualidade e do gerenciamento estratégico da qualidade. Garantir a qualidade é realizar testes ao longo de todo o processo de fabricação de modo que os produtos sejam fabricados conforme as especificações de engenharia. Inovações tecnológicas introduzidas nessa fase que se destaca é o uso de redes de computadores que passa a coordenar o todo o processo industrial, tais como *Computer Aided Manufaturing* (CAM) e o *Computer Aided Design* (CAD), com o objetivo de minimizar o impacto custoso de falhas em um produto após a entrega ao cliente (XU *et al.*, 2018).

Pensar a Qualidade como parte da estratégia da empresa faz com que a função qualidade entre nas discussões de planos da alta administração. O elemento central das organizações é o foco nas necessidades do cliente, e obter vantagens competitivas em relação a concorrência. A operacionalização desse enfoque estratégico é fortalecida por meio da participação de todos na empresa, com a alta gerência exercendo a liderança dos processos relacionados a gestão da qualidade (ZONNENSHAIN; KENETT, 2020; TOLEDO *et al.*, 2012).

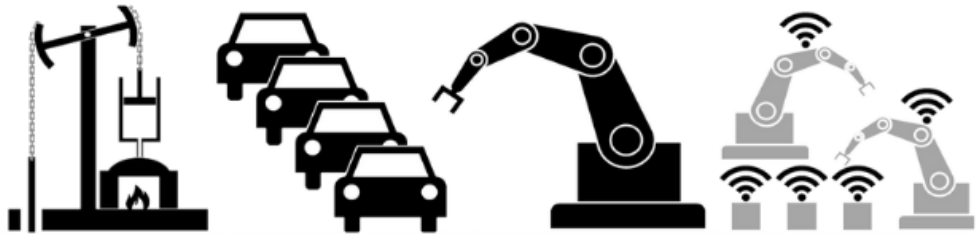
Novos avanços tecnológicos têm impactado de modo significativos o século XXI. O evento mais recente é o da Indústria 4.0, apresentado pela primeira vez em Hannover, Alemanha, no ano de 2011, durante uma importante reunião de negócios. Na ocasião, profissionais do setor industrial e representantes do governo alemão debateram a importância do uso da tecnologia como fator crucial para a competitividade (SANDERS *et al.*, 2016; KAGERMANN *et al.*, 2013). Em 2013, esse termo foi oficialmente anunciado como uma iniciativa estratégica alemã para liderar a revolução no setor de manufatura (XU *et al.*, 2018).

A Indústria 4.0 representa a atual tendência das tecnologias de automação na indústria de manufatura. Essa abordagem abrange principalmente tecnologias habilitadoras, como sistemas ciber-físicos (CPS), *Internet* das Coisas (em inglês: *Internet of Things* - IoT), computação em nuvem, simulação, realidade aumentada, robôs autônomos, manufatura aditiva, *big data analytics* e a cibersegurança (COLOSIMO *et al.*, 2024; NEUMANN *et al.*, 2021; NARDO *et al.*, 2020; XU *et al.*, 2018).

Os CPS combinam estatísticas, modelagem computacional e dados em tempo real extraídos de sistemas físicos para modelar a resposta de um sistema em diversos cenários e tomar decisões em tempo real, com o objetivo final de melhorar a eficiência em todos os níveis de um sistema industrial (KAGERMANN *et al.*, 2013). A introdução do CPS nas indústrias representa um marco importante da Quarta Revolução Industrial (COLOSIMO *et al.*, 2024; NARDO *et al.*, 2020; XU *et al.*, 2018).

Apesar das inúmeras vantagens propiciadas por tecnologias, novos problemas têm surgido para os gestores. Colosimo *et al.* (2024) observa que este novo tipo de sistema produtivo é muito vulnerável à ataques *hacker*, dado sua conectividade. Ataque *hacker* é, segundo Mahmoud *et al.* (2019), qualquer ato malicioso que pode pôr em risco a segurança dos sistemas produtivos e contábeis e financeiros, com impactos na qualidade da fabricação e dos serviços prestados.

Figura 3 – Evolução da indústria e da qualidade ao longo da história



1ª REVOLUÇÃO INDUSTRIAL	2ª REVOLUÇÃO INDUSTRIAL	3ª REVOLUÇÃO INDUSTRIAL	4ª REVOLUÇÃO INDUSTRIAL	
• Energia hidráulica; • Energia a vapor; • Tear mecânico.	• Energia elétrica; • Produção em massa.	• Eletrônicos; • Computação; • Produção automatizada.	• Tecnologias de informação e comunicação; • Sistemas Ciber-Físicos; • Ataques cibernéticos.	Principais características das Revoluções Industriais
• Contabilidade e planejamento; • Artesãos.	• Gráficos de Controle; • Era da inspeção: inspeção do produto final para verificar a uniformidade de produtos finais; • Era do controle e da qualidade do processo: inspeção dos processos para reduzir os produtos não conformes ao fim da produção e reduzir a quantidade de produtos inspecionados.	• Era da garantia da qualidade: testes ao longo dos processos de fabricação para minimizar o impacto custoso de falhas em um produto após a entrega ao cliente; • Era do gerenciamento estratégico da qualidade: foco no cliente e no mercado para impactar na concorrência.	• Qualidade 4.0: inovar os modelos de qualidade para atender às novas exigências do mercado.	Principais características do Gerenciamento da Qualidade

Fonte: Autoria própria (2025)

Dentre várias possibilidades de enfrentamento desse no desafio, esses autores sugerem o uso do monitoramento estatístico do processo (em inglês: *statistical process monitoring* - SPM) para detecção de ataques aos sistemas. Elhabashy *et al.* (2019), Elhabashy *et al.* (2020), Elhabahsy *et al.* (2021), apontam que os ciberataques podem afetar tanto os sistemas de

manufatura quanto os sistemas de qualidade, e que os gráficos de controle multivariados podem ser bastante úteis para detecção de ataques, contudo, ainda existem demais outros métodos, ferramentas, abordagens da gestão da qualidade que podem colaborar para essa questão dos ciberataques. Assim, fica evidente que, com a evolução dos modelos industriais, surge a necessidade de inovar os modelos de qualidade para atender às novas exigências do mercado.

A Figura 3 ilustra a evolução da indústria e da qualidade ao longo da história, conforme exposto nesta sub-seção delineando as principais características de cada área em cada momento da história até os dias atuais, enfatizando que a Qualidade nesta última era ainda está em discussão.

2.2 BACKGROUND DA CIBERSEGURANÇA

Conforme Alshaibi *et al*. (2022) e Huang *et al*. (2023), o mundo moderno interconectado, em que os dispositivos são automatizados e ligados à rede de *internet*, recebe o nome de Sistemas Ciber-Físicos (CPS); estes, estão cada vez mais presente dentro das organizações. Tais sistemas, conforme Alshaibi *et al* (2022), emergem para facilitar o trabalho humano, evitar falhas e agilizar os processos, aumentando a eficiência e eficácia dos sistemas e processos.

Os CPS se encontram cada vez mais presentes no ramo da saúde, controle e segurança de tráfego, controle ambiental, controle de infraestruturas críticas (como, energia elétrica, recursos hídricos, sistemas de comunicação), manufatura, controle de processos, dentre outros (ALSHAIBI *et al*., 2022; HUMAYED *et al*., 2017; LEE, 2008).

Entretanto, a rápida integração entre os sistemas produtivos e à *internet* aumentou o risco de ameaças cibernéticas (HUANG *et al*., 2023; ALSHAIBI *et al*., 2022; RAJESH *et al*., 2022; HUMAYED *et al*., 2017). Existe diversos tipos de ataques maliciosos, por exemplo: *denial of service*, que consiste em causar um congestionamento nos canais de comunicação; *sniffing*, que envolve o roubo ou a interceptação de dados; *spoofing*, neste, o atacante falsifica ou manipula informações para criar a impressão de que os dados são legítimos ou provenientes de uma fonte confiável; *synchronize (SYN) flooding*, trata-se de sobrecarregar um servidor alvo com uma grande quantidade de solicitações de conexão falsas ou incompletas, e, *viruses* e *worms*, ambos tem o propósito de infectar computadores e dispositivos, causando danos e comprometendo a segurança dos sistemas (LIU *et al*., 2021; BOUYEDDOU *et al*., 2017; MISHRA e KESHRI, 2013; LIU *et al*., 2008).

Singh *et al*. (2023), Alshaibi *et al*. (2022) e Humayed *et al*. (2017) apontam que a ciência da computação e a tecnologia da informação foram pioneiras para o desenvolvimento da cibersegurança, ou seja, a segurança de ambientes virtuais e sistemas ciber-físicos por meio de mecanismos como criptografia, controle de acesso, atualizações de sistemas e detecção da intrusão. Inicialmente, a cibersegurança visava combater ataques de *viruses* e *worms*. Conforme os CPS foram incluídos nas organizações, surgiram novas necessidades e desafios para proteger os sistemas produtivos, então emergiram os sistemas de detecção de intrusão (IDS).

De acordo com Rahman e Shafae (2022), Alshaibi *et al*. (2022) e Mahmoud *et al*. (2019) a detecção de intrusão de ataques maliciosos aos sistemas tem sido eficaz para auxiliar a identificar e prevenir os ciberataques. Acrescenta-se a isso o fato de que a gestão da qualidade tem, ao longo dos anos, suprido às organizações com instrumentos para o controle e melhoria de processos. Com base nisso, a hipótese que a gestão da qualidade pode contribuir para a identificação de ataques maliciosos aos CPS, e assim fortalecer a cibersegurança das organizações, é plausível (LIM; LEE, 2023; ELHABASHY *et al*., 2021; AHSAN *et al*., 2018; BOUYEDDOU *et al*., 2017).

Algumas pesquisas já foram realizadas nessa área. Por exemplo, Elhabashy *et al.* (2021) propuseram um controle estatístico de processo multivariado para detectar ataques cibernéticos em manufatura ciber-física; métodos estatísticos para identificar ataques cibernéticos foram propostos por Ahsan *et al.* (2018; 2019; 2020). Nessas pesquisas foram identificados também alguns desafios, por exemplo, coleta e tratamento de grandes volumes de dados em tempo real, alta taxa de falsos positivos e negativos nos modelos de detecção, adaptação dos modelos estatísticos a novos tipos de ataques, complexidade na interpretação de resultados estatísticos, complexidade na integração de métodos estatísticos com sistemas de segurança já existentes (AHSAN *et al.* 2018; 2019; 2020).

Entretanto, essa é uma área ainda a ser pesquisada, pois é essencial explorar a aplicação de normas internacionais, como ISO séria 9000 e ISO 27000, demais *frameworks*, métodos e técnicas, como os gráficos de controle, para fortalecer o ambiente organizacional que promova a segurança cibernética.

Nas seções seguintes serão apresentadas as principias normas que desempenham um papel fundamental na cibersegurança ao fornecer uma estrutura para proteger a informação e os sistemas de uma organização.

2.2.1 ISO série 27000

A família ISO 27000 funciona como um guia para avaliar a segurança da informação nas organizações, conforme Meriah e Rabai (2019). A discussão sobre este assunto começou em 1993, mas foi apenas em 2009 que a norma ISO 27000 foi emitida para fornecer uma visão geral da família de normas ISO 27000 e uma base conceitual comum (MERIAH e RABAI, 2019; DISTERER, 2013).

Disterer (2013) explica que a segurança da informação e o envolvimento sistemático com aspectos de segurança decorrem pelo risco que as empresas se expõem, cujos processos de negócios estão cada vez mais dependentes do processamento de informações e cujas infraestruturas de TI, complexas e interconectadas, são cada vez mais vulneráveis a falhas e interrupções.

A família de normas ISO 27000 faz referência direta ao ciclo "*Plan-Do-Check-Act*" (ciclo PDCA), conhecido do clássico gerenciamento de qualidade de Deming, que enfatiza a necessidade de orientação por processos, bem como a integração do planejamento das operações e a constante verificação da implementação compatível com o planejamento, conforme a Figura 4 mostra.

Figura 4 – Ciclo PDCA para os SGSI

Fonte: Disterer (adaptado) (2013)

Na fase de planejamento para um Sistema de Gestão de Segurança da Informação (SGSI), serão definidos os requisitos para proteção das informações e dos sistemas de informação, os riscos serão identificados e avaliados, e serão desenvolvidos procedimentos e medidas adequadas para reduzir os riscos. Esses procedimentos e medidas serão implementados durante a implementação e operações. As operações serão monitoradas continuamente, para avaliar o desempenho do SGSI. Os relatórios gerados por meio do monitoramento contínuo das operações serão usados para apontar melhorias corretivas e preventivas para o desenvolvimento adicional do SGSI (STEFANOVA-STOYANOVA e DANOV, 2022; DISTERER, 2013).

A norma principal dentro da série é a ISO 27001, que estabelece os requisitos para um Sistema de Gestão de Segurança da Informação (SGSI). Esse sistema é fundamentado em três pilares principais: confidencialidade, integridade e disponibilidade das informações dentro de uma organização. Além disso, a norma define controles e processos para garantir a proteção adequada dos dados, sendo amplamente utilizada por organizações de todos os tipos e tamanhos para demonstrar seu compromisso com a segurança da informação (DIAMANTOPOULOU *et al.*, 2020; MERIAH e RABAI, 2019; HAUFE *et al*., 2018; DISTERER, 2013).

Disterer (2013) aponta que a ISO 27001 não prescreve ações específicas ou um conjunto fixo de medidas que todas as empresas devem seguir. Em vez disso, cada organização deve desenvolver e implementar suas próprias medidas de segurança com base em suas necessidades específicas, contexto e riscos. Essa abordagem flexível permite a adaptação das diretrizes da norma à realidade particular de cada empresa.

Para implementar a ISO 27001, é necessário desenvolver um treinamento adequado para os colaboradores, inspirado no ciclo PDCA de Deming. Nicho (2018) e Disterer (2013) explicam que esse treinamento visa garantir que eles compreendam e sigam os procedimentos estabelecidos e reconheçam a importância dessas práticas. Os autores também apontam que o cumprimento dos procedimentos deve ser monitorado continuamente para garantir que estão sendo seguidos corretamente. Durante o processo de melhoria contínua, os autores enfatizam que as medidas devem ser verificadas e aperfeiçoadas, enquanto os riscos de segurança são identificados e avaliados constantemente para aumentar a eficácia e eficiência do SGSI.

Disterer (2013) ainda observa que a norma descreve os requisitos para a documentação do SGSI, especificando o conteúdo essencial, os documentos necessários e as estruturas de monitoramento para a gestão de documentos, incluindo:

- **Processos de alteração e aprovação:** Como as mudanças nos documentos devem ser gerenciadas e aprovadas.

- **Controle de versão:** Manter o controle sobre as diferentes versões dos documentos.
- **Regras para direitos de acesso e proteção de acesso:** Definir quem pode acessar quais documentos e como esses acessos são protegidos.
- **Especificações para sistemas de arquivamento:** Instruções sobre como os documentos devem ser armazenados e arquivados.

Stefanova-Stoyanova e Danov (2022) explicam que as responsabilidades da alta administração em todas as etapas do ciclo PDCA incluem a criação e implementação de uma política de segurança, a definição clara de papéis e responsabilidades, a contratação e preparação de pessoal, e a provisão dos recursos materiais necessários. Também incluem a tomada de decisões sobre o gerenciamento de riscos.

A alta administração deve garantir a melhoria contínua e o desenvolvimento do SGSI, baseando-se na política de segurança, nos registros e avaliações das operações, nos resultados dos testes e nas ações de melhoria, enfatizam Stefanova-Stoyanova e Danov (2022). Além disso, auditorias internas regulares devem ser realizadas para identificar vulnerabilidades e impulsionar melhorias. A implementação da política de segurança deve ser verificada quanto à sua adequação e completude por meio de revisões anuais de gestão, observa Disterer (2013).

Ainda no que tange a ISO 27001, existe o Anexo 1 dessa norma. Este fornece uma lista detalhada de controles de segurança que podem ser aplicados em um Sistema de Gestão de Segurança da Informação (SGSI). Este anexo é utilizado como uma referência para garantir que todas as áreas importantes da segurança da informação sejam consideradas e abordadas. Este anexo é dividido em 14 seções principais, cada uma cobrindo diferentes domínios da segurança da informação. Cada seção contém vários controles específicos. Por exemplo, a seção de política de segurança da informação tem como objetivos de controle estabeler política de segurança da informação e revisar essas políticas. O Anexo A deste trabalho ilustra o anexo (DISTERER, 2013).

A ISO 27002 é um guia de práticas para a gestão da segurança da informação. Ela complementa a ISO 27001, detalhando centenas de controles ou melhores práticas que as empresas podem implementar para atender aos requisitos de segurança. Esses controles ajudam as empresas a proteger suas informações (DIAMANTOPOULOU *et al.*, 2020; MERIAH; RABAI, 2019; DISTERER, 2013).

Em 2007, a ISO 27002 foi adicionada aos padrões da família 27000. A norma destaca a importância da segurança da informação, os riscos envolvidos e a necessidade de ter medidas específicas (chamadas de "controles") dentro de um Sistema de Gestão da Segurança da

Informação (SGSI). Esses controles incluem diretrizes sobre como gerenciar riscos, proteger ativos, controlar o acesso, garantir a continuidade do negócio, analisar dados qualitativamente e quantitativamente, pontuar vulnerabilidades inerentes aos sistemas e muitas outras áreas essenciais para a segurança da informação. As empresas podem usar essa lista como um ponto de partida e adaptar ou complementar os controles conforme necessário para atender às suas necessidades específicas e ao seu contexto organizacional (DIAMANTOPOULOU *et al.*, 2020; DISTERER, 2013).

A partir das práticas apresentadas com base na ISO 27002, observa-se o potencial de ferramentas que podem auxliar, por exemplo, na análise e classificação de risco. A ISO 27002 contribui para que as organizações adaptem seus métodos de classificação de riscos às suas realidades operacionais. Tanto a análise qualitativa quanto a quantitativa, bem como seus sistemas de pontuação e avaliações de vulnerabilidades, estão alinhados com as práticas recomendadas da norma em questão.

Em linhas gerais, Disterer (2013) explica que para garantir a segurança da informação, as empresas devem definir e implementar políticas de segurança. Essas políticas são importantes para mostrar que a gestão se preocupa com a segurança da informação. As medidas de segurança devem ser bem estabelecidas na empresa, com papéis e responsabilidades claros. Isso inclui regras sobre como manter a confidencialidade e como se comunicar com clientes, fornecedores e autoridades. Todos os ativos da empresa, tanto tangíveis quanto intangíveis, devem ser identificados e classificados para que as medidas de segurança sejam aplicadas corretamente.

Outro ponto relevante observado por Disterer (2013) é que os sistemas de TI também têm vulnerabilidades que podem causar riscos de segurança. Muitos ataques vêm de dentro da própria empresa, usando o conhecimento interno para causar danos. Portanto, os direitos de acesso dos funcionários devem ser restritos ao necessário para o trabalho deles. Quando as responsabilidades dos funcionários mudam ou eles são demitidos, os direitos de acesso devem ser ajustados ou removidos imediatamente.

Medidas de segurança física também são necessárias para proteger a infraestrutura contra acesso não autorizado, roubo, danos e destruição. Para garantir o bom funcionamento dos sistemas de TI, uma boa prática é a documentação das operações em manuais e procedimentos padrões. Também devem ser estabelecidos e documentados procedimentos para lidar com situações excepcionais, como falhas ou desastres. Antes de implementar mudanças técnicas ou organizacionais, é importante verificar como elas afetarão as operações dos sistemas

de TI. Incidentes de segurança devem ser registrados, analisados e usados para melhorar o sistema de segurança.

Finalmente, a empresa deve cumprir os requisitos de conformidade, incluindo direitos autorais, segurança de dados e proteção de dados, conforme especificado na norma. Dessa forma, tendo os objetivos de controle alinhados com as práticas sugeridas pelo ISO 27002, potencializa-se a proteção da informação.

Existem demais normas que fazem parte da família 27000, por exemplo: ISO 27003, a qual consiste em uma orientação para implementação de sistemas de gestão de segurança da informação; tem-se também a ISO 27004, que trata da gestão de segurança da informação; a ISO 27005, a qual orienta para a gestão de riscos de segurança da informação; dentre outras normas (DIAMANTOPOULOU *et al.*, 2020; MERIAH; RABAI, 2019; DISTERER, 2013).

2.2.2 *Framework* MITRE ATT&CK

Conforme Imran *et al*. (2023) , Singh *et al*. (2023) e Rajesh *et al*. (2022) os ciberataques se tornam cada vez mais complexos, hoje, tais ataques levam o título de *Advanced Persistent Threat* (ATP). Lidar com tais ataques tem sido desafiador e as empresas tem buscado aprimorar seus sistemas de cibersegurança ao nível. Para isso, são utilizados métodos, técnicas e normas, como a ISO 27000, apresentada na sub-seção anterior. Outro *framework* que se destaca bastante é o MITRE ATT&CK.

De acordo com Singh *et al*. (2023) este *framework* foi desenvolvido em 2013 por pesquisadores que simularam as ações dos adversários e defensores. Eles objetivavam melhorar a identificação de ameaças pós-comprometimento. Assim, explicam Singh *et al*. (2023) e Imran *et al*. (2023), o *framework* oferece uma análise completa das várias táticas, métodos e procedimentos de ataque (em inglês: *tatics, techniques, procedures* - TTPs). O nome do *framework* MITRE ATT&CK vem da abreviação de MITRE *Adversarial Tactics, Techniques, and Common Knowledge*. As táticas e abstrações tecnológicas do modelo fornecem um registro geral das ações únicas do adversário reconhecido pela segurança cibernética ofensiva e de defesa. A taxonomia ATT&CK é importante para especialistas em segurança cibernética porque oferece uma taxonomia consistente para ofensiva e defesa, enfatiza Singh *et al*. (2023).

Utilizando as TTPs deste *framework*, os departamentos de cibersegurança contam com equipes vermelhas, mais conhecidas como *redteams*, equipes azuis, mais conhecidas como *blueteams*, e com equipes roxas, conhecidas como *purpleteams*, apontam Hossain *et al*. (2024) e Rajesh *et al.* (2022). O Quadro 1 apresenta a relação entre as equipes e o papel delas frente

ao *framework* MITRE ATT&CK. Os *redteams* fazem testes de penetração nos sistemas organizacionais para verificarem as vulnerabilidades presentes, para então os *blueteams* poderem aprimorar estes sistemas contar os ciberataques. Já o *purpleteam* unem forças do *redteam* e *blueteam* para melhorar continuamente a postura de segurança da organização, por meio do compartilhamento de conhecimento e técnicas, garantindo que as defesas sejam constantemente atualizadas e aprimoradas com base nas novas táticas de ataque descobertas (HOSSAIN *et al.*, 2024; REGE *et al.*, 2023; RAJESH *et al.*, 2022).

Quadro 1 – Equipes e o MITRE ATT&CK

	Redteam	*Blueteam*	*Purpleteam*
Papel da equipe	Equipes que simulam ataques cibernéticos para testar a defesa de uma organização. Utilizam técnicas, táticas e procedimentos de atacantes reais para identificar vulnerabilidades nos sistemas de segurança.	Equipes responsáveis por defender a organização contra ataques cibernéticos. Trabalham para identificar, responder e mitigar ataques em tempo real.	Facilitam a comunicação e a cooperação entre as equipes ofensivas (*redteams*) e defensivas (*blueteams*). O objetivo é compartilhar conhecimento e técnicas, garantindo que as defesas sejam constantemente atualizadas e aprimoradas com base nas novas táticas de ataque descobertas.
MITRE ATT&CK	É um repositório de táticas e técnicas adotadas por *redteams* para executar testes de penetração implantados por atacantes ATP.	As equipes azuis podem fortalecer o sistema de defesa imitando comportamentos de invasores e abordagens de mitigação disponíveis no repositório.	Para essa união de equipes, o *purpleteam* usa o *framework* para discutir as técnicas de ataque e defesa, desenvolvem cenários de ataques e defesas, e identificam as lacunas nas defesas atuais facilitando a comunicação entre as equipes.

Fonte: Rajesh *et al.* (2022) (Adaptado)

Rege *et al.* (2022) expõe que os testes de penetração são de natureza técnica e utilizam habilidades como segurança de rede e aplicativo, *scripts*, vários ambientes de sistema operacional, criptografia e tecnologias de acesso remoto para verificar as vulnerabilidades. Entretanto, os autores argumentam que existem outros testes de penetração, geralmente estão associados aos testes de penetração técnicos, nomeados de Engenharia Social (ES). Este, trata-se de uma técnica de persuasão psicológica que os adversários utilizam para obter informações que protegem os sistemas eletrônicos, como senhas, ou a encorajar as vítimas a fornecer acesso a sistemas eletrônicos e informações, por meio do *download* de arquivos maliciosos disfarçados de arquivos limpos.

Como os ataques cibernéticos frequentemente exploram vulnerabilidades humanas, a engenharia social é uma ferramenta poderosa para mostrar como medidas de segurança técnica

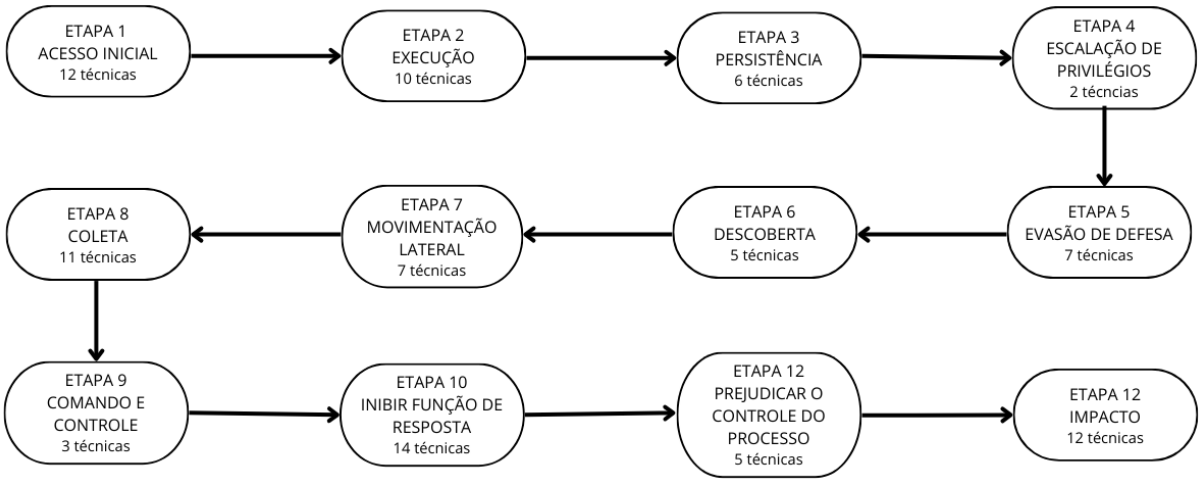
podem ser contornadas. Um teste de penetração que utiliza engenharia social pode demonstrar as fraquezas humanas e como elas podem comprometer a segurança de uma organização, mesmo que os sistemas técnicos sejam robustos (REGE *et al.*, 2023).

O *framework* é bastante amplo e conta com uma infinidade de possibilidades de ciberataques. Classificar os principais tipos de ataque é uma forma interessante de entender métodos de identificação e prevenção de ataques. A literatura aponta alguns ataques, como *phishing* e suas variações, *ransomware*, DoS/DDoS e quebra de senhas como ataques comuns (ABBAS e IBRAHIM, 2024; ALGHASSAB, 2021; GABER *et al.*, 2022).

Para melhor compreensão, o *framework* é separado por etapas do ataque e cada etapa conta com várias técnicas de ataque. Para cada etapa existe recomendações para detectar o ataque e como mitigar o ataque também, tornando o *framework* completo. Além do mais, o *framework* é separado por corporações, *mobiles* e *industrial control system* (ICS), expõe Imran *et al*. (2023). Este trabalho possui o foco em manufatura, portanto, a Figura 5 mostra as etapas de ataque que os ICS podem sofrer.

Na etapa de acesso inicial, o adversário tenta entrar no ambiente ICS comprometendo ativos de tecnologia operacional (OT) e recursos de TI na rede OT. Eles podem atacar entidades terceiras e usuários com acesso privilegiado, além de usar dispositivos externos para interferir nas operações OT (SINGH *et al*., 2023; RAJESH *et al.*, 2022). Durante a execução, o adversário executa código ou manipula funções e dados do sistema de forma não autorizada, utilizando arquivos maliciosos ou comandos de várias interfaces para alterar o comportamento dos dispositivos (SINGH *et al.*, 2023; RAJESH *et al.*, 2022).

Figura 5 – Fluxograma do ciclo de vida do ciberataque em sistemas industriais



Fonte: Autoria própria (2025)

Na etapa de persistência, o adversário mantém acesso aos sistemas ICS após reinicializações ou mudanças de credenciais, substituindo ou sequestrando código e firmware, ou adicionando programas de inicialização em dispositivos, apontam Singh *et al*. (2023) e Rajesh *et al.* (2022). Os autores descrevem que na etapa de escalação de privilégios, o adversário obtém permissões mais altas explorando fraquezas do sistema e vulnerabilidades, permitindo avançar com seus objetivos. Durante a evasão, o adversário evita defesas de segurança removendo indicadores de comprometimento, falsificando comunicações e explorando vulnerabilidades de *software*, apontam Singh *et al*. (2023) e Rajesh *et al.* (2022).

Na descoberta, o adversário pesquisa o ambiente ICS para conhecer a rede interna e dispositivos de controle, utilizando ferramentas para coletar informações e determinar suas próximas ações (RAJESH *et al.*, 2022). Na movimentação lateral, Singh *et al*. (2023) e Rajesh *et al.* (2022) explicam que o adversário se move pela rede, controlando sistemas remotos, abusando de credenciais e serviços vulneráveis, e instalando ferramentas remotas ou utilizando programas e credenciais legítimas. Seguindo a explicação, os autores apontam que durante a coleta, o adversário reúne dados e conhecimento sobre o ambiente ICS, incluindo estados de operação, esquemas de sistemas e funções de dispositivos.

Na etapa de comando e controle, o adversário se comunica e envia comandos para sistemas comprometidos, utilizando dispositivos de comunicação especializados como HMIs, servidores SCADA e estações de trabalho de engenharia, imitando o tráfego de rede esperado para evitar detecção. Na etapa de inibir função de resposta, o adversário impede que as funções de segurança e intervenção do operador respondam a falhas ou riscos, modificando a lógica do sistema ou impedindo respostas com negação de serviço, incluindo a manipulação ou destruição de programas e comunicações (SINGH *et al.*, 2023; RAJESH *et al.*, 2022).

Prejudicar o controle do processo envolve técnicas para manipular, desabilitar ou danificar processos de controle físico, interrompendo a lógica de controle e ameaçando a segurança dos operadores e usuários. Por fim, a etapa de impacto envolve técnicas para manipular, interromper ou destruir sistemas ICS, dados e o ambiente, resultando em interrupção de processos, danos ou perdas de longo prazo, alterando a funcionalidade dos processos para beneficiar seus objetivos enquanto ocultam essas alterações para manter operações aparentemente normais (SINGH *et al.*, 2023; RAJESH *et al.*, 2022).

2.2.3 A Legislação Brasileira Frente A Cibersegurança

Para compreender melhor a posição dos ciberataques às organizações faz sentido estudar as legislações atuais do Brasil que criminalizam o ciberataque de alguma forma. Os prejuízos de roubo de dados, paradas de produção, alteração de padrões de qualidade são imensos. Portanto, ao buscar na legislação brasileira, identificou-se 7 legislações que tentam regulamentar a questão dos ciberataques enquanto cibercrime, ou seja, crime que ocorre no ambiente virtual, conforme Quadro 2. Juntas, elas formam uma linha cronológica, indicando que o assunto ainda está sendo estudado.

Quadro 2 – Legislações atuais e suas datas de lançamento.

Legislações	Data
Lei nº 12.737 – "Lei Carolina Dickmann"	30 de novembro de 2012
Decreto nº 8.771 – Marco Civil da *Internet*	11 de maio de 2016
Resolução nº 4.658	26 de abril de 2018
Lei nº 13.709 – LGPD	14 de agosto de 2018
Resolução nº 740	21 de dezembro de 2020
Decreto nº 10.222	5 de fevereiro de 2020
Decreto nº 11.491	12 de abril de 2023

Fonte: Autoria própria (2025)

A Lei Carolina Dieckmann, de 2012 visa criminalizar a invasão de dispositivos informáticos e a divulgação não autorizada de informações pessoais, protegendo a privacidade e a segurança dos usuários de tecnologia. Ela estabelece penalidades para crimes cibernéticos com previsão de multas e até prisão para os infratores (BRASIL, 2012).

Em 2016 foi lançado o Decreto nº 8.771 regulamenta o Marco Civil da *Internet*, estabelecendo princípios, garantias, direitos e deveres para o uso da *internet* no Brasil, incluindo questões de privacidade e proteção de dados. Ele define diretrizes sobre a neutralidade da rede, responsabilidade dos provedores de serviços *online* em relação aos dados dos usuários, e estabelece obrigações para proteção de informações pessoais (BRASIL, 2016).

A Resolução nº 4.658, de 2018, emitida pelo Banco Central do Brasil, visa estabelecer requisitos para a contratação de serviços de processamento e armazenamento de dados e computação em nuvem por instituições financeiras, com foco na segurança cibernética e proteção de dados sensíveis (BANCO CENTRAL DO BRASIL, 2018).

No mesmo ano, a Lei Geral de Proteção de Dados Pessoais (LGPD) foi lançada. Essa tem como objetivo regulamentar o tratamento de dados pessoais por parte de empresas e organizações, garantindo a privacidade dos indivíduos e estabelecendo diretrizes claras sobre como esses dados devem ser coletados, armazenados, tratados e compartilhados (BRASIL, 2018).

A Resolução nº 740, lançada em 2020 e emitida pelo Conselho Monetário Nacional (CMN), estabelece requisitos e diretrizes específicas para a implementação de políticas de segurança cibernética por instituições financeiras no Brasil, visando proteger informações sensíveis e mitigar riscos cibernéticos (CONSELHO MONETÁRIO NACIONAL, 2020).

No mesmo ano foi lançado o Decreto nº 10.222 que aprova a Estratégia Nacional de Segurança Cibernética (E-Ciber), estabelecendo diretrizes e ações para fortalecer a segurança cibernética no Brasil, protegendo infraestruturas críticas e promovendo a cooperação internacional neste campo. A E-Ciber define metas e iniciativas para melhorar a resiliência cibernética do país, incluindo o desenvolvimento de capacidades técnicas, cooperação entre setores público e privado, e medidas de prevenção e resposta a incidentes cibernéticos (BRASIL, 2020).

Por fim, em 2023, saiu o Decreto nº 11.491 que estabelece a criação de um sistema de gestão de segurança cibernética para o setor público federal no Brasil, visando proteger sistemas e dados governamentais contra ameaças cibernéticas (BRASIL, 2023).

2.3 OS SISTEMAS DE GESTÃO DA QUALIDADE

A Gestão da Qualidade (GQ) tem como propósito garantir que recursos e processos organizacionais e sociais atinjam a qualidade almejada. Em outros termos, é a gestão das atividades e recursos de uma organização para atingir certo patamar de qualidade (CARVALHO *et al.*, 2021; GREMYR *et al.*, 2021; ASIF, 2020).

Diversas abordagens para a gestão da qualidade surgiram ao longo da história, e podem ser usadas, como Sistemas de Gestão da Qualidade (SGQ), por exemplo, a ISO série 9000 e no TQM (GREMYR *et al.*, 2021; ASIF, 2020).

Estes SGQ, conforme Toledo *et al.* (2012), podem ser entendidos com um conjunto de recursos, regras, procedimentos que são implantados em uma organização para satisfazer as necessidades e expectativas das partes interessadas (clientes, acionistas, fornecedores, comunidade, dentre outras partes).

No contexto da Indústria 4.0, segundo Zonnenshain; Kenett (2020) e Broday (2022), a área de gestão da qualidade estagnou, pois, segundo esses autores, pouco se entende o que seria a Qualidade 4.0 e quais as suas áreas de atuação. Carvalho *et al*. (2021) apontam que a Qualidade 4.0 trata-se da digitalização do *Total Quality Management* (TQM), já Broday (2022) e Liu *et al*. (2023) explicam que o termo Qualidade 4.0 surge a partir da integração entre as tecnologias da Indústria 4.0 e o gerenciamento da qualidade, e que, nesta nova era, a qualidade

busca tornar os problemas mais visuais, com maior vantagem em aplicação de sistemas de monitoramento em tempo real e contínuo, sistemas de previsão de defeitos, controle de qualidade inteligente em linha e soluções de inspeção total.

Antony *et al.* (2021) tentaram definir Qualidade 4.0 como "o uso de tecnologias avançadas como IoT, CPS, computação em nuvem para projetar, operar e manter sistemas de qualidade adaptativos, preditivos, autocorretivos e automatizados, juntamente com interação humana aprimorada por meio de planejamento de qualidade, garantia de qualidade, controle de qualidade e melhoria de qualidade para atingir novos ótimos em desempenho, excelência operacional e inovação para atender à visão, missão e objetivos de uma organização", no entanto, estes autores concordam que a definição precisa ainda ser melhorada.

Portanto, conclui-se que, a partir dessas visões, a gestão da qualidade, como é conhecida, tem a capacidade e resiliência de se adaptar ao seu entorno mais próximo e ao seu ambiente externo. O que chama a atenção nessas conceituações sobre Q4.0 é que não é mencionada a vulnerabilidade dos sistemas aos ataques *hackers*. Antony *et al.* (2021) observam que a cibersegurança representa um dos principais obstáculos à Qualidade 4.0, porém não elaboram mais sobre esse assunto. Isso reforça a necessidade de revisão e atualização desse assunto.

Ao olhar em retrospectiva a história da gestão da qualidade, pode-se afirmar que algumas abordagens se destacaram mais que outras, como a *Total Quality Management* (TQM), a qual se tornou um fenômeno mundial (BRODAY, 2022). Outro assunto relacionado a qualidade é a certificação no padrão ISO 9001. Neste, a certificação exige que os sistemas estejam sempre adequados para gerenciar a qualidade (CARVALHO *et al*., 2021; GREMYR *et al*., 2021; ASIF, 2020). Nas sub-seções serão descritos que são esses SGQ, especificamente.

2.3.1 *Total Quality Management* (TQM)

Uma das abordagens da Gestão Total da Qualidade (em inglês: *Total Quality Control* – TQC) é a abordagem japonesa, que surgiu na década de 1960 (SHRIVASTAV, 2023). Essa, enaltece o compromisso de todos os funcionários da empresa para com a qualidade e conta com a administração *top* para atingir esse objetivo, o nome adotado para tal abordagem foi CWQC (*Company Wild Quality Control* – controle da qualidade por toda a empresa) (SHRIVASTAV, 2023; TOLEDO *et al*., 2012). A outra abordagem é o *Total Quality Management* (TQM). Tal abordagem se tornou popular no ocidente na década de 1980 e 1990 e, Toledo *et al*. (2012) explica que o TQM se trata de um modelo customizado da abordagem japonesa (TQC).

A principal diferença entre as abordagens ocorre devido a diferença de significado do termo “controle” para o mundo ocidental e para os japoneses. Os japoneses entendem como “controle” o gerenciamento para manutenção da rotina e para obter melhorias dos processos. Na cultura ocidental, entende por “controle” um policiamento, e não uma gestão. Por isso, os americanos adotaram o termo TQM, trocando “controle” por “gerenciamento” (ou *management*, em inglês), para evidenciar que o objetivo não é controlar, policiar ou acompanhar, mas sim, administrar (TOLEDO *et al.*, 2012).

Dessa forma, entende-se hoje TQM como uma filosofia de gestão integrada com práticas que tem como princípios e valores o foco no cliente, a melhoria contínua dos processos e a tomada de decisões baseada em fatos e dados (MARGHERITA e BRACCINI, 2024; SHRIVASTAV, 2023; TOLEDO *et al.*, 2012).

Merguerita e Braccini (2024) e Shrivastav (2023) enfatizam que o TQM trabalha com o lado *soft* e lado *hard*. O lado *soft* do TQM refere-se aos aspectos comportamentais dos trabalhadores e diz respeito à disseminação da cultura da qualidade e envolvimento dos trabalhadores nas práticas de qualidade. Ele é dividido em duas subcategorias: envolvimento dos trabalhadores, em que o a gestão *top* está comprometida com a comunicação eficaz e reuniões recorrentes para desenvolver uma cultura de qualidade e manter a melhoria contínua; e a outra subcategoria é o desenvolvimento dos trabalhadores, esse foca em aprimorar competências e conhecimentos através de orientação, treinamento e educação, facilitando o empoderamento na tomada de decisões e contribuindo para melhorias contínuas e desempenho organizacional, explica Merguerita e Braccini (2024).

Já o lado *hard* trabalha com aspectos técnicos da produção, por exemplo, as sete ferramentas do gerenciamento da qualidade, descritas pelo Dr. Ishikawa: folha de verificação, diagrama de Pareto, histograma, diagrama de dispersão, diagrama de causa e efeito, estratificações e os gráficos de controle (MARGHERITA e BRACCINI, 2024; LIU *et al.*, 2023; CARVALHO *et al.*, 2021; ASIF, 2020; TOLEDO *et al.*, 2012).

A folha de verificação, trata-se de um formulário utilizado para registrar dados de forma simples que facilitam o uso e a análise (TOLEDO *et al.*, 2012). O diagrama de Pareto trata-se de um gráfico de colunas que ordena as frequências de ocorrência do maior para o menor, permitindo a priorização dos problemas. Seu fundamento é de que 20% das causas produz 80% dos defeitos (NEVES *et al.*, 2024; TOLEDO *et al.*, 2012).

O histograma, ou diagrama de barras, é utilizado para indicar a frequência com que ocorre um valor ou um grupo de valores. A análise desses dados coletados poderá avaliar a

eficiência do processo. Geralmente é utilizado para variáveis contínuas ou quando a amplitude dos valores é muito grande (TOLEDO *et al.*, 2012).

Diagrama de causa e efeito, também conhecido como diagrama de Ishikawa, é um gráfico que identifica, explora e visualiza todas as possíveis causas de um problema específico para encontrar a raiz do problema. (NEVES *et al.*, 2024; TOLEDO *et al*., 2012).

Diagrama de dispersão é uma ferramenta gráfica que permite demonstrar a relação existente entre duas variáveis, ou dois parâmetros, e quantificar a intensidade de tal relação (TOLEDO *et al.*, 2012). Estratificação organiza dados, pessoas e objetos em grupos distintos para identificar padrões. Ele analisa dados categorizando-os por fontes específicas, como máquinas, turnos ou fornecedores, para identificar variações e tendências em diferentes categorias. A partir dessa divisão dos dados é possível montar histogramas, diagramas de dispersão, diagramas de Pareto, dentre outros gráficos. Esta ferramenta é útil para descobrir causas raiz de problemas e para entender melhor como diferentes fatores influenciam um processo (TOLEDO *et al*., 2012).

Gráficos de controle trata-se de um tipo de gráfico comumente utilizado para acompanhá-lo durante um processo. Ele determina uma faixa chamada limites de controle pela parte superior linha (limite de controle superior) e uma linha inferior (limite de controle inferior) e um linha média do processo (limite central), que foram estatisticamente determinado (NEVES *et al*., 2024; TOLEDO *et al*., 2012). Existem vários tipos de gráficos de controle, tanto multivariados como univariados.

Existem diversas outras ferramentas que podem participar do gerenciamento da qualidade (MCDERMOTT *et al.*, 2023), como o fluxograma, FMEA, RCA, entretanto, as ferramentas desenvolvidas pelo Dr. Ishikawa quando aplicadas corretamente podem resolver mais de 95% dos problemas de qualidade (ANTONY *et al*., 2023). A literatura reforça que o lado *hard* tem impacto profundo no desempenho organizacional, permitindo melhoria e otimização do *design* de produtos e operações de processo. A Indústria 4.0 (I4.0) apoia o lado *hard* do TQM com soluções baseadas em dados, sistemas automatizados de gestão da qualidade e métodos estatísticos. Os dados são coletados e monitorados em tempo real também ajudam na análise de causas de falhas e medidas corretivas, além de permitir simulações em gêmeos digitais (MARGHERITA e BRACCINI, 2024).

Nesse sentido, nota-se que há muitos termos empregados atualmente que nos remetem a modelos preditivos classificatórios e de regressão, tais como *machine learning*, *deep learning*, redes neurais e inteligência artificial. Acrescenta-se a esses modelos os métodos estatísticos de monitoramento de processos, gráficos de controle uni e multivariados. Tais

técnicas na área de cibersegurança tem impactos quando associadas a formas de detecção de intrusão, como detecção de comportamento anômalo, antivírus, ferramentas de monitoramento de *log* e eventos, *firewall* e sistemas de autenticação multifatorial (MFA).

2.3.2 ISO série 9000

A série ISO 9000 é um conjunto de normas internacionais que abordam a gestão da qualidade e foram desenvolvidas pela *International Organization for Standardization* (ISO). Tais normas, quando aplicadas adequadamente, permite que a organização consiga aumentar sua vantagem competitiva a partir da qualidade (TOLEDO *et al*., 2012).

A família 9000 conta com 8 princípios que são fundamentais para a implementação da gestão da qualidade: foco no cliente, liderança, engajamento do pessoal, abordagem por processos, abordagem sistêmica para a gestão, melhoria contínua, tomada de decisões baseada em evidência e manutenção de um relacionamento de benefício mútuo com o fornecedor (BENZAQUEN *et al.*, 2021; WILSON e CAMPBELL, 2016). A Quadro 3 explica cada princípio:

Quadro 3 – Princípios da ISO série 9000

Princípio	Explicação
Foco no cliente	As organizações dependem de seus clientes e, portanto, devem entender as necessidades atuais e futuras dos clientes, atender aos seus requisitos e esforçar-se para exceder suas expectativas.
Liderança	Líderes em todos os níveis estabelecem unidade de propósito e direção e criar condições nas quais as pessoas estejam engajadas em alcançar os objetivos de qualidade da organização.
Engajamento do pessoal	Pessoas competentes, capacitadas e engajadas em todos os níveis organização é essencial para melhorar a sua capacidade de criar e entregar valor
Abordagem por processos	Um resultado desejado é alcançado de maneira mais eficiente quando as atividades e os recursos relacionados são gerenciados como processos inter-relacionados que funcionam como um sistema coerente.
Abordagem sistêmica para a gestão	Identificar, entender e gerenciar processos inter-relacionados como um sistema contribui para a eficácia e eficiência da organização no alcance de seus objetivos.
Melhoria contínua	Organizações de sucesso têm um foco contínuo na melhoria
Tomada de decisões baseada em evidências	Decisões baseadas na análise e avaliação de dados e informações têm maior probabilidade de produzir os resultados desejados
Manutenção de um relacionamento de benefício mútuo com o fornecedor	Uma organização e seus fornecedores são interdependentes, e um relacionamento mutuamente benéfico aumenta a capacidade de ambos de criar valor.

Fonte: Benzaquen *et al*. (2021)

De acordo com Bravi e Murmura (2021), a norma mais conhecida da família ISO 9000 é a ISO 9001. Esta especifica os requisitos para um SGQ, e as organizações que desejam obter essa certificação devem ser avaliados por meio de auditorias de qualidade e cumprir tais

requisitos (CARVALHO *et al*., 2021; GREMYR *et al*., 2021; ASIF, 2020; WILSON e CAMPBELL, 2016).

Acredita-se que esta norma se tornou o principal padrão da indústria para eliminar desperdícios, melhorar produtividade e eficiência, proporcionando maior satisfação do cliente e agilizando diariamente rotinas organizacionais (ALMEIDA *et al.*, 2018). Além desses benefícios, a organização que possui a certificação dessa norma tem uma vantagem no mercado, aponta Bravi e Murmura (2022). De forma geral, a implementação da ISO 9001 proporciona benefícios organizacionais a longo prazo, mas, sem dúvida, o principal benefício é obter a certificação, pois ela assegura aos consumidores que a empresa gerenciou corretamente o Sistema de Gestão da Qualidade (SGQ) e, portanto, fornece produtos e serviços bons **(**BENZAQUEN, 2021).

Os requisitos para o SGQ baseado na ISO 9001:2015 são: contexto da organização, liderança, planejamento, apoio, operação, avaliação de desempenho e melhoria. O Quadro 4 descreve detalhadamente qual o objetivo de cada seção.

Quadro 4 – Requisitos e Objetivos de Requisitos da ISO 9001:2015

Requisito	Objetivo do Requisito
Contexto da organização	Esta seção trata da compreensão do contexto interno e externo da organização, das necessidades e expectativas das partes interessadas, da determinação do escopo do sistema de gestão da qualidade (SGQ) e da definição dos processos do SGQ.
Liderança	Foca na responsabilidade da liderança em relação ao SGQ, incluindo a necessidade de demonstrar comprometimento, estabelecer uma política de qualidade, definir papéis, responsabilidades e autoridades dentro da organização.
Planejamento	Envolve ações para abordar riscos e oportunidades, estabelecer objetivos de qualidade e planejar como alcançá-los, além de considerar as mudanças necessárias no SGQ.
Apoio	Inclui os recursos necessários para o SGQ, como pessoas, infraestrutura, ambiente para operação de processos, recursos de monitoramento e medição, competência, conscientização, comunicação e informação documentada.
Operação	Trata do planejamento e controle operacional, requisitos para produtos e serviços, comunicação com o cliente, determinação de requisitos relacionados aos produtos e serviços, design e desenvolvimento, controle de processos, produção e fornecimento de serviços, liberação de produtos e serviços, e controle de saídas não conformes.
Avaliação de desempenho	Envolve monitoramento, medição, análise e avaliação do desempenho do SGQ, incluindo auditorias internas e análises críticas pela direção.
Melhoria	Foca na melhoria contínua do SGQ, abordando não conformidades e ações corretivas, e buscando sempre a melhoria contínua dos processos e do desempenho organizacional.

Fonte: Almeida *et al.* (Adaptado) (2018)

Associado a ISO 9001:2015, existem pesquisas na literatura que apontam os principais fatores de sucesso (FCS) para uma boa implementação dessa norma. São classificados em dez fatores, conforme o Quadro 5. Almeida *et al.* (2018) observa que o principal fator de sucesso para a implementação da norma é o comprometimento da alta gestão.

Quadro 5 – FCS e suas descrições

Fatores Críticos de Sucesso	Descrição
Comprometimento da alta gestão	O envolvimento da alta gestão é crucial para apoiar a implementação, motivar os funcionários e promover a comunicação eficaz sobre a certificação.
Comprometimento da equipe	A implementação é mais eficaz quando há um forte compromisso da equipe interna. O uso excessivo de consultores externos sem a colaboração interna pode resultar em desconexão e falta de adoção verdadeira.
Treinamento	Programas de treinamento ajudam os funcionários a entender e aplicar os padrões de qualidade, além de alinhar as metas estratégicas da organização.
Responsabilidades e Autoridades claramente definidas	Um planejamento adequado e a definição clara de responsabilidades e autoridades garantem a integração dos funcionários no processo de implementação.
Cronograma de Implementação e Manutenção	Um cronograma bem definido para a implementação e um plano de manutenção pós-implementação são essenciais para mitigar dificuldades e assegurar a eficácia do sistema de qualidade.
Cultura de Qualidade	A cultura organizacional baseada em valores de qualidade é fundamental para o comportamento relacionado à qualidade dentro da organização.
Disponibilidade de recursos	Acesso a recursos financeiros e econômicos é crucial para a implementação do sistema de gestão da qualidade, especialmente em setores com desafios estruturais.
Integração entre departamentos	A integração eficaz entre departamentos e a compreensão clara das funções e missões organizacionais são necessárias para o sucesso da implementação.
Nível de burocracia	A burocracia pode ser um obstáculo para a implementação de programas de qualidade, exigindo atenção especial dos stakeholders para evitar falhas no processo.
Conscientização sobre a Importância da ISO 9001	percepção inadequada da importância dos sistemas de qualidade pelos funcionários é um obstáculo crítico para a implementação bem-sucedida.

Fonte: Almeida *et al.* (2018)

Além da ISO 9001, existe outra norma importante. Trata-se da ISO 9004. Esta oferece diretrizes para aumentar a eficiência e eficácia de um SGQ, com o objetivo de melhorar o desempenho global da organização. Não é uma norma em si, funciona mais como uma guia, uma orientação, a qual visa a melhoria contínua dos sistemas (ANTTILA e JUSSILA, 2021; BRAVI e MURMURA, 2021).

A norma sugere a implementação de um processo de medição da organização como ferramenta para avaliar, em todos os níveis, o grau de alcance dos resultados planejados e do desempenho. O último capítulo da norma é dedicado à melhoria, inovação e aprendizado, abordando tanto os aspectos tangíveis quanto intangíveis da organização, incluindo produtos, processos, estrutura organizacional, sistema de gestão, aspectos humanos e culturais, infraestruturas, meio ambiente e relações com as partes interessadas (ANTTILA e JUSSILA, 2021; BRAVI e MURMURA, 2021).

A lógica da melhoria contínua deve se tornar parte integrante da cultura da organização, com um processo real orientado para a melhoria, envolvendo ativamente os funcionários. Em uma organização "madura", as pessoas devem receber a confiança da alta administração, serem valorizadas, incentivadas a participar de atividades de melhoria e a propor ideias. O aprendizado

é reconhecido como a base para uma melhoria eficaz e eficiente e para processos de inovação (ANTTILA e JUSSILA, 2021; BRAVI e MURMURA, 2021).

2.4 HIPÓTESES DE PESQUISA

Neste sub-capítulo, o Quadro 6 apresenta as perguntas que emergiram ao longo do Capítulo 2 e que servirão de base para a pesquisa. No total, foram formuladas 10 perguntas, organizadas conforme suas respectivas seções. Para respondê-las, foram estabelecidas 11 hipóteses. Esse quadro será explorado nos Capítulos 4 e 5, conectando as seções e fundamentando a análise dos resultados.

Quadro 6 – Guia para a pesquisa

Perguntas	Hipóteses
P1: Os guias e métodos para classificação de risco indicados na ISO série 27002 de fato são aplicados e contribuem para segurança de CPS? (Seção 2.2.1)	H1: A ISO 27000 apoia os CPS. H2: Os guias e métodos de classificação de risco da ISO 27002 contribui para cibersegurança.
P2: Qual o tipo de ataque mais comum e com que frequência ocorrem? (Seção 2.2.2)	H3: Há diferentes tipos de ataques de maior ou menor frequência que precisam ser priorizados.
P3: Técnicas estatísticas de monitoramento de processo (CEP) podem ser utilizadas na detecção e prevenção de ataques *hacker*? (Seção 2.3.1)	H4: As técnicas estatísticas de monitoramento são aplicáveis para prevenção e detecção de ataques *hacker*.
P4: *Framework*, como o MITRE ATT&CK e demais diretrizes, como ferramentas de monitoramento atualização de sistemas, auditorias contribuem de fato para a prevenção e detecção de ciberataques? (Seção 2.2.2)	H5: há evidência de que o *framework* e demais diretrizes, como ferramentas de monitoramento atualização de sistemas, auditorias contribuem para prevenção e detecção de ciberataques.
P5: As Legislações brasileiras atuais contribuem para fortalecer os sistemas de cibersegurança das organizações? (Seção 2.2.3)	H6: O Brasil possui legislação sobre cibersegurança, porém pouco efetiva.
P6: O SGQ contribui para a cibersegurança e de que forma que a falta desta pode impactar negativamente os sistemas de cibersegurança? (Seção 2.3)	H7: Há evidência de que atualmente o SGQ tenha contribuído para a cibersegurança.
P7: Há gargalos e desafios (falta de conhecimento) para aplicação de métodos estatísticos na área de cibersecurança? (Seção 2.3.1)	H8: Há gargalos e desafios significativos que inibem a adoção de técnicas estatísticas em sistemas de cibersegurança.
P8: Os profissionais da área conhecem as técnicas para detecção de ataques e as utilizam com qual frequência? Os profissionais da área utilizam o *machine learning*? (Seção 2.3.1)	H9: Há técnicas e métodos de prevenção que são usadas com mais frequência do que outras.
P9: Os princípios da qualidade, como os da família ISO 9000, influenciam a gestão de sistemas de cibersegurança nas organizações para prevenção de ataques? (Seção 2.3.2)	H10: Os princípios da qualidade, como os da família ISO 9000, colaboram na área de cibersegurança para prevenção de ciberataques.

P10: Qual o nível de criticidade dos desafios enfrentados pelas organizações para melhorar continuamente seus sistemas de proteção contra ataques? (Seção 2.3.2)	H11: Há desafios a enfrentar para a melhoria contínua em graus de criticidade sobressai em relação a outros.

Fonte: Autoria própria (2025)

3 METODOLOGIA

Neste capítulo será apresentado a caracterização da pesquisa, no subcapítulo 3.1, bem como os procedimentos escolhidos para a execução da pesquisa, no subcappítulo 3.2. Os procedimentos são aprofundados nas sub-seções 3.2.1 e 3.2.2.

3.1 CARACTERIZAÇÃO DA PESQUISA

No Capítulo 1 deste trabalho foi apresentado o objetivo de pesquisa: mostrar como a gestão da qualidade pode contribuir na prevenção e detecção de ataques de *hackers*. Esse objetivo aponta a natureza **básica** dessa pesquisa. Pesquisas com essa característica visam gerar novos conhecimentos para o avanço da ciência, no caso deste trabalho, para o avanço do gerenciamento da qualidade e da cibersegurança (GERHARDT; SILVEIRA, 2009).

Essa pesquisa tem objetivo de ser **exploratória**, uma vez que possui um enfoque mais teórico e visa gerar novos conhecimentos no campo da gestão da qualidade e da cibersegurança. Pretende-se também utilizar-se de abordagens **quantitativas** e **qualitativas** para aprofundar e compreender o estado da arte atual do tema, as inter-relações entre assuntos e temas que de algum modo transita no entorno do objeto de pesquisa, que é que é o papel dos da gestão da qualidade na prevenção e detecção de ataques *hackers* (GERHARDT; SILVEIRA, 2009).

Os procedimentos escolhidos para a pesquisa se devem muito ao objetivo ser exploratório. Trata-se da **pesquisa bibliográfica** e da **pesquisa de campo**. Esses tipos de procedimentos serão discutidos no próximo subcapítulo.

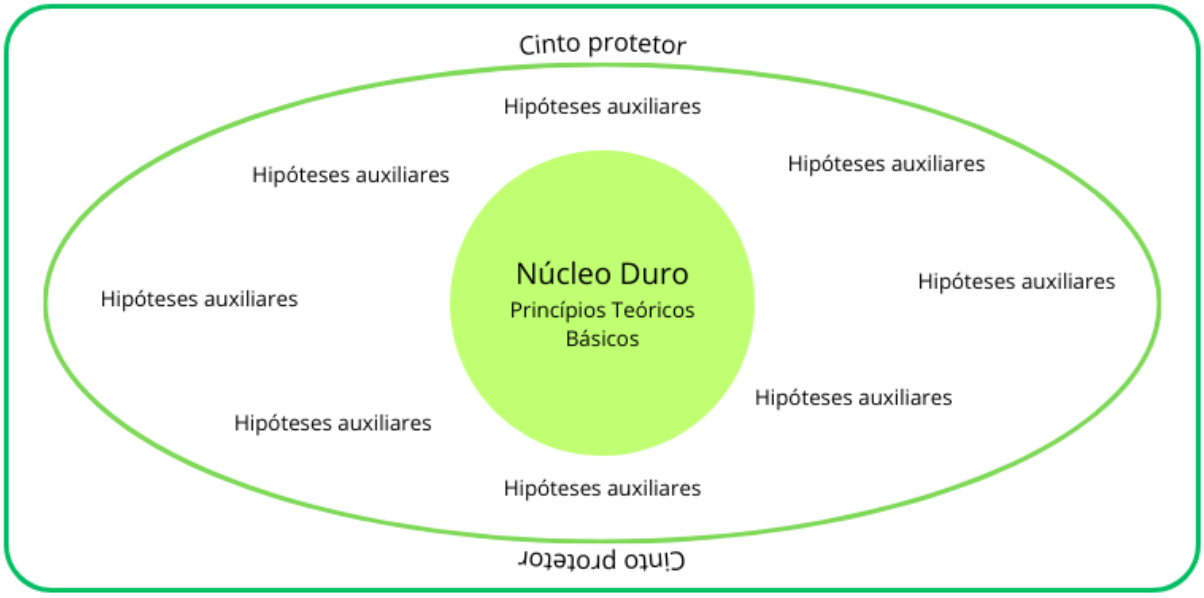
3.2 PESQUISA BIBLIOGRÁFICA

Uma base teórica que sustenta a análise do desenvolvimento de um determinado campo do conhecimento, é a abordagem de programas de pesquisa de Lakatos, que sugere que a ciência avança por meio de programas de pesquisa, que consistem em um "núcleo duro" de princípios teóricos básicos e em um "cinto protetor" de hipóteses auxiliares (LAKATOS, 1978). O conceito de “núcleo duro” é significativo na história e na filosofia da ciência, uma vez que ecoa

a teoria da racionalidade de Lakatos. Imre Lakatos associou um conjunto de teorias com o que ele chamou de programa de pesquisa, cujo núcleo se refere a características comuns das teorias compartilhadas por todos os cientistas que atuam neste programa de pesquisa (LAKATOS, 1978). A Figura 6 mostra de forma lúdica a estrutura do programa de pesquisa de Lakatos.

No contexto da segurança cibernética em sistemas produtivos, o núcleo duro seria composto por princípios fundamentais que são essenciais para a proteção eficaz contra ataques *hackers*. Isso pode incluir a integridade do acesso aos sistemas, a confidencialidade dos dados, a disponibilidade contínua dos serviços essenciais e a resiliência contra ataques. O cinto protetor representa as estratégias e medidas práticas adotadas para adotar os princípios do núcleo duro. Hipóteses auxiliares podem incluir a implementação de protocolos e procedimentos para proteção contra acessos não autorizados, bem como o uso de métodos estatísticos para a detecção de intrusão para identificar atividades suspeitas, a aplicação regular de atualizações para a melhoria contínua nos procedimentos de segurança para mitigar vulnerabilidades conhecidas.

Figura 6 – Representação do programa de pesquisa de Lakatos



Fonte: Autoria própria (2025)

Seguindo a abordagem de Lakatos (1978), poderia se afirmar que deveria haver uma revisão contínua das hipóteses auxiliares em resposta a falhas ou inadequações na proteção contra ataques maliciosos aos sistemas produtivos. Se uma medida de segurança específica não atender às expectativas ou se tornar obsoleta, devido a evoluções na tecnologia ou em estratégias de ataque, ela deveria ser revisada ou substituída. Essa flexibilidade é crucial para se adaptar às ameaças em constante evolução no cenário de segurança cibernética. O progresso

ocorre quando um programa de pesquisa demonstra uma maior capacidade de explicação e predição, mesmo quando as hipóteses auxiliares são revisadas (LAKATOS, 1978). No contexto da segurança cibernética, o progresso seria evidenciado pela melhoria contínua na eficácia das medidas de proteção, na detecção precoce de ameaças e na capacidade de resposta eficiente a incidentes.

Ambos os campos desta pesquisa compartilham o objetivo central de garantir confiabilidade e minimizar riscos. Essa convergência sugere que os princípios fundamentais da gestão da qualidade podem ser adaptados para criar sistemas cibernéticos mais robustos. Ferramentas como análise de risco e conformidade regulatória são pertinentes a ambos, exemplificada pela integração das normas ISO 9001 (gestão da qualidade) com ISO 27001 (segurança da informação). Métodos e ferramentas da qualidade, como o Controle Estatístico de Processo (CEP), o ciclo PDCA e os diagramas de Ishikawa, podem ser empregados para identificar e mitigar riscos cibernéticos em ambientes industriais conectados.

Na década de 1950, já se observa o início das discussões sobre a revisão bibliométrica. Contudo, foi apenas em tempos mais recentes que essa abordagem metodológica ganhou significativa popularidade, especialmente devido à sua eficácia no tratamento de grandes volumes de dados científicos, desempenhando um papel impactante na pesquisa. Em outros termos, a revisão bibliométrica, conforme destacado por Donthu *et al*. (2021), emerge como uma ferramenta valiosa para compreender extensos conjuntos de dados, proporcionando uma compreensão mais profunda e abrangente do cenário científico em questão.

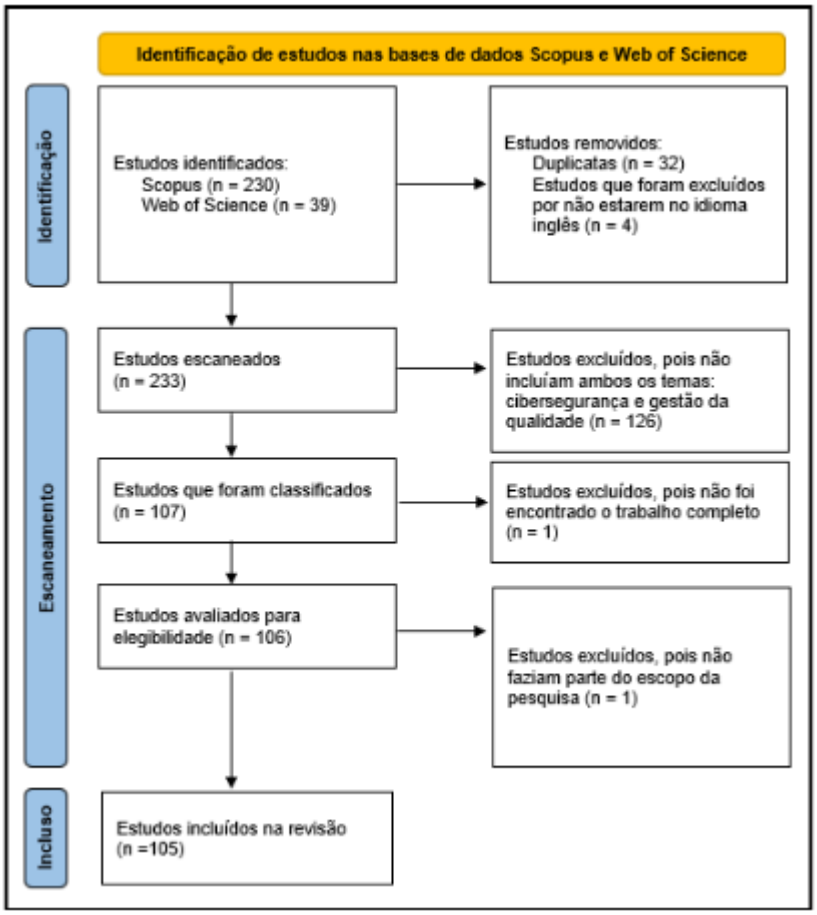
A pesquisa bibliográfica desempenha um papel crucial na análise do desenvolvimento de um programa de pesquisa em ataques cibernéticos, especialmente quando se aplica a perspectiva de Imre Lakatos. Ela permite identificar os princípios fundamentais (núcleo duro) relacionados aos ataques cibernéticos, como as principais vulnerabilidades, estratégias de ataque e princípios subjacentes à segurança cibernética em sistemas produtivos. Ao revisar a literatura, é possível mapear o "cinto protetor" do programa de pesquisa, composto por estratégias específicas, ferramentas e métodos utilizados ao longo do tempo para prevenir ou mitigar ataques cibernéticos. Isso inclui a evolução do uso de métodos estatísticos apropriados, como um sistema de detecção de intrusão.

Analisando trabalhos acadêmicos ao longo do tempo, é possível identificar como o programa de pesquisa em ataques cibernéticos tem progredido. Isso inclui a introdução de novos conceitos, aprimoramentos em técnicas de defesa e adaptações às crescentes complexidades das ameaças cibernéticas. Por fim, a revisão bibliográfica e a bibliometria ajuda a identificar lacunas

na pesquisa existente e os desafios persistentes enfrentados no campo dos ataques maliciosos. Essas lacunas podem indicar áreas que necessitam de mais atenção e desenvolvimento.

Diante disso, foram usadas as bases de dados científicas *Scopus* e *Web of Science* para fazer a análise bibliométrica. As palavras de busca escolhidas para a *string* foram ((*"cyber attack" or "intrusion detection"*) *and* (*"quality control" or "quality system" or "control chart" or "quality management"*)). Com tais termos foi possível encontrar 230 documentos na base de dados *Scopus* e 39 na base de dados *Web of Science*, até a data de 21 de agosto de 2024.

Figura 7 – Estrutura da busca por trabalhos



Fonte: Autoria própria (2025)

Para a análise, documentos duplicados foram inicialmente excluídos, pois foi observado que alguns artigos foram repetidos em diferentes bancos de dados. Portanto, um total de 32 documentos foram excluídos. Um dos critérios de inclusão foi a língua, aceitando apenas documentos em inglês e excluindo documentos em outros idiomas; nesta etapa, 4 artigos foram excluídos. Outro critério de inclusão foi que os documentos deveriam abordar os dois temas principais desta pesquisa (cibersegurança e gestão da qualidade), e, portanto, artigos que não cobriam ambos os temas foram excluídos. Nesta etapa, 107 artigos permaneceram para leitura

completa; no entanto, um dos artigos não foi encontrado na íntegra, reduzindo o número de documentos para 106. Após a leitura destes, observou-se que um dos artigos não estava dentro do escopo da pesquisa, e, portanto, também foi excluído. Seguindo todos os critérios, 105 artigos foram obtidos para análise. A Figura 7 ilustra como a busca bibliográfica nas bases de dados foi conduzida.

Foram propostas duas etapas para análise bibliométrica. A primeira é a análise descritiva, a qual consiste em examinar as contribuições dos elementos da pesquisa em um campo. É uma prática padrão de revisões, e existem inúmeros indicadores que podem ser levados em conta para as análises. Comumente, utiliza-se o número de publicações e citações por ano ou por elemento da pesquisa, em que a publicação é um indicador de produtividade, enquanto a citação é uma medida de impacto e influência (DONTHU *et al.*, 2021).

Para tal análise utilizou-se o *software* RStudio, o qual utiliza a linguagem de programação R, possibilitando a importação de dados em diferentes formatos e oferecendo uma ampla gama de ferramentas de visualização. Isso inclui a capacidade de criar gráficos e tabelas informativas, facilitando a análise de dados. No contexto específico deste trabalho, o pacote Bibliometrix foi empregado para a análise descritiva da bibliometria. Esse pacote permite que os pesquisadores avaliem tendências de pesquisa, redes de coautoria, impacto de periódicos, evolução de palavras-chave, entre outros aspectos relacionados à produção científica.

A segunda etapa trata-se de um mapeamento científico, o qual consiste em examinar as relações entre os elementos da pesquisa. Frequentemente, analisa-se a relação entre as publicações, entre os autores, entre as citações, palavras-chaves, dentre outras (DONTHU *et al*, 2021). Optou-se pelo uso de métodos multivariados e *Text Mining* na análise dos artigos levantados, por meio do *software* Statistica. Este não apenas aplica modelos estatísticos avançados para investigar hipóteses e testar teorias, mas também se destaca na extração eficiente das informações mais relevantes do texto.

Quanto aos métodos estatísticos aplicados na análise de dados, optou-se pela análise fatorial aplicada na análise bibliométrica, que é útil para identificar conceitos-chave no campo, representando o núcleo duro do programa de pesquisa. Nesta análise, os fatores são escolhidos de forma a maximizar a variância explicada nas variáveis originais (HAIR *et al.*, 2009; MANLY, 2008). Os resultados incluem as chamadas "cargas fatoriais", que indicam a relação entre cada variável original e os fatores extraídos. Se a carga fatorial assume valor positivo, significa que a variável está positivamente correlacionada com o fator, caso a carga assuma um valor negativo, significa que a variável está negativamente correlacionada ao fator. Também é

importante observar que quanto maior a carga fatorial, maior contribuição o item possui para o fator (HAIR *et al.*, 2009; MANLY, 2008).

O processo de análise fatorial envolve a extração de fatores a partir das correlações entre as variáveis originais. A ideia é identificar quais variáveis tendem a variar juntas e, assim, agrupá-las sob um fator comum. Esses fatores são interpretados como construtos latentes que não são diretamente observáveis, mas que explicam parte da variabilidade nas variáveis observadas (HAIR *et al.*, 2009; MANLY, 2008).

A análise estatística fornece os valores das covariâncias das palavras principais encontradas nos títulos e resumos dos artigos, assim como os escores dos fatores de cada trabalho. Nessa análise, considerou-se quatro fatores. As palavras destacadas pelo *software* foram comparadas com os *scores* dos trabalhos, caso as palavras tivessem valor negativo eram comparadas com os trabalhos que possuíam maior valor negativo para o fator correspondente. Da mesma forma para quando o valor era positivo.

Quando os fatores subjacentes nos documentos bibliométricos são extraídos, pode-se identificar padrões significativos e conceitos centrais que moldam o entendimento do tema. A análise fatorial permite também explorar as relações entre diferentes variáveis bibliométricas, como número de citações, colaborações entre autores e frequência de palavras-chave. Essas variáveis constituem o cinto protetor do programa de pesquisa, proporcionando uma visão mais ampla das diferentes dimensões do campo estudado. Essa técnica multivariada auxilia também na análise da progressão do programa em termos de mudanças nos padrões e paradigmas, e mesmo identificar fatores emergentes ou em declínio, o que pode indicar como o tema está evoluindo e respondendo a novas tendências e desafios no campo.

Após a análise dos fatores foi feita a análise de agrupamento, a qual é utilizada para classificar um conjunto de objetos ou observações em grupos homogêneos, chamados de *clusters*. O objetivo principal é agrupar elementos semelhantes entre si e distintos dos elementos de outros *clusters*, de forma que a variabilidade interna do grupo seja minimizada, enquanto a variabilidade entre os grupos seja maximizada (HAIR *et al.*, 2009; MANLY, 2008).

A análise de *cluster* foi empregada para identificar agrupamentos de documentos relacionados que representam temas ou conceitos centrais. Esses agrupamentos podem refletir o núcleo duro do programa de pesquisa, revelando conexões significativas entre diferentes áreas do conhecimento. O que é essencial para compreender o cinto protetor do programa de pesquisa, abrangendo diferentes abordagens, métodos e aplicações presentes na literatura. E também, ajudar a avaliar a coerência conceitual do programa de pesquisa em ataques cibernéticos em sistemas produtivos, e revelar subtemas emergentes ou declinantes.

Adoção da abordagem do programa de pesquisa de Lakatos como guia para este estudo permite a identificação de sinergias entre áreas distintas de pesquisa. Ela estabelece uma ponte entre a pesquisa em gestão da qualidade e a proteção de sistemas ciberfísicos. Isso garante que a análise permaneça orientada pela teoria, estruturada e capaz de revelar o progresso compartilhado na evolução desses campos interconectados. A análise bibliométrica inicia-se identificando os princípios "núcleo rígido" de ambos os campos - confiabilidade e minimização de riscos - como valores fundamentais compartilhados. Esta etapa é crítica para estabelecer a relevância teórica da integração entre gestão da qualidade e cibersegurança. A análise se concentra nos "cinturões protetores" examinando ferramentas, estratégias e métodos que evoluíram para sustentar os princípios fundamentais em cada campo. A análise bibliométrica identifica sistematicamente influências interdisciplinares, por exemplo, explorando os gráficos de controle na cibersegurança.

3.3 PESQUISA DE CAMPO

Durante a revisão da literatura no Capítulo 2 deste trabalho, surgiram dúvidas sobre o tema de cibersegurança e de gestão da qualidade, que foram apresentadas no sub-capítulo 2.4. Portanto, em busca de se obter uma melhor compreensão do tema, para verificar se e como a gestão da qualidade consegue ser integrada a área de cibersegurança foi utilizado como método a pesquisa de campo, em específico, a pesquisa participante.

Gerhardt e Silveira (2009) explicam que a pesquisa envolve a coleta de dados diretamente no ambiente onde os fenômenos estudados ocorrem, ou seja, os dados extrapolam a revisão bibliográfica e permitem que o pesquisador utilize de outros recursos para tentar responder o problema de pesquisa levantado no Capítulo 1 deste trabalho.

A pesquisa participante, por sua vez, caracteriza-se pelo envolvimento do pesquisador e dos investigados, explicam Gerhardt e Silveira (2009). Essa abordagem facilita a observação direta das práticas, comportamentos e percepções dos participantes, contribuindo para uma análise mais completa e realista dos processos de integração entre a cibersegurança e o gerenciamento da qualidade.

Como instrumento de coleta de dados, a entrevista com especialistas é uma técnica para obter *insights* detalhados e opiniões qualificadas sobre o tema estudado. As entrevistas complementam a literatura e permitem que o pesquisador tome consciência dos aspectos das questões de pesquisa que a sua própria experiência e leitura não puderam compreender (GERHARDT e SILVEIRA, 2009). Especialistas, com sua experiência e conhecimento

aprofundado, fornecem informações que podem complementar e enriquecer os dados coletados através da observação participante.

Inicialmente as entrevistas foram realizadas de forma semi-estruturada com um roteiro previamente estabelecido, baseado nas perguntas levantadas no Capítulo 2 deste trabalho. O questionário foi validado por um especialista para poder ser aplicado. Em sua primeira avaliação, o especialista pontuou que enfatizar técnicas de detecção significava abordar o tema de forma rasa, e sugeriu que o questionário abordasse em sua maior parte questões voltadas para gestão. Portanto, a revisão da literatura foi refeita e novas dúvidas surgiram, mudando o foco do questionário, que foi aprovado por quatro especialistas. Tais especialistas trabalham com cibersegurança em empresas do ramo de serviços, como agências bancárias, consultoria de cibersegurança e, também na área de manufatura cerâmica.

Após o teste piloto desse modelo de entrevista notou-se que ainda era necessário fazer ajustes para que fosse possível coletar mais dados, portanto, a entrevista aberta foi transformada em fechada em um Google Forms, a qual se encontra no Apêndice A deste trabalho. As perguntas passaram a ter respostas de intensidade ou frequência relacionadas ao tópico abordado na pergunta. O nível das escalas utilizadas foi 3, para perguntas de intensidade utilizou-se os critérios como “Totalmente”, “Parcialmente” e “Pouco”; “Bastante”, “Pouco” e “Nenhum”. Para perguntas de frequência a escala utilizada foi “Muito frequente”, “Frequente” e “Pouco frequente”. Demais escalas foram empregadas, como grau de desafio, grau de criticidade, ambas em nível 3 também.

A escala com 3 níveis foi escolhida por sua simplicidade, clareza e adequação ao objetivo de capturar a variação na intensidade das respostas de forma direta. Essa abordagem evita o excesso de categorias, facilita a análise estatística e está alinhada às recomendações metodológicas para pesquisas com questionários fechados, garantindo respostas consistentes e interpretáveis.

Os participantes foram escolhidos tanto por indicação quanto pela rede social LinkedIn. Os especialistas em questão eram os profissionais especialistas em cibersegurança, que já tivessem tido experiências com a ISO 27000 e com o *framework* MITRE ATT&CK. Os especialistas também deveriam ter experiência com gestão, e não apenas com a parte operacional. O questionário foi enviado à 119 possíveis respondentes e foram obtidos 27 respostas válidas.

As primeiras perguntas foram feitas para caracterização da amostra, como qual cargo ocupa, qual o seguimento atuante e qual a conexão com a cibersegurança, com o objetivo de verificar quem eram esses especialistas entrevistados.

Foram feitas análises descritivas dos dados coletados, utilizando o gráfico de Pareto para revelar a ordem de importância da percepção dos especialistas (questões 4, 5, 6, 7, 8, 11, 14 e 13). O objetivo dessa ferramenta visual é destacar os fatores mais significativos em um conjunto de dados. Dessa forma, as barras mais altas e mais à esquerda do gráfico são as mais importantes ou frequentes, sendo possível classificar a percepção do especialista sobre o tópico da pergunta em questão (MONTGOMERY e RUNGER, 2021).

Para analisar as respostas coletadas no questionário aplicado (questões 9, 10, 12, 15 e 16), foi utilizado o teste qui-quadrado (X_0^2) para tabelas de contingência. Esse teste permite avaliar se há associação (dependência) entre duas variáveis categóricas, comparando as frequências observadas com as frequências esperadas sob a hipótese de independência, explicam Montgomery e Runger (2021).

Montgomery e Runger (2021) explicam que uma hipótese estatística é uma afirmação utilizada como base para a investigação científica. Geralmente, estabelece-se a hipótese nula (H_0) como uma suposição de igualdade ou ausência de efeito, enquanto a hipótese alternativa (H_1) indica a presença de um efeito, relação ou diferença significativa. Ou seja, a hipótese alternativa representa o que é inovador no tema. Por meio do teste de hipóteses, é possível verificar a validade dessas suposições. Esse procedimento utiliza informações provenientes de uma amostra aleatória da população de interesse. Se os dados forem consistentes com a hipótese nula, ela não será rejeitada; caso contrário, a hipótese nula será rejeitada, e a hipótese alternativa será aceita.

Evidencia-se que a veracidade ou falsidade de uma hipótese particular pode nunca ser conhecida com certeza, exceto se possível examinar a população completa. Testar a hipótese trata-se de considerar uma amostra aleatória, computar uma estatística de teste e utilizá-la para auxiliar no processo de tomada de decisões (MONTGOMERY e RUNGER, 2021).

Os n dados observados foram organizados em tabelas com r linhas e c colunas. Em seguida, é necessário saber quais eram os dados esperados, dessa forma, é feita uma nova tabela, com r linhas e c colunas de dados esperados. Conforme Montgomery e Runger (2021), os dados esperados são calculados pela fórmula (1):

$$E_{ij} = \frac{n_{i.} n_{.j}}{n} \qquad (1)$$

Sendo n o total de elementos da amostra;

$n_{i.}$ somatório da frequência observada das linhas;

$n_{.j}$ somatório da frequência observada das colunas;

n somatório das linhas e colunas da tabela de dados observados;

E_{ij} a frequência esperada.

A estatística qui-quadrada (X_0^2) , com $(r-1)(c-1)$ graus de liberdade, é calculada pela fórmula (2) (MONTGOMERY e RUNGER 2021):

$$X_0^2 = \sum_{i=1}^{r} \sum_{j=1}^{c} \frac{(O_{ij} - E_{ij})^2}{E_{ij}} \qquad (2)$$

Sendo O_{ij} a frequência observada;

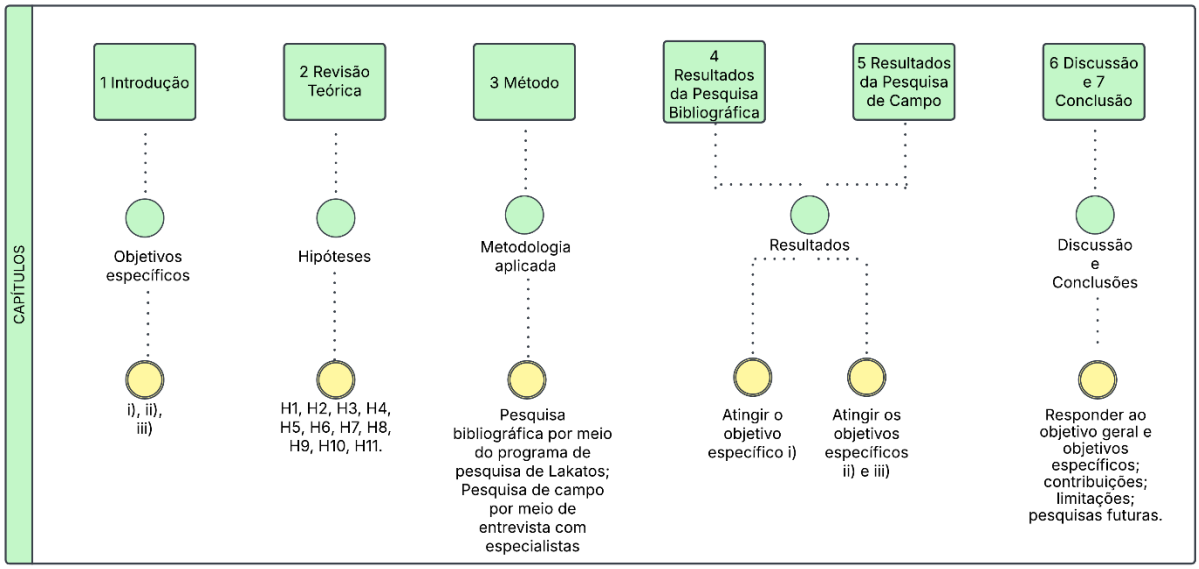
E_{ij} a frequência esperada.

A decisão do teste acontece da seguinte forma: se o X_0^2 calculado é maior que X_0^2 crítico, rejeita-se H_0, utilizando-se um nível de significância (α) pré-determinado pelo pesquisador.

Outra forma de tomar a decisão é baseada no p-*value*, que indica a probabilidade de observar os dados (ou algo mais extremo) caso a hipótese nula seja verdadeira, conforme explicam Montgomery e Runger (2021). Em outras palavras, o p-*value* representa o nível de significância observado.

A decisão é tomada da seguinte forma: se o p-*value* for muito pequeno, ou seja, menor que o nível de significância previamente definido pelo pesquisador (neste trabalho, α = 5%), há evidências significativas para rejeitar H_0. Caso contrário, não há evidências suficientes para rejeitar H_0, concluindo-se que os dados são consistentes com a hipótese de independência (MONTGOMERY e RUNGER 2021).

Figura 8 – Fluxograma da metodologia de pesquisa



Fonte: Autoria própria (2025)

Os cálculos foram realizados no *software* R. As questões foram analisadas individualmente e os resultados apresentados no Capítulo 4 e 5 deste trabalho.

A partir dos resultados foram feitas propostas para tentar integralizar as áreas e fortalecer a segurança cibernética. A Figura 8 apresenta o fluxograma da metodologia da pesquisa, que conecta os capítulos com os pontos principais da pesquisa.

4 RESULTADOS DA REVISÃO BIBLIOGRÁFICA

Neste capítulo será apresentado os resultados da revisão bibliográfica. O primeiro sub-capítulo (4.1) revela a descrição dos trabalhos encontrados. O sub-capítulo 4.2 apresenta o mapeamento científico na cibersegurança, sob a perspectiva de Lakatos. O sub-capítulo 4.3 apresenta um comparativo entre os achados da bibliometria e revisão teórica (Capítulo 2). O último sub-capítulo (4.4) apresenta os fatores relacionados as perguntas e hipóteses levantadas no sub-capítulo 2.4 deste trabalho.

4.1 ANÁLISE DESCRITIVA

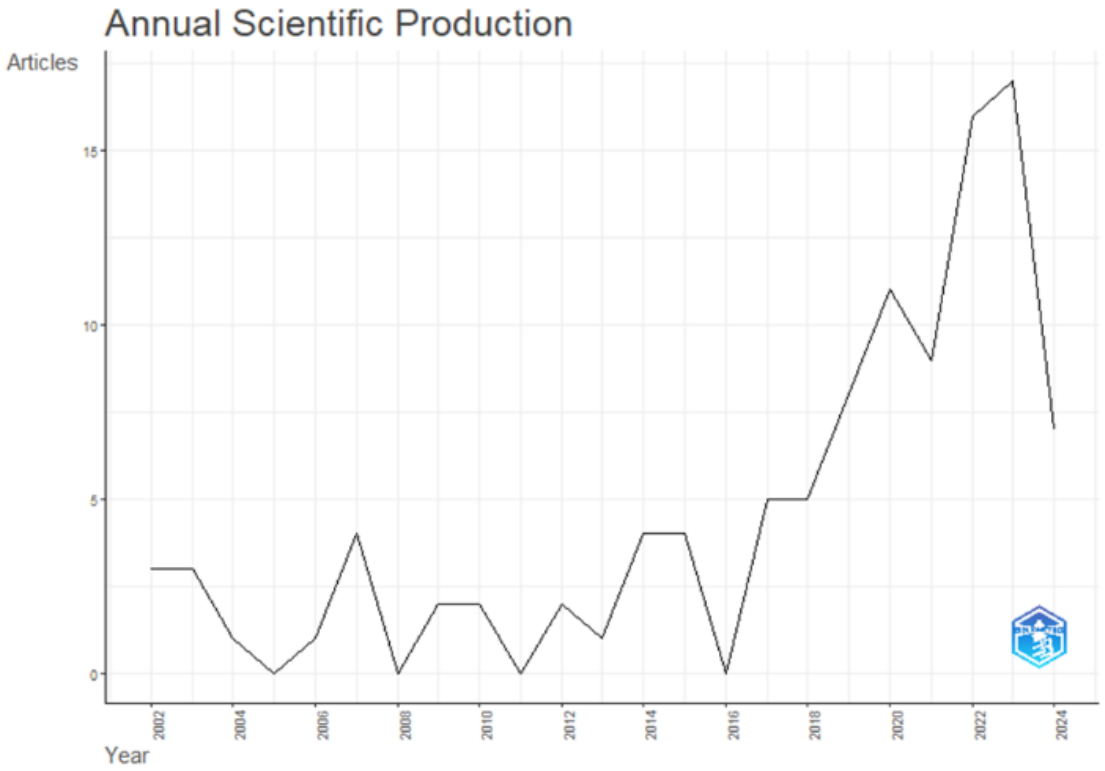
Ao empregar análise descritiva de maneira aprofundada e contextualizada, esta proporcionará uma compreensão clara e detalhada dos fenômenos relacionados às produções científicas sobre ataques *hackers* em sistemas produtivos, promovendo uma base sólida para discussões mais aprofundadas e conclusões embasadas.

Utilizando a metodologia delineada, por meio do *software* RStudio, observou-se que a investigação sobre o tema teve seu início em 2002 e perdura até o presente momento. Contudo,

há somente 105 documentos abordando a temática proposta, como é apresentado no Apêndice B deste trabalho. O levantamento apontou a participação de 308 autores, com um total de 357 palavras-chave.

Constatou-se que, ao examinar as publicações, em 2002 houve apenas 3 publicações, enquanto em 2023 esse número aumentou para 17. Nota-se que o assunto entrou em crescente desde 2017. Embora a quantidade de documentos publicados até o momento seja limitada, vislumbra-se a perspectiva de aumento do número de publicações sobre ataques cibernéticos combinado com temas relacionados à gestão da qualidade. Esse aumento pode ser observado no Gráfico 1.

Gráfico 1 - Quantidade de publicações por ano.



Fonte: Autoria própria (2025)

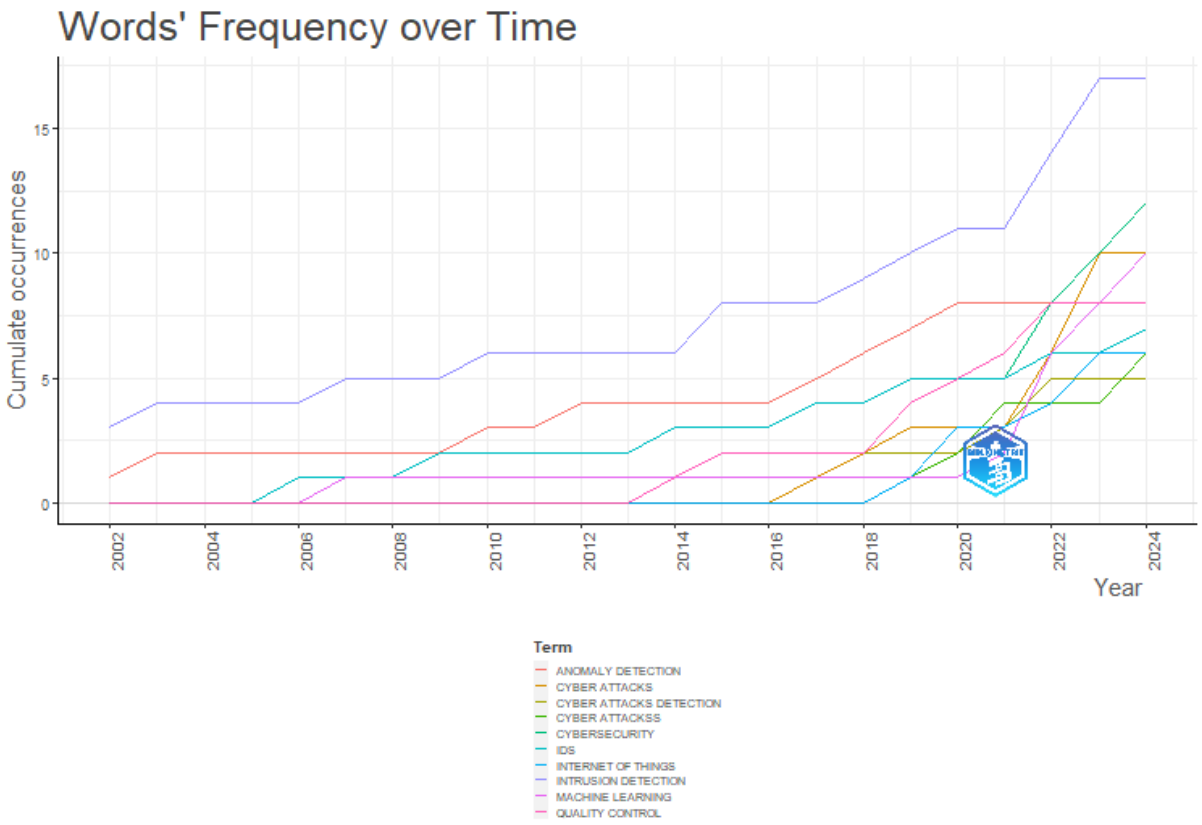
Ao analisar o conteúdo dos títulos e resumos dos artigos, destacaram-se apenas 82 dos 357 termos chave. A Figura 9 mostra a nuvem de palavras destacando as palavras-chave que mais apareceram. O termo “intrusion detection” apareceu 17 vezes, o termo “*cyber attacks*” apareceu 16 vezes, seguido “*cybersecurity*”, que apareceu 12 vezes, “*machine learning*” apareceu 10 vezes, “*anomaly detection*” e “*quality control*” apareceram 8 vezes cada.

Figura 9 – Nuvem de palavras-chave

Fonte: Autoria própria (2025)

A partir dessas palavras foi possível identificar a frequência acumulada de palavras ao longo do tempo, ou seja, verificar quais palavras-chave que estão se tornando cada vez mais populares nesta área ao longo do tempo. A Figura 10 apresenta esta frequência, por exemplo, "*intrusion detection*" e "*anomaly detection*" são palavras que sempre estiveram presentes e em ascensão. Sistemas de detecção de intrusão - IDS surgiram logo em seguida, em 2003. Em 2007 o termo "*machine learning*" apareceu, contudo só começou a ter notoriedade a partir de 2021. A primeira vez que o termo-chave "*quality control*" apareceu foi em 2014, mas foi a partir de 2019 que o termo ganhou destaque dentro da área de ciberataques. O mesmo ocorreu com o tema "*cybersecurity*". Palavras-chave como "*cyber attack*", "*cyber attackss*" e "*cyber attacks detection*" começaram a ganhar notoriedade em 2019, tendo os últimos 3 anos como maior destaque.

Figura 10 – Frequência acumulada de palavras ao longo dos anos



Fonte: Autoria própria (2025)

Quanto aos principais autores, em termos da quantidade de publicações, os autores Ahsan M. e Mashuri M. são os principais pesquisadores do tema, com nove e oito publicações sobre o assunto, respectivamente. Em seguida têm-se os pesquisadores Khusna H., Kuswanto H. e Prastyo. D., com seis publicações. Ye N. é o pioneiro no assunto, começando com as publicações em 2002, e Cisar P. que começou a publicar sobre o tema em 2006. Outros autores que se destacam com publicações relevantes são os seguintes: Wells L. e Camelio J., Elhabashy, Ahsan M., Mashuri M., Khusna H., Kuswanto H. e Prastyo. D. que publicaram seus trabalhos entre 2014 à 2023. O Quadro 6 destaca os principais autores no tema ciberataques e GQ. No Apêndice C é possível encontrar todos os autores encontrados, com seus respectivos trabalhos publicados nesta área e o ano de publicação.

Quadro 7 - Principais autores, trabalhos publicados e anos de publicação.

Principais autores	Nº de trabalhos publicados	Anos de publicação
Ashan M.	9	2018; 2019; 2020; 2021; 2023
Mashuri M.	8	2018; 2019; 2020; 2021
Khusna H.	7	2018; 2019; 2020; 2021; 2023
Kuswanto H.	6	2018; 2019; 2020; 2021
Prastyo D.	6	2018; 2019; 2020; 2021
Wells L.	6	2014; 2015; 2019; 2020; 2021
Camelio J.	5	2014; 2015; 2019; 2020; 2021
Ye N.	5	2002; 2003; 2007

Elhabshy A.	3	2019; 2020; 2021
Cisar P.	3	2006; 2008; 2010

Autor: Autoria própria (2025).

Foi observado que, conforme preconizado por Lakatos, o autor Ye N. é um dos pioneiros no tema, e se destaca não apenas como autor precursor, mas também como um dos maiores detentores do maior número de citações entre todos os documentos identificados. Seu trabalho de 2002 acumula 152 citações. O autor mais citado é Wells L., com uma obra publicada em 2014, é reconhecido com 164 citações, enquanto em terceiro lugar, aparece um pesquisador previamente não mencionado, Haider, cuja publicação de 2017 conta com 142 citações.

A partir desses achados, é possível inferir que as pesquisas mais citadas possuem uma significativa relevância para o tema, sugerindo que estas são aquelas devem desempenhar um papel mais proeminente no desenvolvimento do assunto. Embora haja outros autores com múltiplas citações, a predominância quantitativa recai sobre os três mencionados anteriormente. Essa constatação aponta para a importância de considerar tais trabalhos como referências fundamentais ao conduzir pesquisas futuras na interface entre ciber-ataques e prevenção/detecção, utilizando as ferramentas da gestão da qualidade.

4.2 MAPEAMENTO CIENTÍFICO NA CIBERSEGURANÇA

O *Text Mining* é uma ferramenta útil para a análise sistemática de grandes volumes de dados textuais, desempenhando um papel relevante na identificação e compreensão de padrões subjacentes em pesquisas científicas. Ao aplicar o *Text Mining*, busca-se não apenas extrair informações relevantes, mas também delinear categorias temáticas que possam ser exploradas mais profundamente. Inicialmente, a partir da leitura dos principais artigos, foi construída uma base de termos e frases comumente utilizadas no programa de pesquisa relacionado ao tema. Aplicando ferramentas de *Text Mining*, com base nesse arquivo de termos e frases, foi identificado o número de ocorrência das mesmas nos artigos extraídos das bases de dados. Utilizou-se a tabela de frequência de termos e frases para fazer a análise Fatorial.

Na presente pesquisa empregou-se o *Text Mining* como uma etapa precursora à análise fatorial, por meio do *software* Statistica, adotando uma abordagem estratégica para desvelar os conteúdos latentes presentes nas publicações relacionadas à cibersegurança, qualidade e ataques cibernéticos. A metodologia de Lakatos fundamenta essa escolha, destacando a importância de uma abordagem sistemática e rigorosa para a pesquisa científica, o que possibilitou uma visão panorâmica das temáticas recorrentes, contribuindo para a identificação preliminar de fatores

que podem influenciar a relação entre cibersegurança e qualidade. Essa fase exploratória, em consonância com as diretrizes lakatosianas, visa fornecer uma base sólida para a posterior compreensão da estrutura das relações entre os elementos em estudo.

Por meio da aplicação da análise fatorial, foi possível identificar quatro fatores que se distribuem em domínios específicos dentro do escopo desta pesquisa. O Fator 1 evidenciou publicações centradas em ataques à manufatura, enquanto o Fator 2 engloba a temática do monitoramento estatístico. As publicações relacionadas ao Fator 3 exploram aspectos da manufatura, e o Fator 4 se dedica à revisão da literatura no contexto da qualidade e cibersegurança. O Quadro 8 fornece uma visão detalhada, apresentando os nomes representativos de cada fator e os termos associados a eles. Esse enfoque, alinhado à perspectiva metodológica de Lakatos, fortalece a fundamentação da pesquisa ao desvelar as inter-relações entre os fatores subjacentes a essas áreas temáticas.

Quadro 8 - Relação entre o nome do fator e os termos dos fatores.

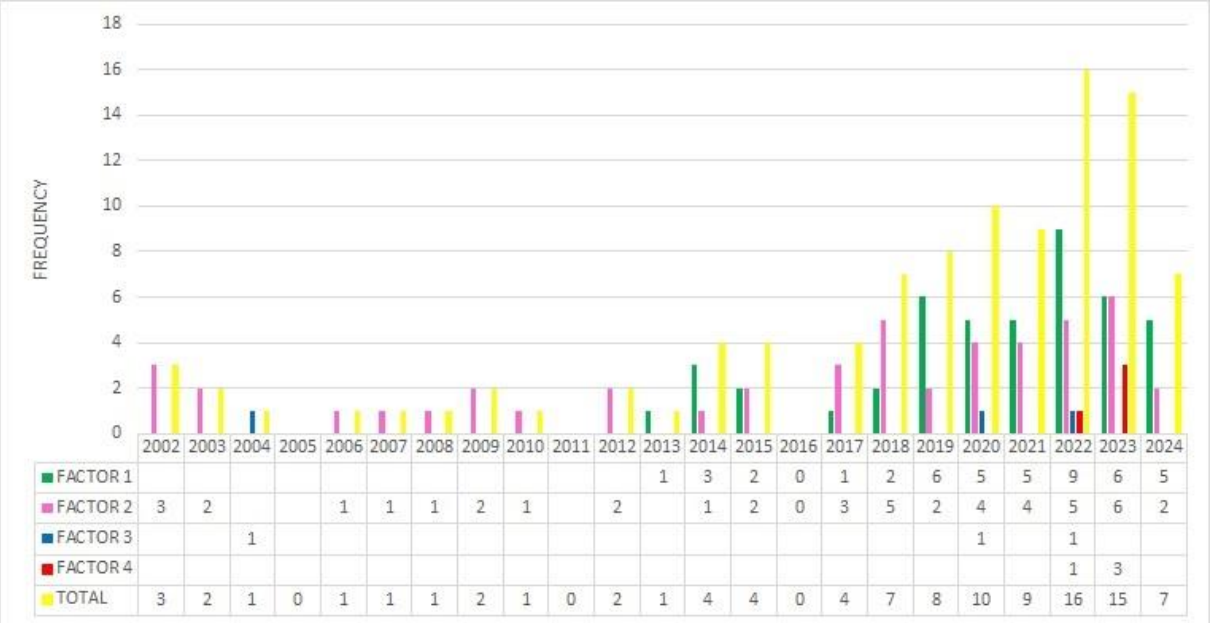
Fator	Nome do fator	Principais termos dos fatores
1	Controle de qualidade, controle de sistemas, melhoria, *machine learning*, vulnerabilidades, fuzzy, riscos	*Attack, cyber-physics, design, manufacturing, products, tools, production, systems*
2	Gráficos de controle: hotelling, CUSUM, EWAM	*Control chart, multivariate, detect, hotelling*
3	Processo de alerta, controle industrial, operacional	*Alert, IDSs, processing, industrial control*
4	Revisão da literatura, medida de desempenho	*Correlation, events, literature, method*

Fonte: Autoria própria (2025).

Também foi feita a classificação da quantidade de artigos por fatores por ano, conforme Gráfico 2. Observa-se que alguns fatores, como o 4, que é o fator de revisão de literatura, surgiu a partir de 2022. Já o Fator 2 sempre esteve presente, ou seja, a temática de gráficos de controle, em específico, tem-se como os gráficos mais utilizados os multivariados, o qui-quadrado, exponencial e o de soma acumulada. Portanto, essas ferramentas da qualidade estão em discussão desde o início dos trabalhos no âmbito de gerenciamento da qualidade e cibersegurança.

O Fator 3 apareceu esporadicamente apenas duas vezes ao longo dos anos e o Fator 1 surgiu a partir do ano de 2013 e manteve-se em alta ao longo dos anos, este fator trata dos processos de controle, voltado para a gestão de riscos dos processos para prevenir a invasão maliciosa. Esse processo é similar ao que ocorreu na manufatura: primeiro as técnicas estatísticas depois a gestão. Dessa forma, nota-se que os fatores de maior importância para esta pesquisa são os Fatores 1 e 2.

Gráfico 2 - Quantidades de publicações separadas por fator e ano.



	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
FACTOR 1												1	3	2	0	1	2	6	5	5	9	6	5
FACTOR 2	3	2			1	1	1	2	1		2		1	2	0	3	5	2	4	4	5	6	2
FACTOR 3			1																1		1		
FACTOR 4																					1	3	
TOTAL	3	2	1	0	1	1	1	2	1	0	2	1	4	4	0	4	7	8	10	9	16	15	7

Fonte: Autoria própria (2025).

A análise de *cluster* é uma estratégia eficaz para consolidar os resultados da análise fatorial. Neste caso, aplicada aos autores e termos-chave de interesse da pesquisa, a análise fatorial permitiu classificar o conjunto de artigos extraídos em temas específicos, relacionando ataques hackers à gestão da qualidade. Tanto a análise fatorial quanto a análise de *cluster* são úteis para estudos exploratórios, que é o objetivo desta pesquisa. Assim, foi realizada uma análise de *cluster* para classificar os artigos de acordo com suas similaridades em termos de conteúdo e cruzou-se esses resultados com as análises fatoriais, proporcionando maior consistência na interpretação dos dados.

Ao cruzar a análise de *cluster* com a análise fatorial, foi identificado que temas como monitoramento estatístico, gráficos de controle e métodos multivariados aplicados na prevenção e detecção de ataques *hackers* estão consolidados em um grupo específico de autores. Por exemplo, o *Cluster* 3 é composto exclusivamente por artigos do Fator 2 (13 artigos), que são caracterizados principalmente pelo uso de estatísticas multivariadas para detectar anomalias do sistema, enquanto o *Cluster* 4 contém apenas artigos do Fator 1 (14 artigos), que focam em temas como aprendizado de máquina, *frameworks* e sistemas de controle. Os *Clusters* 1 e 2 incluem artigos do Fator 1 e do Fator 2: o *Cluster* 1 contém 34 dos 43 artigos do Fator 2, e o *Cluster* 2 contém 24 dos 35 artigos do Fator 1. Isso é explicado pela aleatoriedade na distribuição de palavras entre os artigos, o que afeta a precisão das classificações nas análises de *cluster* e fator.

4.3 COMPARATIVOS DA BIBLIOMETRIA E REVISÃO TEÓRICA

Observa-se que os achados apresentados no texto, referente ao Fator 1, indicam uma gama de temas relacionados à cibersegurança, qualidade e ataques cibernéticos, revelando a complexidade e a interdisciplinaridade inerentes a essa área de pesquisa. A abordagem de Lakatos preconiza a busca por padrões e relações entre variáveis, contribuindo para o desenvolvimento teórico e prático do campo. Em específico, a análise deste fator permitiu observar que a diversidade de temas, como detecção de ataques, segurança em sistemas industriais, qualidade de processos e métodos de prevenção, destaca a amplitude da pesquisa nesse domínio. Nestes artigos, alguns tópicos foram estudados, por exemplo, a aplicação da família ISO série 27000 e do gerenciamento de riscos, e problemas relacionados à qualidade na manufatura. Autores como Ye N., Wells L. e Haider, cujos trabalhos são citados com frequência, emergem como pontos focais na literatura, indicando seu pioneirismo e a possível relevância de suas contribuições para futuras pesquisas.

Temas como "*Total Quality Management in Cyber Security*" e "*Process Control Security Journey*" evidenciam a interseção entre cibersegurança e gestão da qualidade, alinhando-se à perspectiva de Lakatos de explorar relações entre variáveis. Uma taxonomia para identificação e proteção de uma indústria de manufatura conectada foi proposta. Estudos apontam que a análise varia desde a identificação de vulnerabilidades em sistemas cibernéticos até o desenvolvimento de estratégias para prevenção e detecção de ataques, por meio de ferramentas, técnicas e abordagens da qualidade, refletindo um compromisso com a aplicabilidade prática dos resultados.

Temas como "*Multisensorial Self-Learning Systems for Quality Monitoring*" e "*Simulating Cyber-Physical Systems*" destacam a importância de perspectivas multidisciplinares, convergindo aspectos de sensoriamento, aprendizado de máquina e simulação. A presença de trabalhos que abordam desafios específicos, como "*Trojan Detection and Side-channel Analyses*" e "*Security Risk Analysis of Active Distribution Networks*", sugerem uma abordagem sistemática para compreender e enfrentar os desafios na cibersegurança. A introdução de estratégias como "CRSTIP" (*Compliance, Risk Assessment, and Security Testing Improvement Profiling*) e "*Optimizing Security and Quality of Service*" reflete o enfoque na eficiência e no controle de qualidade.

Observando o Fator 2, a análise dos resultados revela uma diversidade de temas e métodos para enriquecer o conhecimento científico sobre o tema. Verificou-se que os resultados

apresentam uma variedade de temas, desde a aplicação de técnicas estatísticas clássicas (como gráficos CUSUM e Hotelling T^2) até a integração de *machine learning* e algoritmos genéticos. Outro ponto é que a detecção de ataques cibernéticos é abordada como uma solução prática e relevante para os ataques *hacker*. Cada técnica ou abordagem identificada na literatura oferece soluções eficientes e eficazes para enfrentar desafios específicos. Várias abordagens destacam a eficiência, rapidez e adaptação a cenários dinâmicos dos ataques ciberneticos. Essa ênfase na eficácia e adaptabilidade das técnicas valoriza pesquisas que buscam aplicação prática e resultados úteis.

A integração de gráficos de controle com a Análise de Fourier representa uma abordagem inovadora para identificar padrões temporais em dados coletados de sistemas ciber-físicos. Aplicando a Transformação de Fourier para decompor esses sinais de dados em seus componentes de frequência, os pesquisadores podem identificar padrões repetitivos ou anomalias periódicas. Isso é particularmente valioso ao monitorar sistemas ciber-físicos, pois permite a detecção de problemas como ataques de negação de serviço (DDoS), que frequentemente se manifestam como padrões de tráfego de rede anormais. Posteriormente, gráficos de controle como o Hotelling T^2 podem ser empregados para monitorar essas frequências ao longo do tempo, oferecendo um método robusto para detecção precoce e resposta a potenciais ameaças.

De maneira geral, gráficos de controle como o Hotelling T^2 e o EWMA podem ser empregados como sistemas de detecção de intrusão (IDS) em cibersegurança, monitorando continuamente o comportamento de variáveis em sistemas de produção. Eles operam identificando padrões operacionais normais e estabelecendo limites de controle com base em dados históricos. O gráfico de Hotelling T^2 é aplicado para monitorar múltiplas variáveis simultaneamente, analisando combinações de dados (por exemplo, tempo de resposta e uso de memória) para detectar anomalias. Se um ponto no gráfico exceder os limites de controle, pode indicar um possível ataque ou comportamento anômalo. O gráfico EWMA é particularmente útil para detectar mudanças graduais nos padrões de comportamento, como a presença de *malware* que altera lentamente os acessos ao sistema. Ao suavizar os dados ao longo do tempo, é eficaz na identificação de tendências antes que elas se transformem em ameaças significativas.

Além disso, aplicando ferramentas de gestão da qualidade, como gráficos de controle, combinadas com técnicas de aprendizado de máquina, as empresas podem aprimorar a segurança ao mesmo tempo que melhoram a eficiência operacional.

As indústrias estão reconhecendo o problema e mostrando cada vez mais interesse em proteger seus sistemas conectados. A busca por inovação e integração de métodos é intrínseca

para o avanço científico. Dessa forma, foram identificadas pesquisas inovadoras que utilizam, por exemplo, a aplicação de *Bayesian Inference Criterion* (BIC) e abordagens não paramétricas. A adaptação das técnicas a contextos emergentes, como *Internet of Things* (IoT), cidades inteligentes e redes sociais, demonstrou a capacidade desse campo de pesquisa em se adaptar a novos desafios e ambientes, o que está em consonância com a visão de Lakatos sobre a evolução da pesquisa científica.

4.4 RESPOSTAS ÀS PERGUNTAS E HIPÓTESES

O Quadro 9 apresenta a que Fator da bibliometria estão associados as perguntas e hipóteses levantadas no Capítulo 2 deste trabalho. Observa-se que as perguntas estão relacionadas aos Fatores 1 e 2 da bibliometria, que foram identificados como pontos focais na revisão bibliográfica, reforçando que o trabalho converge para temas de gerenciamento, controle, riscos, vulnerabilidades para prevenção de ciberataques e técnicas de detecção de intrusão inovadoras, como gráficos de controle associados a técnicas de *machine learning*.

Quadro 9 - Fatores relacionados as perguntas e hipóteses

Perguntas	Hipóteses	Fator
P1: Os guias e métodos para classificação de risco indicados na ISO série 27002 de fato são aplicados e contribuem para segurança de CPS? (Seção 2.2.1)	H1: A ISO 27000 apoia os CPS H2: Os guias e métodos de classificação de risco da ISO 27002 têm contribuído para cibersegurança.	1
P2: Qual o tipo de ataque mais comum e com que frequência ocorrem? (Seção 2.2.2)	H3: Há ataques de maior frequência que precisam ser priorizados.	2
P3: Técnicas estatísticas de monitoramento de processo (CEP) podem ser utilizadas na detecção e prevenção de ataques *hacker*? (Seção 2.3.1)	H4: As técnicas estatísticas de monitoramento são aplicáveis para prevenção e detecção de ataques *hacker*.	2
P4: *Framework*, como o MITRE ATT&CK e demais diretrizes, como ferramentas de monitoramento atualização de sistemas, auditorias contribuem de fato para a prevenção e detecção de ciberataques? (Seção 2.2.2)	H5: há evidência de que o *framework* e demais diretrizes, como ferramentas de monitoramento atualização de sistemas, auditorias contribuem para prevenção e detecção de ciberataques.	1
P5: As Legislações brasileiras atuais contribuem para fortalecer os sistemas de cibersegurança das organizações? (Seção 2.2.3)	H6: O Brasil possui legislação sobre cibersegurança, porém pouco efetiva.	Não se aplica
P6: O SGQ contribui para a cibersegurança e de que forma que a falta desta pode impactar negativamente os sistemas de cibersegurança? (Seção 2.3)	H7: Há evidência de que atualmente o SGQ tenha contribuído para a cibersegurança.	1
P7: Há gargalos e desafios (falta de conhecimento) para aplicação de métodos estatísticos na área de cibersecurança?	H8: Há gargalos e desafios significativos que inibem a adoção de técnicas estatísticas em sistemas de cibersegurança.	2

(Seção 2.3.1)		
P8: Os profissionais da área conhecem as técnicas para detecção de ataques e as utilizam com qual frequência? Os profissionais da área utilizam o *machine learning*? (Seção 2.3.1)	H9: As técnicas não são usadas com mais frequência do que outras.	2
P9: Os princípios da qualidade, como os da família ISO 9000, influenciam a gestão de sistemas de cibersegurança nas organizações para prevenção de ataques? (Seção 2.3.2)	H10: Os princípios da qualidade, como os da família ISO 9000, podem colaborar na área de cibersegurança para prevenção de ciberataques.	1
P10: Qual o nível de criticidade dos desafios enfrentados pelas organizações para melhorar continuamente seus sistemas de proteção contra ataques? (Seção 2.3.2)	H11: Existem desafios para a melhoria contínua em que o grau de criticidade sobressai em relação a outros.	1

Fonte: Autoria própria (2025)

A P5 não está relacionada a nenhum fator da revisão bibliográfica e isso se dá ao fato de que em nenhum trabalho foi observado o tema de legislações brasileiras, sugerindo que tal assunto seja aprofundado na pesquisa de campo com especialistas.

5 RESULTADOS DA PESQUISA DE CAMPO COM ESPECIALISTAS

A pesquisa de campo com especialista foi realizada com o propósito de confirmar ou não o que foi encontrado na revisão bibliográfica, com o foco em atingir os objetivos específicos ii) e iii) do presente trabalho.

Para isso, neste capítulo será apresentado a análise dos dados (5.1), composta pela caracterização geral dos respondentes, pela análise descritiva dos dados coletados e os resultados dos testes estatísticos da pesquisa de campo (5.1). Também será apresentado os principais achados da pesquisa de campo (5.2). Com isso será possível entender a percepção dos especialistas sobre a integração entre os sistemas de gestão da qualidade e cibersegurança, fortalecendo as organizações contra os ataques *hacker*, principalmente, aqueles que cruzam a fronteira do mundo virtual e afetam os ambientes produtivos de manufatura.

5.1 ANÁLISE DOS DADOS

O Quadro 10 descreve o cargo em que os respondentes ocupam atualmente. Nota-se que existem cinco respondentes que atuam como especialistas nas organizações, sendo o cargo mais presente, seguido por analistas e engenheiros.

Quadro 10 – Cargos dos especialistas

Cargo	Frequência
Especialista	5
Analista Sênior	2
Engenheiro de Segurança	2
Analista de Segurança da Informação	2
Consultor em Segurança da Informação	1
CEO	1
Threat hunting Analyst	1
Engenheiro Sênior	1
Consultor de Cibersegurança	1
Empreendedor	1
Técnico	1
Coordenador	1
Coordenador de Segurança da Informação	1
Gerente Sênior de Cibersegurança	1
Analista	1
Líder Técnico	1
Estudante de Cibersegurança	1
Analista de Operações de Segurança	1
Gerente de Segurança Cibernética	1
Assessor Especial	1
TOTAL	27

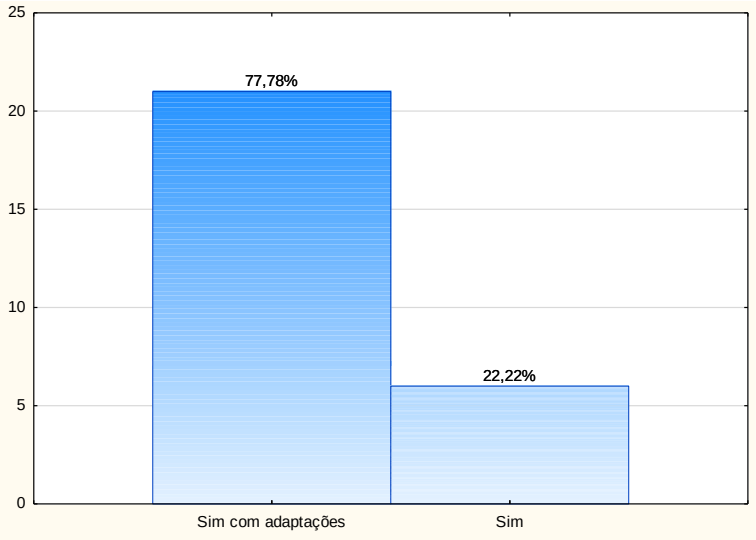
Fonte: Autoria própria (2025)

Os respondentes atuam em diversos seguimentos, como as próprias empresas de tecnologia, tecnologia da informação, consultoria em tecnologia, no setor público, no setor bancário, na área da educação, manufatura, setor petrolífero, e-*commerce* e mobilidade.

Além disso, eles se conectam de diversas formas com a cibersegurança, tanto no ramo público quanto privado, desde o tempo de atuação no mercado, dando destaque aos consultores de cibersegurança que se encontram há mais de dez anos neste ramo, quanto a atuações em mercados externos, como o gerente sênior de cibersegurança, que atua na América Latina.

Para a P1 do Quadro 6, que tratava sobre a aplicação da ISO 27000, os especialistas responderam em sua maioria (77,78%) que a família ISO 27000 funcionaria bem se houver adaptações, conforme Gráfico 3. Os demais respondentes (22,22%) percebem que esta norma já funciona bem para os sistemas produtivos de manufatura. Os especialistas observaram que é necessário necessidades específicas de cada segmento, tanto tecnologia da informação (TI), quanto tecnologia operacional (OT).

Gráfico 3 – Pareto para ISO 27000



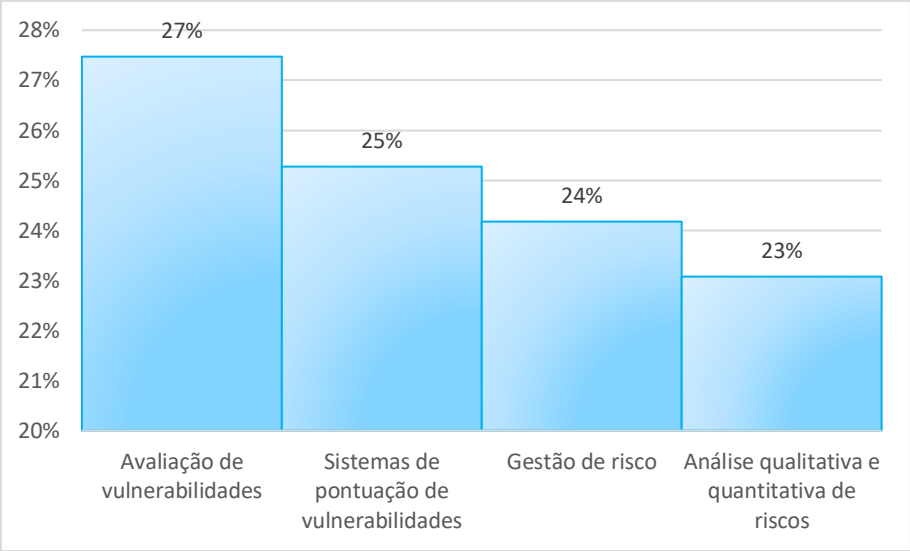
Fonte: Autoria própria (2025)

Em geral, os respondentes explicaram que essa certificação garante que a organização possui processos e políticas de segurança, mas falha em garantir que são estes são seguidos sempre, já que ela não busca evidências, funciona apenas como um guia. Muitos controles cobrados pela família 27000 são rasos e as empresas implementam apenas para fins de auditoria, não possuindo um real impacto na segurança.

No que tange a classificação de risco, tema abordado na norma ISO 27002, os especialistas responderam quanto a aplicação de métodos para prevenção e identificação de ciberataques, conforme a experiência deles. O Gráfico 4 apresenta colunas comparativas entre a quantia de especialistas que já aplicaram ou não os métodos para prevenção e identificação de ciberataques.

Com este gráfico notou-se que o método mais utilizado pelos especialistas para prevenção e identificação de ciberataques é a avaliação de vulnerabilidades. O menos utilizado é a análise qualitativa e quantitativa de riscos.

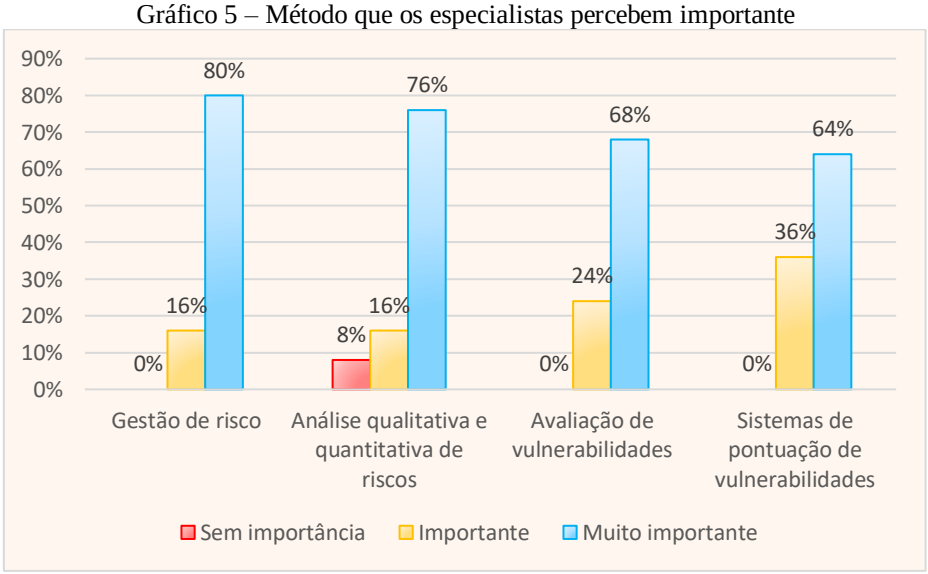
Gráfico 4 – Comparativo entre as aplicações de métodos para classificação de risco



Fonte: Autoria própria (2025)

Os respondentes também apontaram suas percepções acercas desses métodos, revelando o grau de importância que eles enxergam tais métodos, conforme Gráfico 5.

Gráfico 5 – Método que os especialistas percebem importante



Fonte: Autoria própria (2025)

Embora os especialistas apliquem mais a avaliação de vulnerabilidades, eles enxergam a gestão de riscos como o método mais eficiente para prevenção e identificação de ciberataques. Seguido pela análise qualitativa e quantitativa dos riscos, que foi vista como a menos aplicada por eles. Nota-se que três dos quatro os métodos listados possuem alguma importância para os especialistas, revelando que as soluções para proteção dos sistemas de cibersegurança depende e atua com várias frentes.

Tabela 1 – Frequência de enfrentamento observada dos ciberataques

TABELA OBSERVADA	*Phishing* e suas variações	*Ramsonware*	DoS/DDoS	Quebra de senhas	TOTAL
MUITO FREQUENTE	25	6	14	11	56
POUCO FREQUENTE	2	16	13	15	46
NENHUM	0	5	0	1	6
TOTAL	27	27	27	27	108

Fonte: Autoria própria (2025)

A Tabela 1 apresenta a frequência de enfrentamento dos ataques cibernéticos identificados no Capítulo 2 deste trabalho pelos especialistas, referentes a P2 do Quadro 6. As hipóteses testadas para responder essa pergunta são:

H_0: Os ataques ocorrem igualmente em frequência.

H_1: Os ataques não ocorrem em igual frequência.

A Tabela 2 revela a frequência esperada para os dados coletados, calculada a partir da metodologia proposta no capítulo 3. O teste estatístico revelou que o valor calculado do X^2 = 36,06 para um nível de significância de 5% com 6 graus de liberdade e o p-*value* = 2,684e-06. Dessa forma, rejeita-se H_0.

Tabela 2 – Frequência de enfrentamento esperada dos ciberataques

TABELA ESPERADA	*Phishing* e suas variações	*Ramsonware*	DoS/DDoS	Quebra de senhas	TOTAL
MUITO FREQUENTE	14,0	14,0	14,0	14,0	102,0
POUCO FREQUENTE	11,5	11,5	11,5	11,5	52,0
NENHUM	1,5	1,5	1,5	1,5	114,0
TOTAL	27,0	27,0	27,0	27,0	108,0

Fonte: Autoria própria (2025)

Olhando a Tabela 3 é possível ver que o qui-quadrado do *phishing* e suas variações é o que mais se difere dos outros. Sendo seus valores bem altos em “muito frequente” e “pouco frequente”. Revelando que a significância está neste ponto, ou seja, esse é o tipo de ataque que mais ocorre. O ataque que os especialistas lidam com pouca frequência é *ramsomware*, e não lidam são os ataques do tipo DoS/DDoS e quebra de senhas.

Tabela 3 – Cálculo do X^2 para frequência de enfrentamento dos ciberataques

X^2 calculado	*Phishing* e suas variações	*Ramsonware*	DoS/DDoS	Quebra de senhas	TOTAL
MUITO FREQUENTE	8,6429	4,5714	0,0000	0,6429	13,8571
POUCO FREQUENTE	7,8478	1,7609	0,1957	1,0652	10,8696

NENHUM	1,5000	8,1667	1,5000	0,1667	11,3333
TOTAL	17,9907	14,4990	1,6957	1,8747	36,0600

Fonte: Autoria própria (2025)

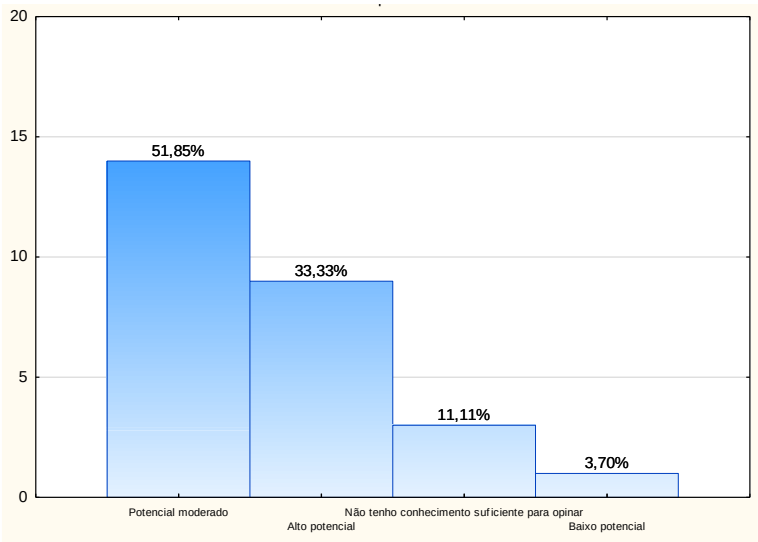
Essa informação é muito relevante, pois entendendo os principais tipos de ataques é possível começar a pensar em soluções, tanto técnicas quanto gerenciais, temas presentes nos Fatores 1 e 2 da revisão biliométrica deste trabalho.

Vale relembrar que o *phishing* é um tipo de ataque que envolve completamente o usuário. Neste os adversários usam técnicas de engenharia social para induzir as vítimas a confiarem neles, portanto, torna-se necessário pensar em medidas que os usuários podem ter para prevenir esse tipo de ataque.

Os especialistas apontam que, neste caso, o comportamento do usuário é crítico e que fazer a capacitação dos usuários dos sistemas colabora para a prevenção de ataques, além disso, enfatizam que promover uma cultura voltada para a segurança também colabora para prevenção de ataques como um todo.

Para responder a P3 do Quadro 6, o Gráfico 6 revela que 51,85% dos especialistas acreditam que o CEP tem potencial moderado. 33,33% acredita que existe um alto potencial. 11,11% não tem conhecimento o suficiente para opinar, e 3,70% acredita que tem baixo potencial.

Gráfico 6 – Potencial do CEP



Fonte: Autoria própria (2025)

A revisão bibliométrica apontou pesquisas que tratavam do CEP como sistemas de detecção de intrusões, dando origem ao Fator 2. A percepção dos especialistas se torna muito relevante neste tema, pois revela que os profissionais da área de cibersegurança acreditam que

existe potencial moderado e alto para a sustentabilidade dos sistemas de cibersegurança, confirmando uma potencial área de estudo a ser explorada.

A Tabela 4 indica a frequência observada da percepção dos especialistas em relação as diretrizes para prevenção de ciberataques, referentes à P4 do Quadro 6. Por exemplo, 19 especialistas percebem que a diretriz "Implementação de *frameworks* e garantia de conformidade com normas e regulamentações de segurança" apoia totalmente a prevenção de ciberataques; 8 especialistas acreditam que essa medida apoia parcialmente. O mesmo raciocínio para as demais medidas.

Tabela 4 – Frequência observada para diretrizes de prevenção de ciberataques

TABELA OBSERVADA	Implementação de *frameworks* e garantia de conformidade com normas e regulamentaçõe s de segurança	Uso de ferramentas de monitoramento contínuo e inteligência artificial para detecção de ameaças	Atualização constante de sistemas e ferramentas de segurança	Realização de testes e auditorias regulares para identificar vulnerabilidades	TOTAL
TOTALMENTE	19	22	25	23	89
PARCIALMENTE	8	5	2	4	19
TOTAL	27	27	27	27	108

Fonte: Autoria própria (2025)

Neste caso, as hipóteses a serem testadas para responder a P4 do questionário são:

H_0: *Frameworks* e demais diretrizes, como ferramentas de monitoramento atualização de sistemas, auditorias não contribuem para prevenção e detecção de ciberataques.

H_1: *Frameworks* e demais diretrizes, como ferramentas de monitoramento atualização de sistemas, auditorias contribuem para prevenção e detecção de ciberataques.

Tabela 5 – Frequência esperada para diretrizes de prevenção de ciberataques

TABELA ESPERADA	Implementação de *frameworks* e garantia de conformidade com normas e regulamentaçõe s de segurança	Uso de ferramentas de monitoramento contínuo e inteligência artificial para detecção de ameaças	Atualização constante de sistemas e ferramentas de segurança	Realização de testes e auditorias regulares para identificar vulnerabilidades	TOTAL
TOTALMENTE	22,25	22,25	22,25	22,25	89,00
PARCIALMENTE	4,75	4,75	4,75	4,75	19,00
TOTAL	27,00	27,00	27,00	27,00	108,00

Fonte: Autoria própria (2025)

Já a Tabela 5 mostra a frequência esperada para esta pergunta. As diretrizes dessa questão eram relacionadas aos Fatores 1 e 2 encontrados na revisão bibliométrica, pois abordam

tópicos na área de controles, vulnerabilidades e na parte de técnicas de monitoramento. Observando Tabela 4 nota-se que a frequência de “totalmente” é bem maior que a frequência de “parcialmente” e que a frequência de alternativas “nenhum” foi zero. Tal observação confirma que as áreas de cibersegurança e qualidade estão entrelaçadas.

Para efeitos de cálculo, foi utilizada uma técnica estatística chamada *boostrap* visando ampliar a amostra e melhor observar e interpretar os dados observados. Aplicando o teste qui-quadrado no R, com α = 5%, obteve-se que o valor calculado do X^2 = 4,7901 com 3 graus de liberdade, e o p-*value* = 0,1878. Portanto, não se rejeita H_0.

Tabela 6 – Cálculo do X^2 para diretrizes de prevenção de ciberataques

X^2 calculado	Implementação de *frameworks* e garantia de conformidade com normas e regulamentaçõe s de segurança	Uso de ferramentas de monitoramento contínuo e inteligência artificial para detecção de ameaças	Atualização constante de sistemas e ferramentas de segurança	Realização de testes e auditorias regulares para identificar vulnerabilidades	TOTAL
TOTALMENTE	0,4747	0,0028	0,3399	0,0253	0,8427
PARCIALMENTE	2,2237	0,0132	1,5921	0,1184	3,9474
TOTAL	2,6984	0,0160	1,9320	0,1437	4,7901

Fonte: Autoria própria (2025)

Entretanto, observa-se na Tabela 6 que o qui-quadrado da segunda linha e das colunas “Implementação de *frameworks* e garantia de conformidade com normas e regulamentações de segurança” e “Atualização constante de sistemas e ferramentas de segurança” é bem mais alto em relação aos demais, mostrando que essas medidas são as causas da significância estatística. Portanto, confirma-se que há diferença entre as colunas e as linhas, e as frequências destacadas são maiores para essa linha.

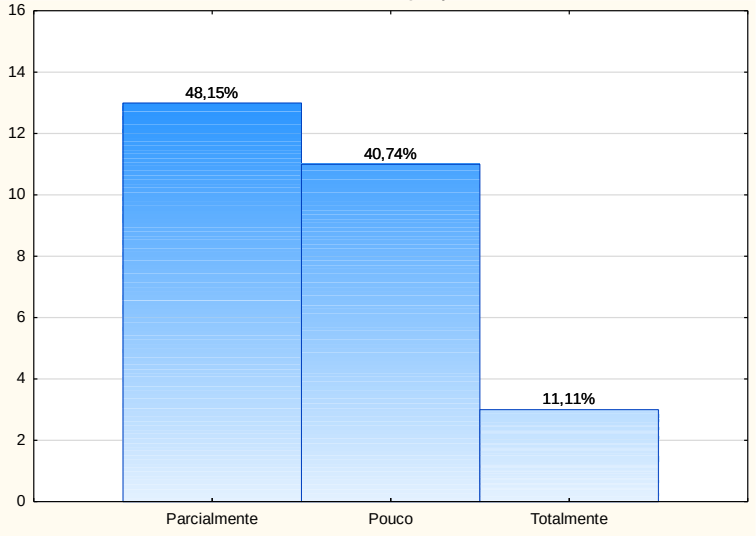
Além do mais, pode mostrar que *frameworks* são medidas aderidas pelas organizações na área de cibersegurança, contudo, ainda não são habituais, enquanto que a atualização de sistemas e ferramentas de segurança já é uma medida muito presente e que colabora positivamente para a cibersegurança.

Em relação a P5, observou-se que, 48,15% dos especialistas percebem que a legislação brasileira contribui parcialmente para fortalecer os sistemas de cibersegurança; 40,74% acredita que contribui pouco e 11,11% acredita que contribui totalmente, mostra o Gráfico 7.

Tais resultados refletem ainda a necessidade de se ter legislações mais robustas e de estudos que aprofundem o tópico. Os especialistas comentaram que as leis de cibsergurança no

Brasil são primárias ainda e precisam de revisão para que se tenha um combate poderoso frente aos ataques *hackers*.

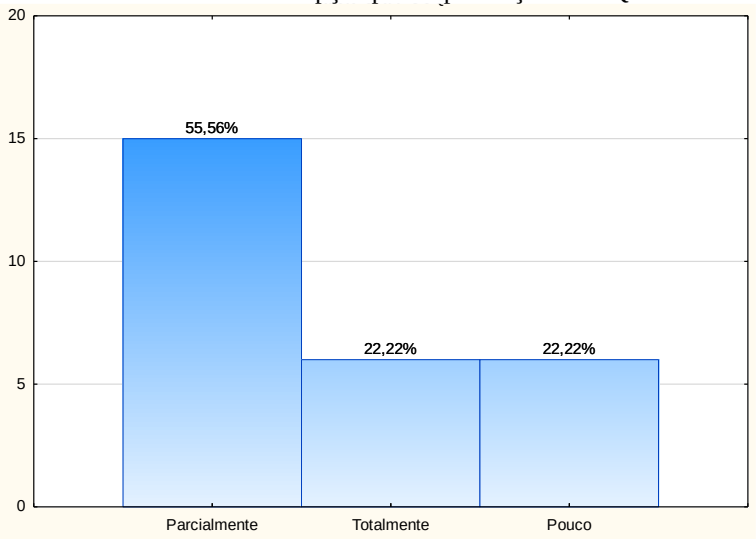
Gráfico 7 – Percepção sobre a legislação brasileira



Fonte: Autoria própria (2025)

Para responder a P6 do Quadro 6, os especialistas responderam sobre suas percepções do impacto da presença e ausência de um SGQ na área de cibersegurança. A partir do Gráfico 8, foi visto que 55,56% dos especialistas afirmam que os SGQ contribuem parcialmente para o gerenciamento da cibersegurança e que, 22,22%, aproximadamente, percebem que os SGQ contribuem totalmente para o gerenciamento da cibersegurança e 22,22% acredita que os SGQ contribuem pouco.

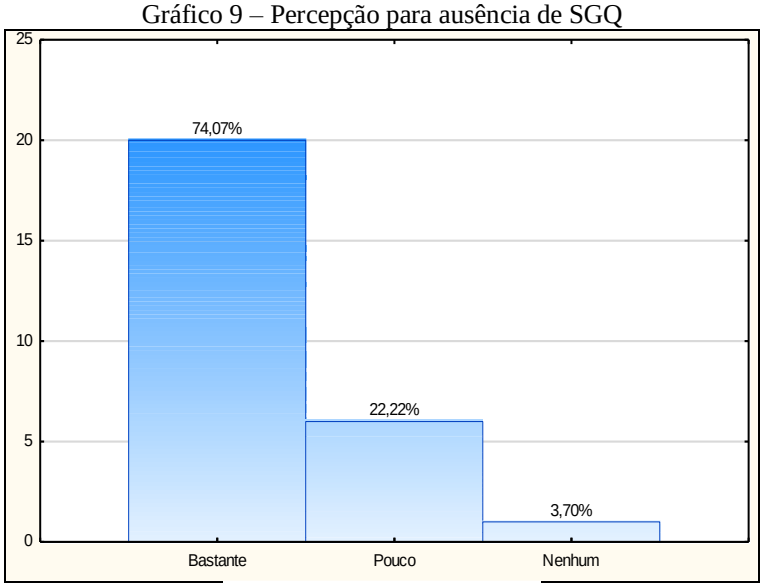
Gráfico 8 – Percepção para a presença de SGQ



Fonte: Autoria própria (2025)

Em contrapartida, observando o Gráfico 9, nota-se que 74,07% dos especialistas percebem que a ausência de um SGQ afeta bastante a gestão da cibersegurança. 22,22% dos especialistas percebem que a ausência de um SGQ afeta pouco a gestão da cibersegurança e, aproximadamente 3,7% dos especialistas percebem que a ausência de um SGQ não afeta a gestão da cibersegurança.

Gráfico 9 – Percepção para ausência de SGQ



Fonte: Autoria própria (2025)

A Tabela 7 mostra a frequência com que os especialistas percebem a intensidade dos desafios enfrentados na aplicação de métodos e técnicas estatísticas na área de cibersegurança, tema relacionado à P7. Para responder a essa pergunta, foram testadas as hipóteses:

H_0: Os gargalos e desafios não são significativos para a adoção de técnicas estatísticas pelos especialistas.

H_1: Os gargalos e desafios são significativos para a adoção de técnicas estatísticas pelos especialistas.

Tabela 7 – Frequência observada dos desafios na aplicação de métodos estatísticos

TABELA OBSERVADA	Desconhe-cimento sobre o tema	Coleta e tratamento de grandes volumes de dados em tempo real	Complexi-dade na interpreta-ção de resultados estatísticos	Complexi-dade na integração de métodos estatísticos com sistemas de segurança já existentes	Alta taxa de falsos positivos e negativos nos modelos de detecção	Adaptação dos modelos estatísticos a novos tipos de ataques e padrões de comportam ento	TOTAL
POUCO DESAFIADOR	5	7	3	2	4	3	24

DESAFIADOR	5	9	14	15	7	10	60
MUITO DESAFIADOR	17	11	10	10	16	14	78
TOTAL	27	27	27	27	27	27	162

Fonte: Autoria própria (2025)

A partir dos dados observados foi calculado a Tabela 8 que apresenta as frequências esperadas para poder então ser aplicado o teste qui-quadrado. O tópico desta questão se torna bastante relevante, ao passo que os métodos estatísticos vêm sendo bastante citados ao longo deste trabalho como uma forma de detectar ciberataques, por exemplo, o Fator 2 da revisão bibliométrica tem como tema principal os gráficos de controle.

Tabela 8 – Frequência esperada dos desafios na aplicação de métodos estatísticos

TABELA ESPERADA	Desconhe-cimento sobre o tema	Coleta e tratamento de grandes volumes de dados em tempo real	Complexi-dade na interpreta-ção de resultados estatísticos	Complexi-dade na integração de métodos estatísticos com sistemas de segurança já existentes	Alta taxa de falsos positivos e negativos nos modelos de detecção	Adaptação dos modelos estatísticos a novos tipos de ataques e padrões de comportam ento	TOTAL
POUCO DESAFIADOR	4	4	4	4	4	4	24
DESAFIADOR	10	10	10	10	10	10	60
MUITO DESAFIADOR	13	13	13	13	13	13	78
TOTAL	27	27	27	27	27	27	162

Fonte: Autoria própria (2025)

Diante disso, ao testar H_0 a um nível de significância (α) de 5% e 10 graus de liberdade, encontra-se X^2 = 15,2923 e o p-*value* = 0,1218. Portanto, não existem evidências científicas o suficiente para se rejeitar H_0. A Tabela 9 apresenta os valores dos qui-quadrados para cada desafio e seu grau de intensidade.

Tabela 9 – Cálculo do X^2 para os desafios na aplicação de métodos estatísticos

X^2 calculado	Desconhe-cimento sobre o tema	Coleta e tratamento de grandes volumes de dados em tempo real	Complexi-dade na interpreta-ção de resultados estatísticos	Complexi-dade na integração de métodos estatísticos com sistemas de segurança já existentes	Alta taxa de falsos positivos e negativos nos modelos de detecção	Adaptação dos modelos estatísticos a novos tipos de ataques e padrões de comportam ento	TOTAL
POUCO DESAFIADOR	0,2500	2,2500	0,2500	1,0000	0,0000	0,2500	4,0000

DESAFIADOR	2,5000	0,1000	1,6000	2,5000	0,9000	0,0000	7,6000
MUITO DESAFIADOR	1,2308	0,3077	0,6923	0,6923	0,6923	0,0769	3,6923
TOTAL	3,9808	2,6577	2,5423	4,1923	1,5923	0,3269	15,2923

Fonte: Autoria própria (2025)

Foi aplicado a técnica do *bootstrap* para encontrar a maior significância nos dados observados, e notou-se que a maior parte dos especialistas percebem o desconhecimento sobre o tema como "desafiador" e "muito desafiador", tornando este um ponto chave quando se pensa em desenvolver novos métodos de detecção de intrusão, impactando em aspectos do Fator 2 da revisão bibliométrica. Os especialistas também consideram "desafiador" a complexidade na integração dos métodos estatísticos com sistemas de segurança já existentes e, a complexidade na interpretação dos resultados estatísticos. Em contrapartida, os especialistas consideram "pouco desafiador" a coleta e tratamento de grandes volumes de dados em tempo real.

Para verificar como os especialistas enxergam as relações entre as técnicas de detecção de ataques e as soluções existentes que podem auxiliar na sua aplicação para detectar ciberataques foi aplicado o teste estatístico na tabela cruzada, conforme P8 do Quadro 6. Os dados da Tabela 10 podem ser interpretados da seguinte forma, por exemplo, para a solução "Detecção do comportamento anômalo" houve 30 votos para a técnica de "Métodos Estatísticos Multivariados". Para a mesma solução, houve 32 votos para "Modelos de *Machine Learning*", 24 para "Modelos de *Deep Learning*", 30 para "Inteligência Artificial", 22 para "Modelos de Redes Neurais" e 16 para "Controle Estatístico do Processo".

Tabela 10 - Técnicas e soluções práticas para a detecção de ciberataques observada

MATRIZ OBSERVADA	Métodos Estatísticos Multivariados	Modelos de *Machine Learning*	Modelos de *Deep Learning*	Inteligência Artifical	Modelos de Redes Neurais	Controle Estatístico do Processo	TOTAL
Detecção de comportamento anômalo	15	16	12	15	11	8	77
Antivírus	5	17	8	18	8	7	63
Ferramentas de monitoramento de logs e eventos	8	14	13	20	9	12	76
Firewall	6	16	14	16	8	7	67
Sistemas de autenticação multifatorial (MFA)	10	13	9	12	8	12	64
TOTAL	44	76	56	81	44	46	347

Fonte: Autoria própria (2025)

Com essa tabela cruzada, foi possível verificar se todas as metodologias são usadas com igual frequência para detectar ataques, por meio das hipóteses:

H_0: As técnicas de detecção são usadas em frequências iguais.

H_1: As técnicas de detecção de ataques são usadas em frequências diferentes.

Para realizar o teste, inicialmente calculou-se a matriz esperada, conforme Tabela 11.

Tabela 11 – Técnicas e soluções práticas para a detecção de ciberataques esperada

MATRIZ ESPERADA	Métodos Estatísticos Multivariados	Modelos de *Machine Learning*	Modelos de *Deep Learning*	Inteligência Artifical	Modelos de Redes Neurais	Controle Estatístico do Processo	TOTAL
Detecção de comportamento anômalo	9,7637	16,8646	12,4265	17,9741	9,7637	10,2075	77,0000
Antivírus	7,9885	13,7983	10,1671	14,7061	7,9885	8,3516	63,0000
Ferramentas de monitoramento de logs e eventos	9,6369	16,6455	12,2651	17,7406	9,6369	10,0749	76,0000
Firewall	8,4957	14,6744	10,8127	15,6398	8,4957	8,8818	67,0000
Sistemas de autenticação multifatorial (MFA)	8,1153	14,0173	10,3285	14,9395	8,1153	8,4841	64,0000
TOTAL	44,0000	76,0000	56,0000	81,0000	44,0000	46,0000	347,0000

Fonte: Autoria própria (2025)

Aplicando o teste qui-quadrado no R, com α = 5%, obteve-se que o valor calculado do X^2 = 13,661 com 20 graus de liberdade, e o p-*value* = 0,8473. Portanto, não existem evidências suficientes para rejeitar H_0 , ou seja, aceita-se que as técnicas são usadas em igual frequência pelos especialistas.

Tabela 12 – Cálculo do X^2 das técnicas e soluções para a detecção de ciberataques

X^2 calculado	Métodos Estatísticos Multivariados	Modelos de *Machine Learning*	Modelos de *Deep Learning*	Inteligência Artifical	Modelos de Redes Neurais	Controle Estatístico do Processo	TOTAL
Detecção de comportamento anômalo	2,8083	0,0443	0,0146	0,4921	0,1565	0,4774	3,9933
Antivírus	1,1180	0,7429	0,4619	0,7378	0,0000	0,2187	3,2794
Ferramentas de monitoramento de logs e eventos	0,2780	0,4205	0,0440	0,2877	0,0421	0,3678	1,4402
Firewall	0,7331	0,1198	0,9395	0,0083	0,0289	0,3987	2,2284
Sistemas de autenticação	0,4377	0,0738	0,1709	0,5784	0,0016	1,4570	2,7194

multifatorial (MFA)							
TOTAL	5,3751	1,4013	1,6310	2,1043	0,2292	2,9197	13,6606

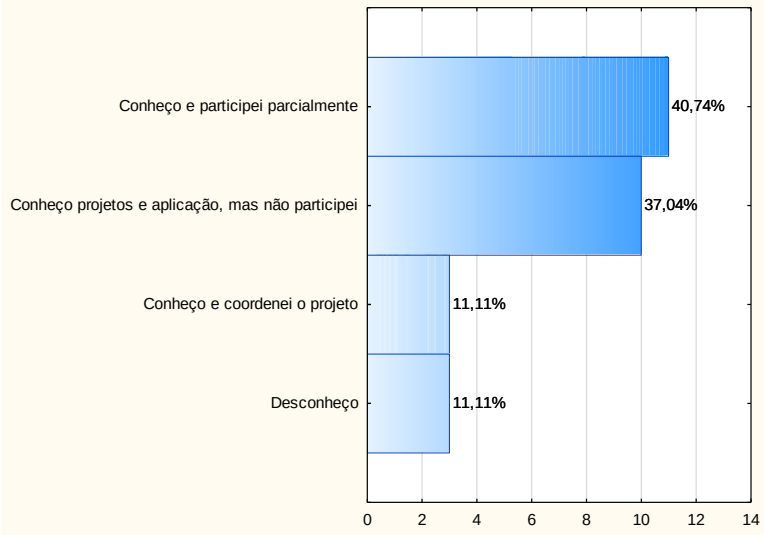
Fonte: Autoria própria (2025)

Contudo, ao aplicar a técnica de *bootstrap* nos dados, com o propósito de ampliar a significância destes, nota-se que uma técnica bastante utilizada pelos especialistas para a detecção do comportamento anômalo são os métodos estatísticos multivariados. Tal técnica também é significativa para o antivírus. O controle estatístico do processo é uma técnica significativa para as soluções em sistemas de autenticação multifatorial, conforme está destacado na Tabela 12.

Tais técnicas também apareceram na revisão bibliométrica, especialmente, no Fator 2, senão como fonte de pesquisa, mas como oportunidades de trabalhos futuros. Ao associar tal conhecimento com a percepção dos especialistas, nota-se que tais técnicas podem colaborar para que os sistemas de proteção contra ataques *hacker* seja mais robusto.

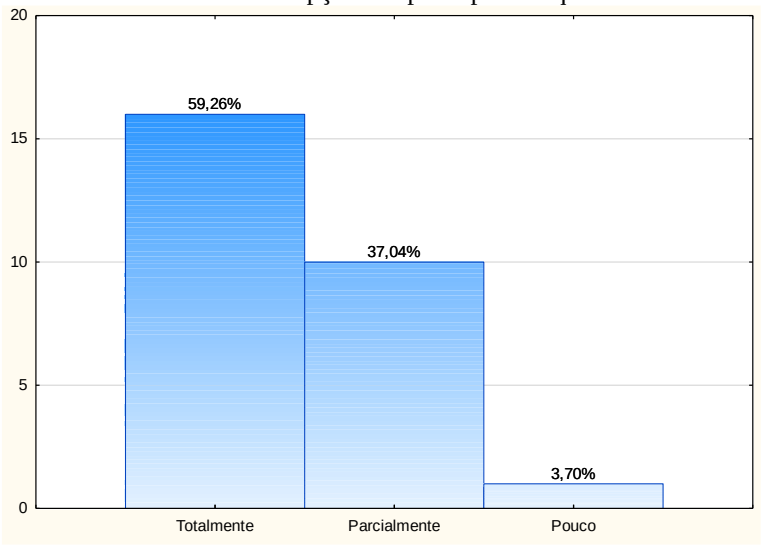
Ainda sobre essa temática, o Capítulo 2 apontou modelos de *machine learning* como uma solução viável para prevenir e identificar ciberataques, e a revisão bibliométrica apontou que tais modelos são relevantes, especialmente quando associados a outras técnicas, por exemplo, modelos estatísticos e algoritmos genéticos. Dessa forma, 40,74% dos especialistas apontam que conhecem e já trabalharam parcialmente com *machine learning* e suas variações, mostra o Gráfico 10. Apenas 11,11% dos especialistas conhecem e coordenaram o projeto. 37,04% conhecem projetos e suas aplicações, contudo não participaram. 11,11% desconhecem o tema.

Gráfico 10 – Uso do *machine learning* pelos especialistas



Fonte: Autoria própria (2025)

Gráfico 11 – Percepção dos princípios da qualidade



Fonte: Autoria própria (2025)

Em resposta a P9, o Gráfico 11 mostra que, na percepção de 59,26% dos especialistas, os princípios da qualidade influenciam totalmente a gestão de sistemas de cibersegurança nas organizações. 37,04% acredita que influencia parcialmente e 3,7% acredita que influencia pouco. Em específico, os especialistas pontuaram que "melhoria contínua", "foco no cliente" e "gestão de riscos" são centrais para a gestão de sistemas de cibersegurança.

A Tabela 13, em resposta a P10, mostra a frequência com que os especialistas percebem a intensidade da criticidade dos desafios para melhorar continuamente seus sistemas de proteção contra ataques *hackers*. As hipóteses a serem testadas nesse caso são:

H_0: O grau de criticidade dos desafios para melhoria contínua é o mesmo para os especialistas.

H_1: O grau de criticidade dos desafios para melhoria contínua não é o mesmo para os especialistas.

Tabela 13 – Intensidade observada da criticidade dos desafios de melhoria contínua

TABELA OBSERVADA	Rápida evolução dos ataques	Insuficiência de investimento/recursos	Baixa valorização da área de cibersegurança	Falta de planejamento adequado	Treinamento inadequado do pessoal da organização como um todo	Alta burocracia e falta de comunicação entre o setor de cibersegurança e demais áreas da organização	Cultura desatenta a cibersegurança	TOTAL

POUCO CRÍTICO	3	0	1	2	0	1	0	7
CRÍTICO	4	5	8	4	5	12	8	46
MUITO CRÍTICO	20	22	18	21	22	14	19	136
TOTAL	27	27	27	27	27	27	27	189

Fonte: Autoria própria (2025)

O tópico de melhoria é presente no Fator 1 da revisão bibliométrica, assim como aspectos de vulnerabilidades e controles. Entendendo o grau de criticidade dos desafios para melhoria contínua é possível pensar em prioridades e soluções que estão presentes nos SGQ. A Tabela 14 mostra a frequência esperada dos dados observados para então ser feito o teste estatístico.

Tabela 14 – Intensidade esperada da criticidade dos desafios de melhoria contínua

TABELA ESPERADA	Rápida evolução dos ataques	Insuficiência de investimento/recursos	Baixa valorização da área de cibersegurança	Falta de planejamento adequado	Treinamento inadequado do pessoal da organização como um todo	Alta burocracia e falta de comunicação entre o setor de cibersegurança e demais áreas da organização	Cultura desatenta a cibersegurança	TOTAL
POUCO CRÍTICO	1	1	1	1	1	1	1	7
CRÍTICO	6,5714	6,5714	6,5714	6,5714	6,5714	6,5714	6,5714	46
MUITO CRÍTICO	19,4286	19,4286	19,4286	19,4286	19,4286	19,4286	19,4286	136
TOTAL	27	27	27	27	27	27	27	189

Fonte: Autoria própria (2025)

O teste qui-quadrado, com significância (α) de 5% e 12 graus de liberdade, revelou um p-*value* = 0,1062 e X^2 = 17,0054. Portanto, não há evidências científicas suficientes para rejeitar H_0. Assim, aceita-se que o grau de criticidade é o mesmo entre os desafios enfrentados pelas organizações para melhorar continuamente seus sistemas de proteção contra ataques *hackers*.

Tabela 15 – Cálculo do X^2 para a criticidade dos desafios de melhoria contínua

X^2 calculado	Rápida evolução dos ataques	Insuficiência de investimento/recursos	Baixa valorização da área de cibersegurança	Falta de planejamento adequado	Treinamento inadequado do pessoal da organização como um todo	Alta burocracia e falta de comunicação entre o setor de cibersegurança e demais áreas da organização	Cultura desatenta a cibersegurança	TOTAL
POUCO CRÍTICO	4,0000	1,0000	0,0000	1,0000	1,0000	0,0000	1,0000	7,0000
CRÍTICO	1,0062	0,3758	0,3106	1,0062	0,3758	4,4845	0,3106	7,5590
MUITO CRÍTICO	0,0168	0,3403	0,1050	0,1271	0,3403	1,5168	0,0095	2,4464
TOTAL	5,0230	1,7161	0,4156	2,1333	1,7161	6,0013	1,3200	17,0054

Fonte: Autoria própria (2025)

Observando a Tabela 15, nota-se que a alta burocracia e falta de comunicação entre o setor de cibersegurança e demais áreas da organização tem destaque no nível de criticidade, sendo visto como “crítico” e “muito crítico” pelos especialistas. O nível de burocracia e a integração entre departamentos foi visto como FCS da ISO 9000 na revisão da literatura do Capítulo 2 deste trabalho. A percepção dos especialistas sobre este desafio reflete a necessidade de conectar as áreas de cibersegurança com as demais áreas da organização, para que a cibersegurança não seja um ponto isolado dentro da organização. A qualidade quando gerenciada holisticamente consegue impactar positivamente toda a organização.

Outro dado significante é que a rápida evolução dos ataques é vista como “pouca crítica” para os especialistas. Isso mostra que os desafios para a melhoria contínua estão relacionados aos temas de gestão, como a ISO 9000 e a ISO 27000. Os especialistas percebem que sem investimentos a área de cibersegurança entra em déficit, impossibilitando a melhoria contínua dos sistemas de cibersegurança, além disso, o treinamento inadequado do pessoal também é um ponto focal, dado que usários mal treinados se tornam pontos de vulnerabilidades dentro dos sistemas, especialmenete para ataques do tipo *phishing*, portanto, são tópicos que são de fato muito críticos para a área.

Além disso, os especialistas relataram que a gestão *top* nem sempre tem um alto conhecimento da cibersegurança e muitas vezes não entende a importância do pessoal da cibersegurança e que essa falta de compreensão dificulta os avanços na área. Além disso, eles pontuaram que a cibersegurança enfrenta obstáculos significativos e que existe uma relevância

de uma abordagem proativa baseada em análise de riscos e melhoria contínua para uma melhor gestão da cibersegurança.

5.2 PRINCIPAIS ACHADOS DA PESQUISA DE CAMPO

Neste sub-capítulo são apresentados os principais achados da pesquisa de campo por meio do Quadro 11. A partir desses achados podemos confirmar os resultados da revisão bibliográfica apresentados no Capítulo 4 e ver possibilidades de atuação da qualidade dentro da cibersegurança, fortalecendo os sistemas de proteção.

Quadro 11 - Resumo dos principais resultados da pesquisa de campo

Perguntas	Hipóteses	Fator	Achados da pesquisa de campo
P1: Os guias e métodos para classificação de risco indicados na ISO série 27002 de fato são aplicados e contribuem para segurança de CPS? (Seção 2.2.1)	H1: A ISO 27000 apoia os CPS H2: Os guias e métodos de classificação de risco da ISO 27002 têm contribuído para cibersegurança.	1	Os especialistas acreditam que a ISO 27K funciona para a manufatura, e que os métodos de classificação de risco sugeridos pela ISO 27002 também possuem importância na cibersegurança.
P2: Qual o tipo de ataque mais comum e com que frequência ocorrem? (Seção 2.2.2)	H3: Há ataques de maior frequência que precisam ser priorizados.	2	Existem ataques que podem ocorrer mais frequentemente, como é o caso do *phishing* e suas variações, tal confirmação abre oportunidades para se ter medidas preventivas adequadas.
P3: Técnicas estatísticas de monitoramento de processo (CEP) podem ser utilizadas na detecção e prevenção de ataques *hacker*? (Seção 2.3.1)	H4: As técnicas estatísticas de monitoramento são aplicáveis para prevenção e detecção de ataques *hacker*.	2	As técnicas estatísticas de monitoramento apesar de pouco aplicada são poderosas na proteção dos CPS.
P4: *Framework*, como o MITRE ATT&CK e demais diretrizes, como ferramentas de monitoramento atualização de sistemas, auditorias contribuem de fato para a prevenção e detecção de ciberataques? (Seção 2.2.2)	H5: há evidência de que o *framework* e demais diretrizes, como ferramentas de monitoramento atualização de sistemas, auditorias contribuem para prevenção e detecção de ciberataques.	1	O *framework* MITRE ATT&CK e demais diretrizes, como atualização constante de sistemas e ferramentas de segurança é visto pelos especialistas de forma a contribuir para melhoria dos sistemas de cibersegurança.
P5: As Legislações brasileiras atuais contribuem para fortalecer os sistemas de cibersegurança das organizações? (Seção 2.2.3)	H6: O Brasil possui legislação sobre cibersegurança, porém pouco efetiva.	Não se aplica	As Legislações brasileiras atuais contribuem para fortalecer os sistemas de cibersegurança das organizações, porém elas não são suficientes.
P6: O SGQ contribui para a cibersegurança e de que forma que a falta desta pode impactar negativamente os sistemas de cibersegurança? (Seção 2.3)	H7: Há evidência de que atualmente o SGQ tenha contribuído para a cibersegurança.	1	A presença de SGQ impacta moderadamente os sistemas de cibersegurança e a ausência destes impacta fortemente os sistemas de cibersegurança.

P7: Há gargalos e desafios (falta de conhecimento) para aplicação de métodos estatísticos na área de cibersecurança? (Seção 2.3.1)	H8: Há gargalos e desafios significativos que inibem a adoção de técnicas estatísticas em sistemas de cibersegurança.	2	Há desafios enfrentados no uso de técnicas *hard* do TQM na I4.0 na proteção de cibersegurança devido a falta de conhecimento.
P8: Os profissionais da área conhecem as técnicas para detecção de ataques e as utilizam com qual frequência? Os profissionais da área utilizam o *machine learning*? (Seção 2.3.1)	H9: As técnicas não são usadas com mais frequência do que outras.	2	Os profissionais da área conhecem as técnicas. O *machine learning*, ao contrário do que a revisão teórica apontou e a bibliométrica também, não foi a técnica mais votada pelos especialistas, dando prioridade a métodos estatísticos e CEP para as soluções.
P9: Os princípios da qualidade, como os da família ISO 9000, influenciam a gestão de sistemas de cibersegurança nas organizações para prevenção de ataques? (Seção 2.3.2)	H10: Os princípios da qualidade, como os da família ISO 9000, podem colaborar na área de cibersegurança para prevenção de ciberataques.	1	Os SGQ que seguem os princípios da qualidade baseados na série ISO 9000 influenciam na gestão de sistemas de cibersegurança.
P10: Qual o nível de criticidade dos desafios enfrentados pelas organizações para melhorar continuamente seus sistemas de proteção contra ataques? (Seção 2.3.2)	H11: Existem desafios para a melhoria contínua em que o grau de criticidade sobressai em relação a outros.	1	O nível de criticidade dos desafios enfrentados pelas organizações para melhorar continuamente seus sistemas de proteção contra ataques é diferente para cada desafio, com ênfase em alta burocracia e falta de comunicação entre o setor de cibersegurança e demais áreas da organização.

Fonte: Autoria própria (2025)

A integração dos achados da revisão bibliográfica com os resultados da pesquisa de campo permite uma análise mais abrangente sobre a interseção entre gestão da qualidade e cibersegurança. A revisão bibliográfica destacou a complexidade e a interdisciplinaridade do tema, revelando uma ampla variedade de abordagens, desde a detecção de ataques cibernéticos até a aplicação de ferramentas de gestão da qualidade na prevenção de ameaças. Esse panorama se reflete na pesquisa de campo, que confirmou a relevância da família ISO 27000 para a segurança dos sistemas ciber-físicos (CPS), conforme apontado pelos especialistas entrevistados.

Também foi identificado na bibliometria a relevância de *frameworks* para gestão que entrelaçam as áreas de qualidade e cibersegurança. Na pesquisa de campo os especialistas apontaram *frameworks* como MITRE ATT&CK, ISO série 27000, bem como de diretrizes para monitoramento e auditoria de sistemas como essas práticas fundamentais para a melhoria dos sistemas de cibersegurança. Isso revela que a integração da gestão da qualidade à cibersegurança é uma possibilidade, com destaque para temas como Total Quality Management

(TQM) e otimização da segurança e qualidade de serviço. Na bibliometria também verificou-se que a presença de um sistema de gestão da qualidade (SGQ) impacta moderadamente a segurança dos sistemas ciber-físicos, enquanto sua ausência pode ter prejudicial. Esse dado reforça a importância de promover a adoção de SGQs nas organizações como parte das estratégias de segurança digital.

Outro ponto relevante diz respeito às legislações brasileiras sobre cibersegurança. Enquanto a bibliometria focou mais na normatização internacional, como a série ISO 27000, a pesquisa de campo apontou que as regulações nacionais apresentam lacunas e que precisam de revisão. Esse achado destaca a necessidade de um aprimoramento contínuo das políticas regulatórias para acompanhar os avanços tecnológicos e os desafios emergentes.

A revisão bibliográfica também indicou que diversos estudos se concentram na detecção de ataques utilizando técnicas como gráficos de controle associados *machine learning* e algoritmos genéticos, reforçando a necessidade de soluções rápidas e adaptáveis. A pesquisa de campo revelou que, na prática, apesar do monitoramento estatístico ser visto como ferramenta poderosa para o fortalecimento dos sistemas de cibersegurança e que essa metodologia seria ideal para as soluções presentes, os profissionais da área as aplicam pouco, e no que tange a métodos estatísticos, ainda há desconhecimento do assunto. Esse achado sugere que, apesar da academia aprofundar seus estudos nessa área, sua adoção na indústria ainda enfrenta desafios, reforçando a necessidade de investimentos na disseminação do conhecimento e na capacitação de profissionais para ampliar o uso dessas ferramentas na indústria.

A integração dos resultados confirma que a cibersegurança é um campo que se beneficia de abordagens multidisciplinares, combinando conceitos da gestão da qualidade, técnicas estatísticas e *frameworks* específicos da área, embora ainda existam desafios a serem enfrentados, como disseminação do conhecimento na área estatística. Os desafios identificados apontam para a necessidade de maior disseminação do conhecimento e de soluções que aliem robustez teórica e viabilidade prática.

6 DISCUSSÃO DOS RESULTADOS

Na perspectiva de Lakatos, os princípios fundamentais (“núcleo rígido”) relacionados a ciberataques incluem vulnerabilidades, estratégias de ataque e princípios subjacentes à cibersegurança em sistemas produtivos. Com a revisão bibliográfica, foi possível mapear o “cinturão protetor” do programa de pesquisa, composto por estratégias, ferramentas e métodos

utilizados para prevenir ou mitigar ciberataques. Isso inclui a evolução no uso de métodos estatísticos apropriados, como os aplicados em sistemas de detecção de intrusão.

A análise fatorial possibilitou compreender a estrutura, evolução e adaptação do campo de estudo, identificando padrões significativos e conceitos centrais que moldam a compreensão dos ataques cibernéticos. Por meio da revisão bibliométrica, que utilizou ferramentas como *text mining* e análise fatorial, foi identificado que a problemática é atual e relevante, além de evidenciar a necessidade de aprofundar estudos sobre as vulnerabilidades dos sistemas organizacionais conectados. Essas vulnerabilidades incluem roubo de dados, alterações em projetos, interrupções na produção e bloqueios de sistemas.

A metodologia empregada permitiu que fosse entendido qual o estado da arte atual e quais as tendências do tema, por meio da revisão bibliométrica, atingindo o objetivo específico i) deste trabalho. Tal revisão pontuou que a problemática é atual e relevante e que existe a necessidade de aprofundar os estudos para combater os ciberataques. Também foi observado a necessidade de entender que os sistemas organizacionais que são conectados possuem vulnerabilidades, as quais podem atingir o mundo real, trazendo como consequências: roubo de dados e informações, mudança no design do produto e do projeto, paradas não previstas na produção, bloqueio de sistemas, dentre outros problemas.

A detecção de intrusão foi destacada como uma estratégia eficaz para combater ciberataques, dada a crescente sofisticação desses ataques. Inicialmente, o combate aos ciberataques se baseava exclusivamente em modelagem e computação. Contudo, uma tendência emergente reconhece o potencial de ferramentas de gestão da qualidade, como aquelas usadas em sistemas de detecção de intrusão, para mitigação de ataques. Essa abordagem reflete a natureza multidisciplinar do problema, exigindo colaboração além do setor de TI.

Pesquisas, ao longo das últimas duas décadas, revelaram que os gráficos de controle associados à sistemas de *machine learning*, algoritmos genéticos, têm sido bastante úteis para a identificação de ciberataques nas organizações. Diversas pesquisas apontaram alguns gráficos multivariados, como CUSUM, Hotelling T^2, EWMA para identificação de ataques maliciosos. A partir disso, entende-se que existe a necessidade de gerenciar esses dados coletados nos gráficos, portanto, de gerenciar a qualidade. Assim, atinge-se o objetivo deste trabalho: mostrar como a gestão da qualidade pode contribuir na prevenção e detecção de ataques de *hackers*.

Os sistemas de gestão da qualidade (SGQ), em específico, o que cuidam da organização de forma holística, como o TQM ou a série ISO 9000, são aplicáveis à Indústria 4.0. Alémde otimizar processos produtivos, esses modelos auxiliam para a identificação e prevenção dos ciberataques, contribuindo para a chamada Qualidade 4.0.

Os resultados da pesquisa de campo corroboram os achados da revisão bibliométrica e compreendem as métricas de monitoramento e atualização dos sistemas, atingindo os objetivos específicos ii) e iii).

Um ponto central emergente é a percepção da família ISO 27000 como uma referência, mas com limitações quando aplicada de forma estrita. Os especialistas concordam que existe a necessidade se investir em programas de conscientização e na integração de diferentes soluções e metodologias de segurança e isso pode ser visto como parte essencial da estratégia de gestão da qualidade, uma vez que atualmente os ataques transcendem o mundo virtual e atingem o mundo físico, o que reflete uma ampliação do conceito de Qualidade 4.0.

Os especialistas apontam que princípios da qualidade, como melhoria contínua e foco no cliente, são presentes e relevantes no âmbito da cibersegurança, e enfatizam que é sempre necessário entender as necessidades do cliente, contudo lembram que a liderança e o engajamento do pessoal são pontos fundamentais para que ocorra uma boa gestão da cibersegurança. Nota-se que tais observações estão intrinsicamente relacionadas aos pilares da ISO série 27000: confidencialidade, integridade e disponibilidade.

O Fator 1 da bibliometria evidenciou a relação entre qualidade e cibersegurança nos sistemas produtivos e gerenciais. Os especialistas indicaram que a presença de SGQ contribui para a segurança cibernética, enquanto sua ausência compromete significativamente a gestão dos riscos. Além disso, *frameworks* são vistos como medidas eficazes para mitigar ataques, com destaque para o *phishing* como uma das ameaças mais frequentes, assim como a atualização contantes de sistemas.

Desafios como burocracia e falta de comunicação foram apontados como críticos para a melhoria contínua da cibersegurança, reforçando a necessidade de soluções baseadas na gestão da qualidade.

O Fator 2 da bibliometria destacou o uso de gráficos de controle multivariados na detecção de intrusão, alinhado à percepção dos especialistas sobre a poderosa relevância do monitoramento estatístico para detectar anomalias. A integração entre CEP, gráficos de controle e *machine learning* ainda é pouco explorada, indicando um campo promissor para futuras pesquisas.

No contexto da Indústria 4.0, a GQ se consolida como linha de defesa estratégica na prevenção de ataques cibernéticos, fortalecendo a resiliência organizacional. A violação de dados impacta diretamente a integridade, confidencialidade e disponibilidade dos recursos, evidenciando que a segurança não é apenas uma questão técnica, mas também gerencial.

Dessa forma, sugere-se que estudos futuros aprofundem a integração da gestão da qualidade com a cibersegurança, ampliando a adoção de princípios da ISO 9000 e do TQM na área de cibersegurança, além de desenvolver um sistema de gestão integrado que combine normas de qualidade (ISO série 9001) e segurança (ISO série 27001). Ferramentas da qualidade, como listas de verificação e diagramas de causa e efeito, podem ser exploradas para mitigar ataques de *phishing* e outras vulnerabilidades. Métodos estatísticos, como gráficos de controle, são promissores para monitoramento de anomalias, auxiliando equipes de segurança.

Histogramas, gráficos de Pareto e FMEA podem mapear vulnerabilidades e impactos de incidentes cibernéticos. O uso de *machine learning* para otimizar a detecção e mitigação de ataques é outra frente relevante. Essas abordagens devem ser mais bem investigadas para consolidar sua aplicação e eficácia na proteção de sistemas industriais.

Os achados desta pesquisa destacam caminhos práticos para as organizações navegarem pelos desafios da cibersegurança na Indústria 4.0. Ao aproveitar ferramentas de gestão da qualidade, como gráficos de controle multivariados, as organizações podem fortalecer suas defesas contra ameaças cibernéticas, particularmente na detecção e resposta a anomalias dentro de sistemas interconectados. Essa abordagem minimiza potenciais interrupções causadas por ciberataques e estabelece a gestão da qualidade como um componente crítico da resiliência organizacional. Além disso, a integração dessas ferramentas às estratégias de cibersegurança sublinha o valor de uma perspectiva multidisciplinar, conectando a gestão da qualidade aos domínios tecnológico e operacional. Essa integração tem o potencial de otimizar processos, garantir a integridade dos dados e aprimorar a confiabilidade do sistema, abordando assim vulnerabilidades e reduzindo custos operacionais e tempo de inatividade. Em última análise, esses achados capacitam as organizações a se adaptarem melhor às complexidades dos ambientes industriais modernos, promovendo confiança e segurança em ecossistemas cada vez mais digitalizados.

7 CONCLUSÕES

O escopo desta pesquisa exploratória visou investigar de maneira abrangente como a gestão da qualidade pode desempenhar um papel crucial na mitigação das vulnerabilidades inerentes aos sistemas ciber-físicos. Ao longo da revisão teórica, notou-se que a cibersegurança, inicialmente vinculada predominantemente às equipes de TI, concentrava-se em solucionar questões de natureza mais simples. Contudo, à medida que os ambientes produtivos evoluíram para cenários cada vez mais complexos e interconectados, os ataques cibernéticos também se

tornaram mais desafiadores. Diante dessa evolução, as organizações viram-se compelidas a adotar novos métodos de identificação e prevenção para lidar com a crescente sofisticação das ameaças.

Em paralelo, o gerenciamento da qualidade, historicamente considerado essencial para fornecer produtos e serviços de excelência aos clientes, evoluiu ao longo das décadas. Observou-se que a abordagem holística da gestão da qualidade emergiu como a maneira mais adequada de garantir a entrega de produtos de alta qualidade aos clientes. Nesse contexto, a presente pesquisa propôs um olhar mais aprofundado sobre como os ataques cibernéticos impactam os sistemas produtivos. Dessa forma, o objetivo geral deste trabalho surgiu como uma resposta à interseção entre a crescente influência dos ataques cibernéticos nos sistemas produtivos e a necessidade de uma gestão da qualidade holística para enfrentar os desafios emergentes.

A partir da revisão bibliométrica conduzida utilizando a metodologia de Lakatos, notou-se que os resultados revelaram uma convergência relevante entre a cibersegurança e os sistemas de gestão da qualidade. Dentre os principais achados, tem-se os gráficos de controle em destaque, em especial os multivariados, como CUSUM, EWMA, Hotelling T^2 para a identificação de ciberataques. Pesquisas apontam que os gráficos de controle identificam anomalias no tráfego de dados, ou seja, quando o dado coletado se encontra fora dos limites superiores e inferiores de controle, há a necessidade de averiguar se está ocorrendo um ataque *hacker* no sistema de produção. Frequentemente, essas ferramentas são associadas à sistemas de *machine learning* e algoritmos genéticos. Outro ponto relevante encontrado nas pesquisas é a importância de entender as vulnerabilidades dos sistemas conectados, para que estes possam ser monitorados mais cuidadosamente. A partir disso conclui-se que identificando os ciberataques, por meio dos gráficos de controle, é possível desenvolver estratégias de segurança nos sistemas de produção. Além disso, a integração de gráficos de controle, como o EWMA (Média Móvel Ponderada Exponencial), com a Análise de Fourier representa uma abordagem inovadora para identificar padrões temporais em dados coletados de sistemas ciberfísicos, atingindo o objetivo específico i) dessa dissertação, que era verificar pontos de integração entre as áreas de gestão da qualidade e a segurança dos CPS.

As entrevistas com especialistas corroboraram os achados da revisão bibliométrica, destacando a importância da família ISO 27000, embora limitada quando aplicada de forma estrita. Foi enfatizada a necessidade de integração de soluções técnicas e humanas, além de programas de conscientização, para abordar ataques que afetam tanto o mundo virtual quanto o físico. Princípios de qualidade, como melhoria contínua e foco no cliente, foram identificados

como relevantes na cibersegurança, com a liderança e o engajamento de equipes desempenhando papéis críticos.

Desafios gerenciais, como burocracia e falta de comunicação entre setores, foram apontados como barreiras à melhoria contínua, sugerindo que soluções inspiradas na gestão da qualidade podem mitigar tais dificuldades. Além disso, *frameworks* e atualização constante de sistemas para prevenção de ataques, como *phishing*, e ferramentas de gestão, como fluxogramas e folhas de verificação, foram reconhecidos como potencialmente eficazes para identificar e gerenciar vulnerabilidades.

Os gráficos de controle, integrados a *machine learning*, demonstraram ser ferramentas promissoras, embora ainda pouco exploradas, indicando a necessidade de maior investigação acadêmica e aplicação prática. Essa abordagem multidisciplinar reforça a importância de conectar a gestão da qualidade às áreas tecnológica e operacional para otimizar processos, proteger dados e melhorar a confiabilidade dos sistemas. Portanto, com os achados da pesquisa de campo, foram respondidos os objetivos ii) e iii) deste trabalho.

Dessa forma, esta dissertação atingiu seu objetivo geral ao analisar e indicar como a gestão da qualidade pode contribuir para a prevenção e detecção de ataques cibernéticos. Os achados da pesquisa demonstraram que ferramentas da qualidade, como gráficos de controle multivariados, e práticas associadas à metodologias de gestão holística, possuem papel relevante no fortalecimento dos sistemas de cibersegurança paraprevenção e identificação de ciberataques.

As implicações práticas desta pesquisa são particularmente relevantes para organizações que adotam tecnologias da Indústria 4.0. Ao integrar ferramentas de gestão da qualidade, como gráficos de controle multivariados, com estratégias de cibersegurança, as organizações podem aprimorar sua capacidade de detectar e responder a ameaças cibernéticas de forma proativa. Por exemplo, a aplicação de gráficos de controle como EWMA e Hotelling T^2 permite o monitoramento em tempo real de sistemas de produção, melhorando a detecção de anomalias que podem indicar ciberataques. Além disso, essa integração promove uma abordagem holística, onde a gestão da qualidade se estende além da excelência operacional para se tornar um elemento fundamental da segurança organizacional. Os achados destacam a importância da adoção de perspectivas multidisciplinares para enfrentar os desafios da cibersegurança, realçando o papel das ferramentas da qualidade na garantia da integridade dos dados e da confiabilidade do sistema, reduzindo ao mesmo tempo o tempo de inatividade e os custos operacionais.

Este estudo apresenta algumas limitações relacionadas à metodologia adotada. Embora o *text mining* seja uma ferramenta poderosa para identificar padrões e tendências em grandes volumes de dados textuais, sua eficácia depende diretamente da qualidade e consistência dos dados analisados. Dados incompletos ou mal estruturados podem comprometer a confiabilidade dos resultados. Além disso, a interpretação dos resultados gerados por métodos como análise fatorial ou de *cluster* pode introduzir vieses subjetivos. Apesar dessas limitações, o uso complementar de outras abordagens, como análises qualitativas e quantitativas, pode ajudar a mitigar esses desafios, contribuindo para uma compreensão mais abrangente e robusta do campo de estudo.

Existem limitações no que tange a pesquisa de campo, pois a amostra coletada, ou seja, a quantidade de entrevistados foi pequena e os resultados podem estar com viés. Mesmo com a análise descritiva e os testes estatísticos, as respostas podem ser influenciadas pelas percepções individuais e experiências específicas de cada participante.

Considerando os resultados e as limitações, há uma clara necessidade de explorar as possibilidades de integração entre a gestão da qualidade e as estratégias de proteção cibernética. Portanto, como oportunidades para trabalhos futuros, além de aprofundar estudos nas abordagens e ferramentas do Capítulo 6, sugere-se investigar a escalabilidade dessas ferramentas em diferentes ambientes organizacionais, bem como sua adaptabilidade a novas ameaças cibernéticas. Sugere-se também um estudo para verificar o comportamento das organizações quando confrontadas com o problema de ataques de *hackers* atualmente e, finalmente, sugere-se uma simulação de como os gráficos de controle multivariados associados a técnicas de *machine learning* funcionam em diferentes ambientes para identificar anomalias. Estudos na área de gestão se fazem necessários também, identificar fatores críticos de sucesso para entender como a cibersegurança e a qualidade podem estar se entrelaçando cada vez mais pode ser um caminho.

REFERÊNCIAS

ABDULKADHUM ABBAS, S. A.; ABDU IBRAHIM, A. Fortifying IoT Infrastructure Using Machine Learning for DDoS Attack within Distributed Computing-based Routing in Networks. **Qubahan Academic Journal**, v. 4, n. 2, p. 569–581, 30 jun. 2024.

AGYEPONG, E. *et al.* A systematic method for measuring the performance of a cyber security operations centre analyst. **Computers & Security**, v. 124, p. 102959, jan. 2023.

AHANGER, T. A.; TARIQ, U.; NUSIR, M. **Real-Time Methodology for Improving Cyber Security in Internet of Things Using Edge Computing During Attack Threats**. 2019 International Conference on Smart Systems and Inventive Technology (ICSSIT). **Anais**... Em: 2019 INTERNATIONAL CONFERENCE ON SMART SYSTEMS AND INVENTIVE TECHNOLOGY (ICSSIT). Tirunelveli, India: IEEE, nov. 2019. Disponível em: <https://ieeexplore.ieee.org/document/8987779/>. Acesso em: 28 ago. 2024

AHSAN, M. *et al.* T^2 Control Chart based on Successive Difference Covariance Matrix for Intrusion Detection System. **Journal of Physics: Conference Series**, v. 1028, p. 012220, jun. 2018a.

AHSAN, M. *et al.* Intrusion Detection System Using Multivariate Control Chart Hotelling's T2 Based on PCA. **International Journal on Advanced Science, Engineering and Information Technology**, v. 8, n. 5, p. 1905–1911, 7 out. 2018b.

AHSAN, M.; MASHURI, M.; KUSWANTO, H.; PRASTYO, D. D. Intrusion detection system using the bootstrap resampling approach of T2 control chart based on successive difference covariance matrix. **International Journal On Advanced Science, Engineering And Information Technology**, v. 96, n. 8, p. 2128-2138, 2018c.

AHSAN, M.; MASHURI, M.; KHUSNA, H. Hybrid James-Stein and successive difference covariance matrix estimators based Hotelling's T2 chart for network anomaly detection using bootstrap. **Journal of Theoretical and Applied Information Technology**, v. 96, n. 20, p. 6828-6841, 2018d.

AHSAN, M. *et al.* MULTIVARIATE T2 CONTROL CHART BASED ON JAMES-STEIN AND SUCCESSIVE DIFFERENCE COVARIANCE MATRIX ESTIMATORS FOR INTRUSION DETECTION. **Malaysian Journal of Science**, v. 38, p. 23–35, 30 set. 2019.

AHSAN, M. *et al.* Robust adaptive multivariate Hotelling's T2 control chart based on kernel density estimation for intrusion detection system. **Expert Systems with Applications**, v. 145, p. 113105, maio 2020.

AHSAN, M. *et al.* Support vector data description with kernel density estimation (SVDD-KDE) control chart for network intrusion monitoring. **Scientific Reports**, v. 13, n. 1, p. 19149, 6 nov. 2023.

AHSAN, M.; MASHURI, M.; KHUSNA, H. HYBRID JAMES-STEIN AND SUCCESSIVE DIFFERENCE COVARIANCE MATRIX ESTIMATORS BASED HOTELLING'S T2 CHART FOR NETWORK ANOMALY DETECTION USING BOOTSTRAP. . **Vol.**, n. 20, 2005.

ALEKSANDROVA, S. V.; VASILIEV, V. A.; ALEKSANDROV, M. N. **Problems of Implementing Information Security Management Systems**. 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS). **Anais**... Em: 2020 INTERNATIONAL CONFERENCE ON QUALITY MANAGEMENT, TRANSPORT AND INFORMATION SECURITY, INFORMATION TECHNOLOGIES (IT&QM&IS). Yaroslavl, Russia: IEEE, 7 set. 2020. Disponível em: <https://ieeexplore.ieee.org/document/9322896/>. Acesso em: 28 ago. 2024

ALGHASSAB, M. Analyzing the Impact of Cybersecurity on Monitoring and Control Systems in the Energy Sector. **Energies**, v. 15, n. 1, p. 218, 29 dez. 2021.

ALI, H. *et al.* **CellSecure: Securing Image Data in Industrial Internet-of-Things via Cellular Automata and Chaos-Based Encryption**. 2023 IEEE 98th Vehicular Technology Conference (VTC2023-Fall). **Anais**... Em: 2023 IEEE 98TH VEHICULAR TECHNOLOGY CONFERENCE (VTC2023-FALL). Hong Kong, Hong Kong: IEEE, 10 out. 2023. Disponível em: <https://ieeexplore.ieee.org/document/10333478/>. Acesso em: 28 ago. 2024

ALMEIDA, D.; PRADHAN, N.; MUNIZ JR, J. Assessment of ISO 9001:2015 implementation factors based on AHP: Case study in Brazilian automotive sector. **International Journal of Quality & Reliability Management**, v. 35, n. 7, p. 1343–1359, 6 ago. 2018.

ALSHAIBI, A. *et al.* The Comparison of Cybersecurity Datasets. **Data**, v. 7, n. 2, p. 22, 29 jan. 2022.

ALSULAMI, H. Implementation analysis of reliable unmanned aerial vehicles models for security against cyber-crimes: Attacks, tracebacks, forensics and solutions. **Computers and Electrical Engineering**, v. 100, p. 107870, maio 2022.

AMIN, S. O. *et al.* RIDES: Robust Intrusion Detection System for IP-Based Ubiquitous Sensor Networks. **Sensors**, v. 9, n. 5, p. 3447–3468, 11 maio 2009.

ANTONY, J.; MCDERMOTT, O.; SONY, M. Revisiting Ishikawa's Original Seven Basic Tools of Quality Control: A Global Study and Some New Insights. **IEEE Transactions on Engineering Management**, v. 70, n. 11, p. 4005–4020, nov. 2023.

ANTONY, J.; MCDERMOTT, O.; SONY, M. Quality 4.0 conceptualisation and theoretical understanding: a global exploratory qualitative study. **The TQM Journal**, v. 34, n. 5, p. 1169-1188, 17 ago. 2021.

ANTTILA, J.; JUSSILA, K. ISO 9004 - A stimulating quality management standard for the creative leaders of contemporary sustainable organizations. **Production Engineering Archives**, v. 27, n. 2, p. 148–155, 1 jun. 2021.

ASIF, M. Are QM models aligned with Industry 4.0? A perspective on current practices. **Journal of Cleaner Production**, v. 258, p. 120820, jun. 2020.

Autoesporte. Honda é alvo de ataque hacker e suspende parte da produção, incluindo no Brasil. **G1**, 10 jun. 2020. Disponível em: https://autoesporte.globo.com/videos/noticia/2020/06/honda-e-alvo-de-ataque-hacker-e-suspende-parte-da-producao-incluindo-no-brasil.ghtml. Acesso em: 4 dez. 2023.

BASICEVIC, I.; OCOVAJ, S.; POPOVIC, M. Evaluation of entropy-based detection of outbound denial-of-service attacks in edge networks. **Security and Communication Networks**, v. 8, n. 5, p. 837–844, 25 mar. 2015.

BEN HAMIDA, S. *et al.* Adaptive sampling for active learning with genetic programming. **Cognitive Systems Research**, v. 65, p. 23–39, jan. 2021.

BENZAQUEN, J. *et al.* Quality in private health companies in Peru: The relation of QMS & ISO 9000 principles on TQM factor. **International Journal of Healthcare Management**, v. 14, n. 2, p. 311–319, 3 abr. 2021.
BOUYEDDOU, B. et al. **Detecting SYN flood attacks via statistical monitoring charts: A comparative study**. 2017 5th International Conference on Electrical Engineering - Boumerdes (ICEE-B). **Anais**... Em: 2017 5TH INTERNATIONAL CONFERENCE ON ELECTRICAL ENGINEERING - BOUMERDES (ICEE-B). Boumerdes: IEEE, out. 2017. Disponível em: <http://ieeexplore.ieee.org/document/8192118/>. Acesso em: 28 ago. 2024

BRAVI, L.; MURMURA, F. Evidences about ISO 9001:2015 and ISO 9004:2018 implementation in different-size organisations. **Total Quality Management & Business Excellence**, v. 33, n. 11–12, p. 1366–1386, 18 ago. 2022.

BRENTAN, B.; REZENDE, P.; BARROS, D.; MEIRELLES, G.; LUVIZOTTO, E.; IZQUIERDO, J. Cyber-Attack Detection in Water Distribution Systems Based on Blind Sources Separation Technique. **Water**, [S.L.], v. 13, n. 6, p. 795, 14 mar. 2021.

BRODAY, E. E. The evolution of quality: from inspection to quality 4.0. **International Journal of Quality and Service Sciences**, v. 14, n. 3, p. 368–382, 10 ago. 2022.

CAI, X. *et al*. Fuzzy Memory Controller Design Based-Machine Learning Algorithm and Stability Analysis for Nonlinear NCSs Under Asynchronous Cyber Attacks. **IEEE Transactions on Systems, Man, and Cybernetics: Systems**, v. 54, n. 2, p. 1082–1093, fev. 2024.

CALLEGARI, C.; GIORDANO, S.; PAGANO, M. **Anomaly detection: An overview of selected methods**. 2017 International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON). **Anais**... Em: 2017 INTERNATIONAL MULTI-CONFERENCE ON ENGINEERING, COMPUTER AND INFORMATION SCIENCES (SIBIRCON). Novosibirsk: IEEE, set. 2017. Disponível em: <http://ieeexplore.ieee.org/document/8109836/>. Acesso em: 28 ago. 2024

CARVALHO, A. V. *et al.* Quality 4.0: An Overview. **Procedia Computer Science**, v. 181, p. 341–346, 2021.

CAVDAR, B. *et al*. Cascaded fractional order automatic generation control of a PV-reheat thermal power system under a comprehensive nonlinearity effect and cyber-attack. **Electrical Engineering**, v. 105, n. 6, p. 4339–4360, dez. 2023.

CHAN, R. *et al*. Vulnerability Assessments of Building Management Systems. Em: STAGGS, J.; SHENOI, S. (Eds.). **Critical Infrastructure Protection XIV**. IFIP Advances in Information and Communication Technology. Cham: Springer International Publishing, 2020. v. 596p. 209–220.

CHEN, L.; WANG, X. Quickest attack detection in smart grid based on sequential Monte Carlo filtering. **IET Smart Grid**, v. 3, n. 5, p. 686–696, out. 2020.

ČISAR, P.; ČISAR, S.. Quality Control in Function of Statistical Anomaly Detection in Intrusion Detection Systems. **4Th Serbian-Hungarian Joint Symposium On Intelligent Systems**, [*s. l*], v. 4, p. 209-220, jan. 2006.

ČISAR, P.; ČISAR, S. M. Optimized EWMA control charts in function of intrusion detection. In: **9th International Symposium of Hungarian Researchers on Computational Intelligence and Informatics**, v. 9, [s.n.], p. 387-396, jan. 2008.

ČISAR, P.; BOŠNJAK, S.; ČISAR, S. EWMA Algorithm in Network Practice. **International Journal of Computers Communications & Control**, v. 5, n. 2, p. 160, 1 jun. 2010.
CISAR, P.; CISAR, S. M. EWMA Statistic in Adaptive Threshold Algorithm. **11Th International Conference on Intelligent Engineering Systems,** 2007, pp. 51-54.

CNN Brasil. Google, Amazon e CloudWare confirmam ter sofrido maior ataque cibernético da história. **CNN Brasil**, 12 jun. 2023. Disponível em: https://www.cnnbrasil.com.br/economia/google-amazon-e-cloudware-confirmam-ter-sofrido-maior-ataque-cibernetico-da-historia/. Acesso em: 4 dez. 2023.

COLOSIMO, B. M. *et al.* Statistical Process Monitoring from Industry 2.0 to Industry 4.0: Insights into Research and Practice. **Technometrics**, p. 1–35, 13 mar. 2024.

Decreto nº 8.771, de 11 de maio de 2016. Marco Civil da Internet. Diário Oficial da União, Brasília, 12 maio 2016. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm>. Acesso em: 23 de maio de 2024.

Decreto nº 10.222, de 8 de janeiro de 2020. Diário Oficial da União, Brasília, 9 jan. 2020. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm>. Acesso em: 23 de maio de 2024.

Decreto nº 11.491, de 11 de agosto de 2023. Diário Oficial da União, Brasília, 14 ago. 2023. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.htm#:~:text=DECRETO%20N%C2%BA%2011.491%2C%20DE%2012,23%20de%20novembro%20de%202001.>. Acesso em: 23 de maio de 2024.

DEUERLEIN, J. *et al.* Graph decomposition in risk analysis and sensor placement for water distribution network security. [s.d.].

DIAMANTOPOULOU, V.; TSOHOU, A.; KARYDA, M. From ISO/IEC 27002:2013 Information Security Controls to Personal Data Protection Controls: Guidelines for GDPR Compliance. Em: KATSIKAS, S. et al. (Eds.). **Computer Security**. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2020. v. 11980p. 238–257.

DISTERER, G. ISO/IEC 27000, 27001 and 27002 for Information Security Management. **Journal of Information Security**, v. 04, n. 02, p. 92–100, 2013.

DONTHU, N. *et al.* How to conduct a bibliometric analysis: An overview and guidelines. **Journal of Business Research**, v. 133, p. 285–296, set. 2021.

DROMARD, Juliette; KHATOUN, Rida; KHOUKHI, Lyes. Adaptive CUSUM Algorithm to Detect Malicious Behaviors in Wireless Mesh Networks. **Lecture Notes In Computer Science**, Berlin, Heidelberg, v. 8508, n. 1, p. 29-41, 2014. Springer Berlin Heidelberg.

ELHABASHY, A. E. *et al.* A cyber-physical attack taxonomy for production systems: a quality control perspective. **Journal of Intelligent Manufacturing**, v. 30, n. 6, p. 2489–2504, ago. 2019.

ELHABASHY, A. E. *et al.* Random sampling strategies for multivariate statistical process control to detect cyber-physical manufacturing attacks. **Quality Engineering**, v. 33, n. 2, p. 300–317, 3 abr. 2021.

ELHABASHY, A. E.; WELLS, L. J.; CAMELIO, J. A. Cyber-physical attack vulnerabilities in manufacturing quality control tools. **Quality Engineering**, v. 32, n. 4, p. 676–692, 1 out. 2020.

EMRAN, S. M.; YE, N. Robustness of Chi-square and Canberra distance metrics for computer intrusion detection. **Quality and Reliability Engineering International**, v. 18, n. 1, p. 19–28, jan. 2002.

FAHMY, Y.; ALSUHLI, G.; KHATTAB, A. Optimizing Environment-aware VANET Clustering using Machine Learning. **International Journal of Intelligent Transportation Systems Research**, v. 21, n. 3, p. 394–408, dez. 2023.

FAROOQ, A. *et al.* Impact of cyber-attack on coordinated voltage control in low voltage grids. **IET Renewable Power Generation**, v. 17, n. 11, p. 2887–2894, ago. 2023.

FRANKÓ, A. *et al.* Applied Machine Learning for IIoT and Smart Production—Methods to Improve Production Quality, Safety and Sustainability. **Sensors**, v. 22, n. 23, p. 9148, 25 nov. 2022.

G1. Hospital Universitário da USP sofre ataque de hackers e deixa de atender ao menos 700 pacientes em uma semana. **G1**, São Paulo, 30 mar. 2023. Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2023/03/30/hospital-universitario-da-usp-sofre-ataque-de-hackers-e-deixa-de-atender-ao-menos-700-pacientes-em-uma-semana.ghtml. Acesso em: 24 maio 2023.

G1. JBS diz que pagou US$ 11 milhões em resposta a ataque hacker em operações nos EUA. **G1**, 9 jun. 2021. Disponível em: https://g1.globo.com/economia/noticia/2021/06/09/jbs-diz-que-pagou-11-milhoes-em-resposta-a-ataque-hacker-em-operacoes-nos-eua.ghtml. Acesso em: 4 dez. 2023.

GABER, T.; EL-GHAMRY, A.; HASSANIEN, A. E. Injection attack detection using machine learning for smart IoT applications. **Physical Communication**, v. 52, p. 101685, jun. 2022.

GERHARDT, T. E.; SILVEIRA, D. T. **Métodos de Pesquisa**. 1. ed. [s.l.] Editora da UFRGS, 2009.

GREMYR, I. *et al.* Increasing the value of quality management systems. **International Journal of Quality and Service Sciences**, v. 13, n. 3, p. 381–394, 14 set. 2021.

GUO, Y. *et al.* Unsupervised Anomaly Detection in IoT Systems for Smart Cities. **IEEE Transactions on Network Science and Engineering**, v. 7, n. 4, p. 2231–2242, 1 out. 2020.

HAGEDORN, D.; HONDA, B.; PETERSON, D. **Process Control Security Journey**. Conference Record of 2007 Annual Pulp and Paper Industry Technical Conference. **Anais**... Em: CONFERENCE RECORD OF 2007 ANNUAL PULP AND PAPER INDUSTRY TECHNICAL CONFERENCE. Williamsburg, VA, USA: IEEE, jun. 2007. Disponível em: <http://ieeexplore.ieee.org/document/4286292/>. Acesso em: 28 ago. 2024

HAIDER, W. *et al*. Generating realistic intrusion detection system dataset based on fuzzy qualitative modeling. **Journal of Network and Computer Applications**, v. 87, p. 185–192, jun. 2017.

HAIR, Joseph. F. *et al. Análise multivariada de dados*. 6 ed. Porto Alegre, RS: Bookman, 2009.

HAUFE, K. *et al.* Improving Transparency and Efficiency in IT Security Management Resourcing. **IT Professional**, v. 20, n. 1, p. 53–62, jan. 2018.

HAZRATI-MARANGALOO, H.; NOOROSSANA, R. A nonparametric change detection approach in social networks. **Quality and Reliability Engineering International**, v. 37, n. 6, p. 2916–2935, out. 2021.

HOSSAIN, M. S.; ISLAM, M. S.; RAHMAN, M. A. A Cyber Range Framework for Emulating Secure and Private IT/OT Consumer Service Verticals Towards 6G. **IEEE Transactions on Consumer Electronics**, p. 1–1, 2024.

HU, K.; YE, J.; SONG, W. Vulnerability Assessments of Induction Machine-Based Multistage Rolling Mill System Under Sensor Integrity Attacks. **IEEE Transactions on Industrial Informatics**, v. 20, n. 6, p. 8616–8627, jun. 2024.

HUANG, X. *et al.* EEFED: Personalized Federated Learning of Execution&Evaluation Dual Network for CPS Intrusion Detection. **IEEE Transactions on Information Forensics and Security**, v. 18, p. 41–56, 2023.
HUMAYED, A. et al. Cyber-Physical Systems Security—A Survey. **IEEE Internet of Things Journal**, v. 4, n. 6, p. 1802–1831, dez. 2017.

HUSÁK, M. *et al.* Lessons Learned from Automated Sharing of Intrusion Detection Alerts: The Case of the SABU Platform. **Digital Threats: Research and Practice**, v. 4, n. 4, p. 1–11, 31 dez. 2023.

IMRAN, M. *et al.* A performance overview of machine learning-based defense strategies for advanced persistent threats in industrial control systems. **Computers & Security**, v. 134, p. 103445, nov. 2023.

JIANG, Baoxiang; LIU, Yang; LIU, Huixiang; REN, Zehua; WANG, Yun; BAO, Yuanyi; WANG, Wenqing. An Enhanced EWMA for Alert Reduction and Situation Awareness in Industrial Control Networks. **2022 Ieee 18Th International Conference On Automation Science And Engineering (Case)**, [S.L.], p. 888-894, 20 ago. 2022.

KAGERMANN, H.; WAHLSTER, W.; HELBIG, J. Recommendations for Implementing the Strategic Iniciative Industrie 4.0: Securing the Future of German Manufacturing Industry. Final Reporte Industrie 4.0 Working Group of Acatech, 2013.

KHAN, M. S.; CUI, L. **Statistical process control based chart for information systems security**. (C. M. Falco, X. Jiang, Eds.). Em: SEVENTH INTERNATIONAL CONFERENCE ON DIGITAL IMAGE PROCESSING (ICDIP15). Los Angeles, United States: 6 jul. 2015. Disponível em: <http://proceedings.spiedigitallibrary.org/proceeding.aspx?doi=10.1117/12.2197092>. Acesso em: 28 ago. 2024

KIM, H. K.; IM, K. H.; PARK, S. C. DSS for computer security incident response applying CBR and collaborative response. **Expert Systems with Applications**, v. 37, n. 1, p. 852–870, jan. 2010.

KOLOSOK, I.; GURINA, L. Monitoring and analysis of SCADA and WAMS data for EPS digitalization. **E3S Web of Conferences**, v. 209, p. 02015, 2020.

KOTENKO, I. V.; PARASHCHUK, I. B. Specification of Quality Indicators for Security Event and Incident Management in the Supply Chain. **International Journal of Computing**, *[S. l.]*, v. 20, n. 1, p. 22-30, 2021.

KOTENKO, I.; GAIFULINA, D.; ZELICHENOK, I. Systematic Literature Review of Security Event Correlation Methods. **IEEE Access**, v. 10, p. 43387–43420, 2022.

KUHL, M.; WIENER, T.; KRAUSS, M. Multisensorial Self-learning Systems for Quality Monitoring of Carbon Fiber Composites in Aircraft Production. **Procedia CIRP**, v. 12, p. 103–108, 2013.

LAKATOS, Imre. *The methodology of scientific research programmes*. 1. ed. New York, NY, USA: Cambridge University Press, 1978.

LEE, Edward A.. Cyber Physical Systems: design challenges. **2008 11Th Ieee International Symposium On Object And Component-Oriented Real-Time Distributed Computing (Isorc)**, [S.L.], p. 363-369, maio 2008.

Lei nº 12.737, de 30 de novembro de 2012. "Lei Carolina Dickmann". Diário Oficial da União, Brasília, 3 dez. 2012. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 23 de maio de 2024.

Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Diário Oficial da União, Brasília, 15 ago. 2018. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 23 de maio de 2024.

LEITE, J. B.; MANTOVANI, J. R. S. Detecting and Locating Non-Technical Losses in Modern Distribution Networks. **IEEE Transactions on Smart Grid**, v. 9, n. 2, p. 1023–1032, mar. 2018.

LI, W.; SHI, Y.; LI, Y. Research on secure control and communication for cyber-physical systems under cyber-attacks. **Transactions of the Institute of Measurement and Control**, v. 41, n. 12, p. 3421–3437, ago. 2019.

LI, Y. *et al.* Monitoring Runtime Metrics of Fog Manufacturing via a Qualitative and Quantitative (QQ) Control Chart. **ACM Transactions on Internet of Things**, v. 3, n. 2, p. 1–19, 31 maio 2022.

LIANG, J. *et al.* Security Risk Analysis of Active Distribution Networks with Large-Scale Controllable Loads under Malicious Attacks. **Complexity**, v. 2021, n. 1, p. 6659879, jan. 2021.

LIM, Johan; LEE, Sungim. Improved control chart for statistical process control using combined X and delayed EWMA statistics. **Journal Of The Korean Statistical Society**, [S.L.], v. 52, n. 4, p. 944-959, 21 set. 2023.

LIU, W.; SUN, J.; WANG, G.; BULLO, F.; CHEN, J. Resilient control under quantization and denial-of-service: Codesigning a deadbeat controller and transmission protocol. IEEE Transactions on Automatic Control, v. 67, n. 8, p. 3879-3891, 2021

MAHAN, T.; MENOLD, J. Simulating cyber-physical systems: Identifying vulnerabilities for design and manufacturing through simulated additive manufacturing environments. **Additive Manufacturing**, v. 35, p. 101232, out. 2020.

MAHMOUD, M. S.; HAMDAN, M. M.; BAROUDI, U. A. Modeling and control of Cyber-Physical Systems subject to cyber attacks: A survey of recent advances and challenges. **Neurocomputing**, v. 338, p. 101–115, abr. 2019.

MANLY, Bryan. F. J. *Métodos estatísticos variados: uma introdução*. 3 ed. Porto Alegre, RS: Bookman, 2008.

MARGHERITA, E. G.; BRACCINI, A. M. The impact of Industry 4.0 technologies and the soft side of TQM on organisational performance: a multiple case study analysis on manufacturing organisations. **The TQM Journal**, v. 36, n. 3, p. 812–831, 18 mar. 2024.

MASHURI, M. *et al.* Comparing the performance of T^2 chart based on PCA Mix, Kernel PCA Mix, and Mixed Kernel PCA for Network Anomaly Detection. **Journal of Physics: Conference Series**, v. 1752, n. 1, p. 012008, 1 fev. 2021.

MCDERMOTT, O. *et al.* The use and application of the 7 new quality control tools in the manufacturing sector: a global study. **The TQM Journal**, v. 35, n. 8, p. 2621–2639, 5 dez. 2023.

MENG, X. *et al.* **Packet Representation Learning for Traffic Classification**. Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining. **Anais**... Em: KDD '22: THE 28TH ACM SIGKDD CONFERENCE ON KNOWLEDGE DISCOVERY AND DATA MINING. Washington DC USA: ACM, 14 ago. 2022. Disponível em: <https://dl.acm.org/doi/10.1145/3534678.3539085>. Acesso em: 28 ago. 2024

MERIAH, I.; ARFA RABAI, L. B. Comparative Study of Ontologies Based ISO 27000 Series Security Standards. **Procedia Computer Science**, v. 160, p. 85–92, 2019.

MISHRA, B. K.; KESHRI, N. Mathematical model on the transmission of worms in wireless sensor network. **Applied Mathematical Modelling**, v. 37, n. 6, p. 4103–4111, mar. 2013.

MOHAN, A.; KHURANA, H. Implementing Cyber Security Requirements and Mechanisms in Microgrids. Em: RICE, M.; SHENOI, S. (Eds.). **Critical Infrastructure Protection IX**. IFIP Advances in Information and Communication Technology. Cham: Springer International Publishing, 2015. v. 466p. 229–244.

MOHY-EDDINE, M. *et al.* An efficient network intrusion detection model for IoT security using K-NN classifier and feature selection. **Multimedia Tools and Applications**, v. 82, n. 15, p. 23615–23633, jun. 2023.

MOLNAR, A.-J.; GROSSMANN, J. **CRSTIP -- An Assessment Scheme for Security Assessment Processes**. 2014 IEEE International Symposium on Software Reliability Engineering Workshops. **Anais**... Em: 2014 IEEE INTERNATIONAL SYMPOSIUM ON SOFTWARE RELIABILITY ENGINEERING WORKSHOPS (ISSREW). Naples, Italy: IEEE, nov. 2014. Disponível em: <https://ieeexplore.ieee.org/document/6983856>. Acesso em: 28 ago. 2024

MONTGOMERY, Douglas. C.; RUNGER, George. C. *Estatística Aplicada e Probabilidade para Engenheiros*. 7 ed. Rio de Janeiro, RJ: LTC, 2021.

MUJTABA, Muhammad; NANDA, Priyadarsi; HE, Xiangjian. Border Gateway Protocol Anomaly Detection Using Failure Quality Control Method. **2012 Ieee 11Th International Conference On Trust, Security And Privacy In Computing And Communications**, [S.L.], v. 11, n. 1, p. 1239-1244, jun. 2012.

NADEEM, A.; HOWARTH, M. **Adaptive intrusion detection & prevention of denial of service attacks in MANETs**. Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly. **Anais**... Em: IWCMC '09: 2009 INTERNATIONAL WIRELESS COMMUNICATIONS AND MOBILE COMPUTING CONFERENCE. Leipzig Germany: ACM, 21 jun. 2009. Disponível em: <https://dl.acm.org/doi/10.1145/1582379.1582581>. Acesso em: 28 ago. 2024

NARDO, M.; FORINO, D.; MURINO, T. The evolution of man–machine interaction: the role of human in Industry 4.0 paradigm. **Production & Manufacturing Research**, v. 8, n. 1, p. 20–34, 1 jan. 2020.
NEUMANN, W. P. et al. Industry 4.0 and the human factor – A systems framework and analysis methodology for successful development. **International Journal of Production Economics**, v. 233, p. 107992, mar. 2021.

NEVES, F. *et al.* Construction of taxonomy of conceptualization of sustainability in improving the industrial production process. **International Journal of Quality & Reliability Management**, v. 41, n. 5, p. 1377–1399, 8 abr. 2024.

NGUYEN, T. H. *et al.* **One-Sided Synthetic-RZ control charts: a new method for anomaly detection**. 2019 6th NAFOSTED Conference on Information and Computer Science (NICS). **Anais**... Em: 2019 6TH NAFOSTED CONFERENCE ON INFORMATION AND COMPUTER SCIENCE (NICS). Hanoi, Vietnam: IEEE, dez. 2019. Disponível em: <https://ieeexplore.ieee.org/document/9023851/>. Acesso em: 28 ago. 2024

POONAWALA, Mustafa; SONAWANE, Atharva; LODHA, Mokshit; GOHOKAR, Vinaya; ASKHEDKAR, Anjali; DANVE, Shruti. LoRa-Based Farm Monitoring System. **Lecture Notes In Networks And Systems**, [S.L.], v. 782, n. 1, p. 281-289, 22 dez. 2023.

RAHMAN, M. H.; SHAFAE, M. Physics-based detection of cyber-attacks in manufacturing systems: A machining case study. **Journal of Manufacturing Systems**, v. 64, p. 676–683, jul. 2022.

RAJESH, P. *et al.* **Analysis Of Cyber Threat Detection And Emulation Using MITRE Attack Framework**. 2022 International Conference on Intelligent Data Science Technologies and Applications (IDSTA). **Anais**... Em: 2022 INTERNATIONAL CONFERENCE ON INTELLIGENT DATA SCIENCE TECHNOLOGIES AND APPLICATIONS (IDSTA). San Antonio, TX, USA: IEEE, 5 set. 2022. Disponível em: <https://ieeexplore.ieee.org/document/9923170/>. Acesso em: 28 ago. 2024

RAISINGHANI, Mahesh S.. Can Total Quality Management Exist in Cyber Security. **Cyber Security And Threats**, [S.L.], v. 1, n. 1, p. 1403-1415, maio 2014.

RANSEWA, S.; ELZ, N.; THANON, N.; INTAJAG, S. Anomaly detection using source port data with Shannon entropy and EWMA control chart. In: **18th International Conference on Control, Automation and Systems (ICCAS)**, 2018, PyeongChang, Korea (South). [s.n.], 2018. p. 596-601.

RAVIKUMAR, G.; HYDER, B.; GOVINDARASU, M. **Hardware-in-the-Loop CPS Security Architecture for DER Monitoring and Control Applications**. 2020 IEEE Texas Power and Energy Conference (TPEC). **Anais**... Em: 2020 IEEE TEXAS POWER AND ENERGY CONFERENCE (TPEC). College Station, TX, USA: IEEE, fev. 2020. Disponível em: <https://ieeexplore.ieee.org/document/9042578/>. Acesso em: 28 ago. 2024

REGE, A. *et al.* Students' Application of the MITRE ATT&CK® Framework via a real-time Cybersecurity Exercise. **European Conference on Cyber Warfare and Security**, v. 22, n. 1, p. 384–394, 19 jun. 2023.

Resolução nº 4.658, de 26 de junho de 2018. Diário Oficial da União, Brasília, 27 jun. 2018. Disponível em: < https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=RESOLU%C3%87%C3%83O&numero=4658>. Acesso em: 23 de maio de 2024.

Resolução nº 740, de 13 de outubro de 2020. Diário Oficial da União, Brasília, 14 out. 2020. Disponível em: < https://informacoes.anatel.gov.br/legislacao/resolucoes/2020/1497-resolucao-740>. Acesso em: 23 de maio de 2024.

RODRÍGUEZ MARTÍNEZ, C. *et al.* A Novel Approach for Detection and Location of Cyber-Attacks in Water Distribution Networks. Em: HERNÁNDEZ HEREDIA, Y.; MILIÁN NÚÑEZ, V.; RUIZ SHULCLOPER, J. (Eds.). **Progress in Artificial Intelligence and Pattern Recognition**. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2021. v. 13055p. 79–90.

RODRÍGUEZ-MARTÍNEZ, C.; QUIÑONES-GRUEIRO, M.; LLANES-SANTIAGO, O. Cyberattack Diagnosis in Water Distribution Networks Combining Data-Driven and Structural Analysis Methods. **Journal of Water Resources Planning and Management**, v. 149, n. 5, p. 04023013, maio 2023.

SACOMANO, J. B.; GONÇALVES, R. F.; SILVA, M. T.; BONILLA, S. H.; SÁTYRO, W. C.. Indústria 4.0: conceitos e fundamentos. São Paulo: Edgard Blucher, 2018.

SAHA, S. *et al.* Towards an Optimized Ensemble Feature Selection for DDoS Detection Using Both Supervised and Unsupervised Method. **Sensors**, v. 22, n. 23, p. 9144, 25 nov. 2022.

SANDERS, A.; ELANGESWARAN, C.; WULFSBERG, J. Industry 4.0 implies lean manufacturing: Research activities in industry 4.0 function as enablers for lean manufacturing. **Journal of Industrial Engineering and Management**, v. 9, n. 3, p. 811, 21 set. 2016.

SARHAN, M.; LAYEGHY, S.; PORTMANN, M. Towards a Standard Feature Set for Network Intrusion Detection System Datasets. **Mobile Networks and Applications**, v. 27, n. 1, p. 357–370, fev. 2022.
SEN, Ö. et al. On using contextual correlation to detect multi-stage cyber attacks in smart grids. **Sustainable Energy, Grids and Networks**, v. 32, p. 100821, dez. 2022.

SHAFAE, M. S.; WELLS, L. J.; PURDY, G. T. Defending against product-oriented cyber-physical attacks on machining systems. **The International Journal of Advanced Manufacturing Technology**, v. 105, n. 9, p. 3829–3850, dez. 2019.

SHAOHUI, M. *et al.* PCA mix-based Hotelling's T^2 multivariate control charts for intrusion detection system. **IET Information Security**, v. 16, n. 3, p. 161–177, maio 2022.

SHRIVASTAV, S. K. How *The TQM Journal* has addressed "quality": a literature review using bibliometric analysis. **The TQM Journal**, v. 35, n. 8, p. 2640–2657, 5 dez. 2023.

SINGH, G. P.; SANDHU, J. K.; HOODA, M. K. **BiLSTM Classifier: A New Approach for Detecting Cyber-Attacks in MITRE ATTACK Framework**. 2023 6th International Conference on Contemporary Computing and Informatics (IC3I). **Anais**... Em: 2023 6TH INTERNATIONAL CONFERENCE ON CONTEMPORARY COMPUTING AND INFORMATICS (IC3I). Gautam Buddha Nagar, India: IEEE, 14 set. 2023. Disponível em: <https://ieeexplore.ieee.org/document/10398021/>. Acesso em: 28 ago. 2024

SKLAVOUNOS, D.; EDOH, A.; PLYTAS, M. **A Statistical Approach Based on EWMA and CUSUM Control Charts for R2L Intrusion Detection**. 2017 Cybersecurity and Cyberforensics Conference (CCC). **Anais**... Em: 2017 CYBERSECURITY AND CYBERFORENSICS CONFERENCE (CCC). London: IEEE, nov. 2017. Disponível em: <http://ieeexplore.ieee.org/document/8252897/>. Acesso em: 28 ago. 2024

STEFANOVA-STOYANOVA, V.; DANOV, P. **Comparative Analysis of Specialized Standards and Methods on Increasing the Effectiveness and Role of PDCA for Risk Control in Management Systems**. 2022 10th International Scientific Conference on Computer Science (COMSCI). **Anais**... Em: 2022 10TH INTERNATIONAL SCIENTIFIC CONFERENCE ON COMPUTER SCIENCE (COMSCI). Sofia, Bulgaria: IEEE, 30 maio 2022. Disponível em: <https://ieeexplore.ieee.org/document/9912583/>. Acesso em: 28 ago. 2024

SUNDARARAJAN, A. *et al.* Survey on synchrophasor data quality and cybersecurity challenges, and evaluation of their interdependencies. **Journal of Modern Power Systems and Clean Energy**, v. 7, n. 3, p. 449–467, maio 2019.

SUNNY, K.; SHEIKH, A.; WAGH, S. **Application of Dynamic Mode Decomposition for Temperature Analysis in Smart Building**. 2020 7th International Conference on Control, Decision and Information Technologies (CoDIT). **Anais**... Em: 2020 7TH INTERNATIONAL CONFERENCE ON CONTROL, DECISION AND INFORMATION TECHNOLOGIES (CODIT). Prague, Czech Republic: IEEE, 29 jun. 2020. Disponível em: <https://ieeexplore.ieee.org/document/9263862/>. Acesso em: 28 ago. 2024

TOLEDO, José Carlos; BORRÁS, Miguel Angel A.; MERGULHÃO, Ricardo Coser; MENDES, Glauco H. S. **Qualidade: gestão e métodos**. São Paulo: Editora Atlas, 2005. ISBN 978-85-216-2117-3.

TSAI, Y.-T. *et al.* Using WPCA and EWMA Control Chart to Construct a Network Intrusion Detection Model. **IET Information Security**, v. 2024, n. 1, p. 3948341, jan. 2024.

VELLINGIRI, J. *et al.* Strategies for classifying water quality in the Cauvery River using a federated learning technique. **International Journal of Cognitive Computing in Engineering**, v. 4, p. 187–193, jun. 2023.

VINCENT, H. *et al.* Trojan Detection and Side-channel Analyses for Cyber-security in Cyber-physical Manufacturing Systems. **Procedia Manufacturing**, v. 1, p. 77–85, 2015.

VIINIKKA, Jouni; DEBAR, Hervé. Monitoring IDS Background Noise Using EWMA Control Charts and Alert Information. **Lecture Notes In Computer Science**, [S.L.], v. 7, n. 1, p. 166-187, set. 2004

VITORINO, J. *et al.* Reliable feature selection for adversarially robust cyber-attack detection. **Annals of Telecommunications**, 7 jun. 2024.

WANG, Q. *et al.* Source-Load Coordinated Reserve Allocation Strategy Considering Cyber-Attack Risks. **IEEE Access**, v. 7, p. 111332–111340, 2019.

WELLS, L. J. *et al.* Cyber-physical security challenges in manufacturing systems. **Manufacturing Letters**, v. 2, n. 2, p. 74–77, abr. 2014.

WILSON, J. P.; CAMPBELL, L. Developing a knowledge management policy for ISO 9001: 2015. **Journal of Knowledge Management**, v. 20, n. 4, p. 829–844, 11 jul. 2016.

WU, Xiaoyong; MAHADIK, V.A.; REEVES, D.s.. A summary of detection of denial-of-QoS attacks on DiffServ networks. **Proceedings Darpa Information Survivability Conference And Exposition**, [S.L.], v. 2, n. 1, p. 277-282, 22 abr. 2003.

WURZENBERGER, M. *et al.* **Creating Character-based Templates for Log Data to Enable Security Event Classification**. Proceedings of the 15th ACM Asia Conference on Computer and Communications Security. **Anais**... Em: ASIA CCS '20: THE 15TH ACM ASIA CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY. Taipei Taiwan: ACM, 5 out. 2020. Disponível em: <https://dl.acm.org/doi/10.1145/3320269.3384722>. Acesso em: 28 ago. 2024
XIAN, X.; WANG, A. A Nonparametric Adaptive Sampling Strategy for Online Monitoring of Big Data Streams. [s.d.].

XIAO, J. *et al.* **Virtual Impedance Control for Load Sharing and Bus Voltage Quality Improvement**. 2023 25th European Conference on Power Electronics and Applications (EPE'23 ECCE Europe). **Anais**... Em: 2023 25TH EUROPEAN CONFERENCE ON POWER ELECTRONICS AND APPLICATIONS (EPE'23 ECCE EUROPE). Aalborg, Denmark: IEEE, 4 set. 2023. Disponível em: <https://ieeexplore.ieee.org/document/10264242/>. Acesso em: 28 ago. 2024

XIAO, J. *et al.* Virtual Impedance Control for Load Sharing and Bus Voltage Quality Improvement in Low-Voltage AC Microgrid. **IEEE Transactions on Smart Grid**, v. 15, n. 3, p. 2447–2458, maio 2024.

XU, L. D.; XU, E. L.; LI, L. Industry 4.0: state of the art and future trends. **International Journal of Production Research**, v. 56, n. 8, p. 2941–2962, 18 abr. 2018.

YANG, W. *et al.* Online detection of cyber-incidents in additive manufacturing systems via analyzing multimedia signals. **Quality and Reliability Engineering International**, v. 38, n. 3, p. 1340–1356, abr. 2022.

YE, N. *et al.* Multivariate statistical analysis of audit trails for host-based intrusion detection. **IEEE Transactions on Computers**, v. 51, n. 7, p. 810–820, jul. 2002.

YE, N.; BORROR, C. M.; PARMAR, D. Scalable Chi-Square Distance versus Conventional Statistical Distance for Process Monitoring with Uncorrelated Data Variables. **Quality and Reliability Engineering International**, v. 19, n. 6, p. 505–515, nov. 2003.

YE, N.; BORROR, C.; ZHANG, Y. EWMA techniques for computer intrusion detection through anomalous changes in event intensity. **Quality and Reliability Engineering International**, v. 18, n. 6, p. 443–451, nov. 2002.

YE, N.; CHEN, Q. Attack–norm separation for detecting attack-induced quality problems on computers and networks. **Quality And Reliability Engineering International**, [S.L.], v. 23, n. 5, p. 545-553, 7 nov. 2006.

YE, Z.; LIU, C.; KAN, C. Stereo vision enabled flexible in-situ process authentication of additive manufacturing. **Manufacturing Letters**, v. 35, p. 1155–1162, ago. 2023.

ZHANG, J.; YE, J. **Cyber-Attack Detection for Active Neutral Point Clamped (ANPC) Photovoltaic (PV) Converter using Kalman Filter**. 2022 IEEE Applied Power Electronics Conference and Exposition (APEC). **Anais**... Em: 2022 IEEE APPLIED POWER ELECTRONICS CONFERENCE AND EXPOSITION (APEC). Houston, TX, USA: IEEE, 20 mar. 2022. Disponível em: <https://ieeexplore.ieee.org/document/9773382/>. Acesso em: 28 ago. 2024

ZHANG, M. *et al*. Distributed Observer-Based Event-Triggered Load Frequency Control of Multiarea Power Systems Under Cyber Attacks. **IEEE Transactions on Automation Science and Engineering**, v. 20, n. 4, p. 2435–2444, out. 2023.

ZHANG, Y.; LI, S. Kinematic Control of Serial Manipulators Under False Data Injection Attack. **IEEE/CAA Journal of Automatica Sinica**, v. 10, n. 4, p. 1009–1019, abr. 2023.

ZHANG, Z.; ZHU, X.; JIN, J. **SVC-Based Multivariate Control Charts for Automatic Anomaly Detection in Computer Networks**. Third International Conference on Autonomic and Autonomous Systems (ICAS'07). **Anais**... Em: THIRD INTERNATIONAL CONFERENCE ON AUTONOMIC AND AUTONOMOUS SYSTEMS (ICAS'07). Athens, Greece: IEEE, jun. 2007. Disponível em: <http://ieeexplore.ieee.org/document/4437933/>. Acesso em: 28 ago. 2024

ZHONG, Y. *et al*. Detecting Anomalous Robot Motion in Collaborative Robotic Manufacturing Systems. **IEEE Internet of Things Journal**, v. 11, n. 8, p. 13722–13733, 15 abr. 2024.

ZHOU, H. *et al*. **Echo State Network Learning for the Detection of Cyber Attacks in Additive Manufacturing**. 2021 IEEE 17th International Conference on Automation Science and Engineering (CASE). **Anais**... Em: 2021 IEEE 17TH INTERNATIONAL CONFERENCE ON AUTOMATION SCIENCE AND ENGINEERING (CASE). Lyon, France: IEEE, 23 ago. 2021. Disponível em: <https://ieeexplore.ieee.org/document/9551673/>. Acesso em: 28 ago. 2024

ZINEDDINE, M. Optimizing security and quality of service in a real-time operating system using multi-objective Bat algorithm. **Future Generation Computer Systems**, v. 87, p. 102–114, out. 2018.

ZONNENSHAIN, A.; KENETT, R. S. Quality 4.0—the challenging future of quality engineering. **Quality Engineering**, v. 32, n. 4, p. 614–626, 1 out. 2020.

APÊNDICE A

Roteiro da Entrevista

APRESENTAÇÃO:

Gostaria de agradecer você por ter aceitado participar desta pesquisa. Meu nome é Fernanda e eu sou mestranda da UFSCar. Com essa pesquisa eu quero explorar os diversos aspectos relacionados à gestão da segurança cibernética em organizações. Além disso, busco entender quais são as métricas de monitoramento e acompanhamento da eficácia do sistema, bem como saber de que modo o sistema se atualiza e responde a novas ameaças. Portanto estou enviando este questionário para especialistas da área. O questionário conta com 3 perguntas descritivas, e as demais são teste. Não há respostas certas ou erradas; simplesmente estou buscando entender suas visões e experiências, então por favor sinta-se à vontade para responder o que realmente pensa. Estimo que o senhor(a) irá demorar 15 minutos para responder o questionário por completo.

Qualquer dúvida, meu e-*mail* para contato é: fernanda.berretta@estudante.ufscar.br ou (19) 97169-2603

DADOS DO PARTICIPANTE:

1- Inicialmente vou coletar dados sobre você, para fins descritivos. Qual o seguimento que o senhor(a) atua?

2- Qual seu atual cargo?

3- Qual sua conexão com a cibersegurança?

4- A ISO 27000 é voltada para segurança da informação, entretanto, os ataques hoje estão cruzando essa linha e afetando o mundo real. Dado sua experiência, é possível que essa ISO funcione também para sistemas de produção (manufatura) conectados?

   a. Sim ( )
   b. Sim com adaptações ( )
   c. Não ( )

5- A ISO 27000, voltada à segurança da informação, tem suas bases no gerenciamento da qualidade (ciclo PDCA de Deming). Em sua opinião, os princípios da qualidade (como foco no cliente, liderança, engajamento dos colaboradores, abordagem por processos, abordagem sistêmica para gestão, melhoria contínua, tomada de decisão baseada em evidências, manutenção de uma relação de benefício mútuo com o fornecedor) influenciam a gestão de sistemas de cibersegurança nas organizações?

   a. Totalmente ( )
   b. Parcialmente ( )
   c. Pouco ( )

6- Na sua percepção, as organizações que possuem sistemas de gestão da qualidade como a ISO 9000, contribuem com que grau para os sistemas de cibersegurança.

   a. Totalmente ( )
   b. Parcialmente ( )
   c. Pouco ( )

7- Na sua percepção, com que grau a ausência de um sistema de questão da qualidade nas organizações afeta a cibersegurança?

   a. Nenhum ( )
   b. Pouco ( )
   c. Bastante ( )

8- Na sua percepção, com que grau as Legislações brasileiras atuais contribuem para fortalecer os sistemas de cibersegurança das organizações?

   a. Totalmente ( )
   b. Parcialmente ( )
   c. Pouco ( )

9- Assinale a seguir, na sua percepção, o grau com que as medidas listadas a seguir apoiam a prevenção de ciberataques.

Implementação de *frameworks* e garantia de conformidade com normas e regulamentações de segurança (ex.: ISO 27001, MITRE ATT&CK)	Totalmente ( ) Parcialmente ( ) Pouco ( )
Uso de ferramentas de monitoramento contínuo e inteligência artificial para detecção de ameaças	Totalmente ( ) Parcialmente ( ) Pouco ( )
Atualização constante de sistemas e ferramentas de segurança	Totalmente ( ) Parcialmente ( ) Pouco ( )
Realização de testes e auditorias regulares para identificar vulnerabilidades	Totalmente ( ) Parcialmente ( ) Pouco ( )

10- Assinale, dado sua experiência, com que frequência você lida com esses tipos de ataques.

Phishing e suas variações	muito frequente ( ) pouco frequente ( ) nenhum ( )
Ransomware	muito frequente ( ) pouco frequente ( ) nenhum ( )
DoS/DDoS	muito frequente ( ) pouco frequente ( ) nenhum ( )
Quebra de senhas	muito frequente ( ) pouco frequente ( ) nenhum ( )

11- Em sua percepção, qual é o potencial do uso do monitoramento estatístico para avaliar a sustentabilidade dos sistemas de cibersegurança?

a. Alto potencial ( )
b. Potencial moderado ( )
c. Baixo potencial ( )
d. Não tenho conhecimento suficiente para opinar ( )

12- Abaixo estão listadas soluções de segurança comumente utilizadas para detectar ciberataques. Para cada solução, selecione os métodos que podem auxiliar na sua aplicação para detectar ciberataques.

	Métodos Estatísticos Multivariados	Modelos de *Machine Learning*	Modelos de *deep learning*	Inteligência Artifical	Modelos de redes neurais	Controle Estatístico do Processo
a. Detecção de comportamento anômalo						
b. Antivírus						
c. Ferramentas de monitoramento de *logs* e eventos						
d. *Firewall*						
e. sistemas de autenticação multifatorial (MFA)						

13- Você conhece ou já participou de algum projeto envolvendo o uso de *Machine Learning*, IA, demais técnicas de *deep learning* na cibersegurança?

a. Conheço projetos e aplicação, mas não participei ( )
b. Conheço e participei parcialmente ( )
c. Conheço e coordenei o projeto ( )
d. Desconheço ( )

14- Na tabela abaixo são listadas as ferramentas de classificação de risco, assinale aquelas que você já aplicou e indique o grau de importância para a cibersegurança, de acordo com a sua percepção.

	Você aplicou	Grau de importância
a. Análise qualitativa e quantitativa de riscos	Sim ( ) Não ( )	1 ( ) 2 ( ) 3 ( )
b. Sistemas de pontuação de vulnerabilidades	Sim ( ) Não ( )	1 ( ) 2 ( ) 3 ( )
c. Gestão de risco	Sim ( ) Não ( )	1 ( ) 2 ( ) 3 ( )
d. Avaliação de vulnerabilidades	Sim ( ) Não ( )	1 ( ) 2 ( ) 3 ( )

15- A seguir, estão listados desafios comuns na aplicação de métodos e técnicas estatísticas em segurança cibernética. Avalie cada item com uma escala de 1 a 3, em que 1 é “pouco desafiador” e 3 é “muito desafiador”:

Desconhecimento sobre o tema	1 ( ) 2 ( ) 3 ( )
Coleta e tratamento de grandes volumes de dados em tempo real	1 ( ) 2 ( ) 3 ( )
Complexidade na interpretação de resultados estatísticos	1 ( ) 2 ( ) 3 ( )
Complexidade na integração de métodos estatísticos com sistemas de segurança já existentes	1 ( ) 2 ( ) 3 ( )
Alta taxa de falsos positivos e negativos nos modelos de detecção	1 ( ) 2 ( ) 3 ( )
Adaptação dos modelos estatísticos a novos tipos de ataques e padrões de comportamento	1 ( ) 2 ( ) 3 ( )

16- Assinale o grau de criticidade dos desafios enfrentados pelas organizações para melhorar continuamente seus sistemas de proteção contra ataques *hackers*. Avalie cada item de 1 a 3, sendo 1 "pouco crítico" e 3 "muito crítico":

Rápida evolução dos ataques	1 ( ) 2 ( ) 3 ( )
Insuficiência de investimento/recursos	1 ( ) 2 ( ) 3 ( )
Baixa valorização da área de cibersegurança	1 ( ) 2 ( ) 3 ( )
Falta de planejamento adequado	1 ( ) 2 ( ) 3 ( )
Treinamento inadequado do pessoal da organização como um todo	1 ( ) 2 ( ) 3 ( )
Alta burocracia e falta de comunicação entre o setor de cibersegurança e demais áreas da organização	1 ( ) 2 ( ) 3 ( )
Cultura desatenta a cibersegurança	1 ( ) 2 ( ) 3 ( )

ENCERRAMENTO:

Estamos agora chegando ao fim do questionário. Considerando todos os temas discutidos até agora, o senhor(a) gostaria de fazer alguma outra consideração que considere relevante para o tema? Gostaria de agradecê-lo(a) por sua participação.

APÊNDICE B

Autores	Título	Ano
Emran; Ye	*Robustness of Chi-square and Canberra distance metrics for computer intrusion detection*	(2002)
Ye; Borror; Zhang	*EWMA techniques for computer intrusion detection through anomalous changes in event intensity*	(2002)
Ye; Emran; Chen; Vilbert	*Multivariate statistical analysis of audit trails for host-based intrusion detection*	(2002)
Wu; Mahadik; Reeves	*A summary of detection of denial-of-QoS attacks on DiffServ networks*	(2003)
Ye; Borror; Parmar	*Scalable Chi-Square Distance versus Conventional Statistical Distance for Process Monitoring with Uncorrelated Data Variables*	(2003)
Vinikka; Debar	*Monitoring IDS background noise using EWMA control charts and alert information*	(2004)
Cisar; Cisar	*Quality control in function of statistical anomaly detection in intrusion detection systems*	(2006)
Cisar; Cisar	*EWMA Statistic in Adaptive Threshold Algorithm*	(2007)
Hagedorn; Honda; Peterson	*Process control security journey*	(2007)
Ye; Chen	*Attack-norm separation for detecting attack-induced quality problems on computers and networks*	(2007)
Zhang; Zhu; Jin	*SVC-based multivariate control charts for automatic anomaly detection in computer networks*	(2007)
Cisar; Cisar	*Optimized EWMA control charts in function of intrusion detection*	(2008)
Amin; Siddiqui; Hong; Lee	*RIDES: Robust intrusion detection system for IP-based Ubiquitous Sensor Networks*	(2009)
Nadeem; Howarth	*Adaptive intrusion detection and prevention of denial of service attacks in MANETs*	(2009)
Cisar; Bosnjak; Cisar	*EWMA algorithm in network practice*	(2010)
Kim; Im; Park	*DSS for computer security incident response applying CBR and collaborative response*	(2010)
Deuerlein; Wolters; Meyer-Harries; Simpson	*Graph decomposition in risk analysis and sensor placement for water distribution network security*	(2012)
Mujtaba; Nanda; He	*Border gateway protocol anomaly detection using failure quality control method*	(2012)
Kuhl; Wiener; Krauß	*Multisensorial self-learning systems for quality monitoring of carbon fiber composites in aircraft production*	(2013)

Dromard; Khatoun; Khoukhi	*Adaptive CUSUM algorithm to detect malicious behaviors in wireless mesh networks*	(2014)
Molnar; Grossmann	*CRSTIP - An assessment scheme for security assessment processes*	(2014)
Raisinghani	*Can total quality management exist in cyber security: Is it present? Are we safe?*	(2014)
Wells; Camelio; Williams; White	*Cyber-physical security challenges in manufacturing systems*	(2014)
Basicevic; Ocovaj; Popovic	*Evaluation of entropy-based detection of outbound denial-of-service attacks in edge networks*	(2015)
Khan; Cui	*Statistical process control based chart for information systems security*	(2015)
Mohan; Khurana	*Implementing cyber security requirements and mechanisms in microgrids*	(2015)
Vincent; Wells; Tarazaga; Camelio	*Trojan Detection and Side-channel Analyses for Cyber-security in Cyber-physical Manufacturing Systems*	(2015)
Bouyeddou; Harrou; San; Kadri	*Detecting SYN flood attacks via statistical monitoring charts: A comparative study*	(2017)
Callegari; Giordano; Pagano	*Anomaly detection: An overview of selected methods*	(2017)
Haider; Hu; Slay; Turnbull; Xie	*Generating realistic intrusion detection system dataset based on fuzzy qualitative modeling*	(2017)
Sklavounos; Edoh; Plytas	*A Statistical Approach Based on EWMA and CUSUM Control Charts for R2L Intrusion Detection*	(2017)
Xian; Wang; Liu	*A nonparametric adaptive sampling strategy for online monitoring of big data streams*	(2017)
Ahsan; Mashuri; Khusna	*Intrusion detection system using bootstrap resampling approach of T^2 control chart based on successive difference covariance matrix*	(2018a)
Ahsan; Mashuri; Kuswanto; Prastyo	*Intrusion detection system using multivariate control chart Hotelling's T2 based on PCA*	(2018b)
Ahsan; Mashuri; Kuswanto; Prastyo; Khusna	*T^2 Control Chart based on Successive Difference Covariance Matrix for Intrusion Detection System*	(2018c)
Ashan; Mashuri; Khusna	*Hybrid James-Stein and successive difference covariance matrix estimators based hotelling's T^2 chart for network anomaly detection using bootstrap*	(2018d)
Leite; Mantovani	*Detecting and locating non-technical losses in modern distribution networks*	(2018)
Ransewa; Elz; Thanon; Intajag	*Anomaly detection using source port data with shannon entropy and EWMA control chart*	(2018)

Zineddine	*Optimizing security and quality of service in a real-time operating system using multi-objective Bat algorithm*	(2018)
Ahanger; Tariq; Nusir	*Real-Time Methodology for Improving Cyber Security in Internet of Things Using Edge Computing during Attack Threats*	(2019)
Ahsan; Mashuri; Kuswanto; Prastyo; Khusna	*Multivariate T2 control chart based on james-Stein and successive difference covariance matrix estimators for intrusion detection*	(2019)
Elhabashy; Wells; Camelio; Woodall	*A cyber-physical attack taxonomy for production systems: a quality control perspective*	(2019)
Li; Shi; Li	*Research on secure control and communication for cyber-physical systems under cyber-attacks*	(2019)
Nguyen; Nguyen; Tran; Truong; Phung; Nguyen; Le; Tran	*One-sided synthetic-RZ control charts: A new method for anomaly detection*	(2019)
Shafae; Wells; Purdy	*Defending against product-oriented cyber-physical attacks on machining systems*	(2019)
Sundararajan; Khan; Moghadasi; Sarwat	*Survey on synchrophasor data quality and cybersecurity challenges, and evaluation of their interdependencies*	(2019)
Wang; Li; Tang; Ni	*Source-Load Coordinated Reserve Allocation Strategy Considering Cyber-Attack Risks*	(2019)
Ahsan; Mashuri; Lee; Kuswanto; Prastyo	*Robust adaptive multivariate Hotelling's T2 control chart based on kernel density estimation for intrusion detection system*	(2020)
Aleksandrova; Vasiliev; Aleksandrov	*Problems of implementing information security management systems*	(2020)
Chan; Tan; Teo; Kow	*Vulnerability assessments of building management systems*	(2020)
Chen; Wang	*Quickest attack detection in smart grid based on sequential Monte Carlo filtering*	(2020)
Elhabashy; Wells; Camelio	*Cyber-physical attack vulnerabilities in manufacturing quality control tools*	(2020)
Guo; Ji; Wang; Yu; Min; Li	*Unsupervised Anomaly Detection in IoT Systems for Smart Cities*	(2020)
Kolosok; Gurina	*Monitoring and analysis of SCADA and WAMS data for EPS digitalization*	(2020)
Mahan; Menold	*Simulating cyber-physical systems: Identifying vulnerabilities for design and manufacturing through simulated additive manufacturing environments*	(2020)
Ravikumar; Hyder; Govindarasu	*Hardware-in-the-loop CPS security architecture for der monitoring and control applications*	(2020)

Sunny; Sheikh; Wagh	*Application of Dynamic Mode Decomposition for Temperature Analysis in Smart Building*	(2020)
Wurzenberger; Höld; Landauer; Skopik; Kastner	*Creating Character-based Templates for Log Data to Enable Security Event Classification*	(2020)
Alghassab	*Analyzing the impact of cybersecurity on monitoring and control systems in the energy sector*	(2021)
Ben Hamida; Hmida; Borgi; Rukoz	*Adaptive sampling for active learning with genetic programming*	(2021)
Brentan; Rezende; Barros; Meirelles; Luvizotto; Izquierdo	*Cyber-attack detection in water distribution systems based on blind sources separation technique*	(2021)
Elhabashy; Dastoorian; Wells; Camelio	*Random sampling strategies for multivariate statistical process control to detect cyber-physical manufacturing attacks*	(2021)
Hazrati-Marangaloo; Noorossana	*A nonparametric change detection approach in social networks*	(2021)
Kotenko; Parashchuk	*Specification of Quality Indicators for Security Event and Incident Management in the Supply Chain*	(2021)
Liang; Wu; Li; Chen; Tong; Ni	*Security Risk Analysis of Active Distribution Networks with Large-Scale Controllable Loads under Malicious Attacks*	(2021)
Mashuri; Ahsan; Kuswanto; Prastyo; Khusna; Wibawati	*Comparing the performance of T^2 chart based on PCA Mix, Kernel PCA Mix, and Mixed Kernel PCA for Network Anomaly Detection*	(2021)
Rodríguez Martínez; Quiñones-Grueiro; Verde; Llanes-Santiago	*A Novel Approach for Detection and Location of Cyber-Attacks in Water Distribution Networks*	(2021)
Zhou; Liu; Tian; Kan;	*Echo State Network Learning for the Detection of Cyber Attacks in Additive Manufacturing*	(2021)
Alsulami	*Implementation analysis of reliable unmanned aerial vehicles models for security against cyber-crimes: Attacks, tracebacks, forensics and solutions*	(2022)
Frankó; Hollosi; Ficzere; Varga	*Applied Machine Learning for IIoT and Smart Production-Methods to Improve Production Quality, Safety and Sustainability*	(2022)
Gaber; El-Ghamry; Hassanien	*Injection attack detection using machine learning for smart IoT applications*	(2022)
Jiang; Liu; Liu; Ren; Wang; Bao; Wang	*An Enhanced EWMA for Alert Reduction and Situation Awareness in Industrial Control Networks*	(2022)
Kotenko; Gaifulina; Zelichenok	*Systematic Literature Review of Security Event Correlation Methods*	(2022)
Li; Wang; Lee; Jin	*Monitoring Runtime Metrics of Fog Manufacturing via a Qualitative and Quantitative (QQ) Control Chart*	(2022)

Meng; Wang; Ma; Luo; Li; Zhang	*Packet Representation Learning for Traffic Classification*	(2022)
Shaohui; Tuerhong; Wushouer; Yibulayin	*PCA mix-based Hotelling's T² multivariate control charts for intrusion detection system*	(2022)
Rahman; Shafae	*Physics-based detection of cyber-attacks in manufacturing systems: A machining case study*	(2022)
Saha; Priyoti; Sharma; Haque	*Towards an Optimized Ensemble Feature Selection for DDoS Detection Using Both Supervised and Unsupervised Method*	(2022)
Sen; Van der Velde; Lühman; Sprünken; Hacker; Ulbig; Andres; Henze	*On using contextual correlation to detect multi-stage cyber attacks in smart grids*	(2022)
Sarhan; Layeghy; Portmann	*Towards a Standard Feature Set for Network Intrusion Detection System Datasets*	(2022)
Yang; Chen; Zhang; Paynabar	*Online detection of cyber-incidents in additive manufacturing systems via analyzing multimedia signals*	(2022)
Zhang; Ye	*Cyber-Attack Detection for Active Neutral Point Clamped (ANPC) Photovoltaic (PV) Converter using Kalman Filter*	(2022)
Agyepong; Cherdantseva; Reinecke; Burnap	*A systematic method for measuring the performance of a cyber security operations centre analyst*	(2023)
Ahsan; Khusna; Wibawati; Lee	*Support vector data description with kernel density estimation (SVDD-KDE) control chart for network intrusion monitoring*	(2023)
Ali; Khan; Driss; Ahmad; Buchanan; Pitropakis	*CellSecure: Securing Image Data in Industrial Internet-of-Things via Cellular Automata and Chaos-Based Encryption*	(2023)
Cavdar; Sahin; Sesli; Akyazi; Nuroglu	*Cascaded fractional order automatic generation control of a PV-reheat thermal power system under a comprehensive nonlinearity effect and cyber-attack*	(2023)
Fahmy; Alsuhli; Khattab;	*Optimizing Environment-aware VANET Clustering using Machine Learning*	(2023)
Farooq; Shahid; Gui; Olsen	*Impact of cyber-attack on coordinated voltage control in low voltage grids*	(2023)
Husák; Sokol; Žádník; Bartoš; Horák	*Lessons Learned from Automated Sharing of Intrusion Detection Alerts: The Case of the SABU Platform*	(2023)
Lim; Lee	*Improved control chart for statistical process control using combined X and delayed EWMA statistics*	(2023)
Mohy-Eddine; Guezzaz; Azrour	*An efficient network intrusion detection model for IoT security using K-NN classifier and feature selection*	(2023)
Poonawala; Sonawane; Lodha; Gohokar; Askhedkar; Danve	*LoRa-Based Farm Monitoring System*	(2023)

Rodrigues-Martinez; Quiñones-Grueiro; Llanes-Santiago	*Cyberattack Diagnosis in Water Distribution Networks Combining Data-Driven and Structural Analysis Methods*	(2023)
Vellingiri; Kalaivanan; Gopinath; Gobinath; Prabhakar; Sarathkumar	*Strategies for classifying water quality in the Cauvery River using a federated learning technique*	(2023)
Xiao; Wang; Qin; Bauer	*Virtual Impedance Control for Load Sharing and Bus Voltage Quality Improvement*	(2023)
Ye; Liu; Kan	*Stereo Vision enabled Flexible In-situ Process Authentication of Additive*	(2023)
Zhang; Dong; Shi; Chen; Guan	*Distributed Observer-Based Event-Triggered Load Frequency Control of Multiarea Power Systems Under Cyber Attacks*	(2023)
Zhang; Lee	*Kinematic Control of Serial Manipulators Under False Data Injection Attack*	(2023)
Abbas; Ibrahim	*Fortifying IoT Infrastructure Using Machine Learning for DDoS Attack within Distributed Computing-based Routing in Networks*	(2024)
Cai; Shi; Sun; Wen; Yan	*Fuzzy Memory Controller Design Based-Machine Learning Algorithm and Stability Analysis for Nonlinear NCSs Under Asynchronous Cyber Attacks*	(2024)
Hu; Ye; Song	*Vulnerability Assessments of Induction Machine-Based Multistage Rolling Mill System Under Sensor Integrity Attacks*	(2024)
Tsai; Wang; Chang; Tong	*Using WPCA and EWMA Control Chart to Construct a Network Intrusion Detection Model*	(2024)
Vitorino; Silva; Maia; Praça	*Reliable feature selection for adversarially robust cyber-attack detection*	(2024)
Xiao; Wang; Bauer; Qin	*Virtual Impedance Control for Load Sharing and Bus Voltage Quality Improvement in Low Voltage AC Microgrid*	(2024)
Zhong; Wen; Hopko; Karthikeyan; Pagilla; Mehta; Bukkapatnam	*Detecting Anomalous Robot Motion in Collaborative Robotic Manufacturing Systems*	(2024)

APÊNDICE C

Autores	Nº de trabalhos publicados	Ano de publicação	Autores	Nº de trabalhos publicados	Ano de publicação
Ashan M	9	2018; 2019; 2020; 2021; 2023	Yibulayin T	2	2022
Mashuri M	8	2018; 2019; 2020; 2021	Ye J	2	2022; 2024
Khusna H	7	2018; 2019; 2020; 2021; 2023	Zhang Y	2	2002; 2022
Kuswanto H	6	2018; 2019; 2020; 2021	Alsulami H	1	2022
Prastyo D	6	2018; 2019; 2020; 2021	Alsuhli G	1	2023
Wells L	6	2014; 2015; 2019; 2020; 2021	Amin S	1	2009
Camelio J	5	2014; 2015; 2019; 2020; 2021	Andres M	1	2022
Ye N	5	2002; 2003; 2007	Abbas S	1	2024
Elhabshy A	3	2019; 2020; 2021	Agyepong E	1	2023
Cisar P	3	2006; 2008; 2010	Ahanger T	1	2019
Cisar S	3	2006; 2008; 2010	Ahmad J	1	2023
Bauer P	2	2023; 2024	Akyazi O	1	2023
Borror C	2	2002; 2003	Aleksandrov M	1	2020
Chen Q	2	2002; 2007	Aleksandrova S	1	2020
Emran S	2	2002	Ali H	1	2023
Kan C	2	2021; 2023	Alghassab M	1	2021
Kotenko I	2	2021; 2022	Azrour M	1	2023
Lee S	2	2009; 2023	Bao Y	1	2022
Lee M	2	2020; 2023	Barros D	1	2021
Li Y	2	2019; 2022	Bartoš V	1	2023
Liu C	2	2021; 2023	Basicevic I	1	2015
Llanes-Santiago O	2	2021; 2023	Ben H S	1	2021
Ni M	2	2019; 2021	Benkirane S	1	2023
Qin Z	2	2023; 2024	Borgi A	1	2021
Quiñones-Grueiro M	2	2021; 2023	Bouyeddou B	1	2017
Rodríguez-Martínez C	2	2021; 2023	Bošnjak S	1	2010
Shafae M	2	2019; 2022	Brentan B	1	2021
Tran K	2	2019	Buchanan W	1	2023
Tuerhong G	2	2022	Bukkapatnam S	1	2024
Wang L	2	2023; 2024	Burnap P	1	2023
Wang Q	2	2019; 2020	Cai X	1	2024
Wang Y	2	2022	Caldeira F	1	2023
Wibawati	2	2021; 2023	Callegari C	1	2017
Wushouer M	2	2022	Cavdar B	1	2023
Xiao J	2	2023; 2024	Chan R	1	2020

Chang Y	1	2024	Hu K	1	2024
Chen G	1	2023	Husák M	1	2023
Chen J	1	2022	Hyder B	1	2020
Chen L	1	2020	Höld G	1	2020
Chen X	1	2021	Hopko S	1	2024
Cherdantseva Y	1	2023	Ibrahim A	1	2024
Cruz T	1	2023	Im K	1	2010
Cui L	1	2015	Intajag S	1	2018
Dastoorian R	1	2021	Izquierdo J	1	2021
Debar H	1	2004	Ji T	1	2020
Deuerlein J	1	2012	Jiang B	1	2022
Dong S	1	2023	Jin J	1	2007
Driss M	1	2023	Jin R	1	2022
Dromard J	1	2014	Kadri B	1	2017
Edoh A	1	2017	Kalaivanan K	1	2023
El-Ghamry A	1	2022	Kastner W	1	2020
Elz N	1	2018	Khan M	1	2015
Fahmy Y	1	2023	Khan M	1	2023
Farooq A	1	2023	Khan T	1	2019
Ficzere D	1	2022	Karthikeyan A	1	2024
Frankó A	1	2022	Khatoun R	1	2014
Gaber T	1	2022	Khattab A	1	2023
Gaifulina D	1	2022	Khoukhi L	1	2014
Giordano S	1	2017	Khurana H	1	2015
Gobinath C	1	2023	Kim H	1	2010
Gopinath M	1	2023	Kolosok I	1	2020
Govindarasu M	1	2020	Kow B	1	2020
Grossmann J	1	2014	Krauß M	1	2013
Guan X	1	2023	Kuhl M	1	2013
Guezzaz A	1	2023	Landauer M	1	2020
Gui Y	1	2023	Layeghy S	1	2022
Guo Y	1	2020	Le T	1	2019
Gurina L	1	2020	Lee D	1	2022
Hacker I	1	2022	Leite J	1	2018
Hagedorn D	1	2007	Li J	1	2021
Haider W	1	2017	Li M	1	2019
Haque A	1	2022	Li P	1	2020
Harrou F	1	2017	Li S	1	2023
Hassanien A	1	2022	Li W	1	2019
Hazrati-Marangaloo H	1	2021	Li X	1	2022
He X	1	2012	Liang J	1	2021
Henriques J	1	2023	Lim J	1	2023
Henze M	1	2022	Liu H	1	2022
Hmida H	1	2021	Liu K	1	2017
Hollósi G	1	2022	Liu Y	1	2022
Honda B	1	2007	Lodha M	1	2023
Hong C	1	2009	Luo H	1	2022
Horák M	1	2023	Luvizotto E	1	2021
Howarth M	1	2009	Lühman M	1	2022
Hu J	1	2017	Ma R	1	2022

Mahadik V	1	2003	Rukoz M	1	2021
Mahan T	1	2020	Saha S	1	2022
Maia E	1	2024	Sahin E	1	2023
Mantovani J	1	2018	Sarhan M	1	2022
Mehta R	1	2024	Sarwat A	1	2019
Meirelles G	1	2021	Sen Ö	1	2022
Meng X	1	2022	Sesli E	1	2023
Menold J	1	2020	Shahid K	1	2023
Meyer-Harries L	1	2012	Shaohui M	1	2022
Min G	1	2020	Sharma A	1	2022
Mo S	1	2022	Sheikh A	1	2020
Moghadasi A	1	2019	Shi K	1	2024
Mohan A	1	2015	Shi P	1	2023
Mohy-eddine	1	2023	Shi Y	1	2019
Molnar A	1	2014	Siddiqui M	1	2009
Mujtaba M	1	2012	Simões P	1	2023
Nadeem A	1	2009	Simpson A	1	2012
Nanda P	1	2012	Silva M	1	2024
Nguyen H	1	2019	Sklavounos D	1	2017
Nguyen L	1	2019	Skopik F	1	2020
Nguyen T	1	2019	Slay J	1	2017
Noorossana R	1	2021	Song W	1	2024
Nuroglu F	1	2023	Sonawane A	1	2023
Nusir M	1	2019	Sokol P	1	2023
Ocovaj S	1	2015	Sprünken F	1	2022
Olsen R	1	2023	Subramaniam P	1	2023
Pagano M	1	2017	Sun Y	1	2024
Pagilla P	1	2024	Sun Y	1	2017
Parashchuk I	1	2021	Sundararajan A	1	2019
Park S	1	2010	Sunny K	1	2020
Parmar D	1	2003	Tan F	1	2020
Paynabar K	1	2022	Tang Y	1	2019
Peterson D	1	2007	Tarazaga P	1	2015
Phung K	1	2019	Tariq U	1	2019
Pitropakis N	1	2023	Teo U	1	2020
Plytas M	1	2017	Thanon N	1	2018
Poonawala M	1	2023	Tian W	1	2021
Popovic M	1	2015	Tong H	1	2021
Portmann M	1	2022	Tong L	1	2024
Praça I	1	2024	Truong T	1	2019
Priyoti A	1	2022	Tsai Y	1	2024
Purdy G	1	2019	Turnbull B	1	2017
Rahman M	1	2022	Ulbig A	1	2022
Raisinghani M	1	2014	Van D V D	1	2022
Rangarajan S	1	2023	Varga P	1	2022
Ransewa S	1	2018	Vasiliev V	1	2020
Ravikumar G	1	2020	Vellingiri J	1	2023
Reeves D	1	2003	Verde C	1	2021
Reinecke P	1	2023	Viinikka J	1	2004
Ren Z	1	2022	Vilbert S	1	2002
Vincent H	1	2015			

Rezende P	1	2021
Vitorino J	1	2024
Wagh S	1	2020
Wang A	1	2017
Wang C	1	2024
Wang L	1	2022
Wang W	1	2022
Wang X	1	2020
White J	1	2014
Wen S	1	2024
Wen Y	1	2024
Wiener T	1	2021
Williams C	1	2014
Wolters A	1	2012
Woodall W	1	2019
Wu X	1	2003
Wu Y	1	2021
Wurzenberger M	1	2020
Xian X	1	2017
Xie Y	1	2024
Xie Y	1	2017
Yan H	1	2024
Yang W	1	2022
Ye Z	1	2023
Yu L	1	2020
Žádník	1	2023
Zelichenok I	1	2022
Zhang C	1	2022
Zhang J	1	2022
Zhang M	1	2023
Zhang Y	1	2023
Zhang Z	1	2007
Zhou H	1	2021
Zhong Y	1	2024
Zhu X	1	2007
Zineddine M	1	2018

ANEXO A

Seções	Objetivos de controle
Política de segurança da informação	Estabelecer política de segurança da informação; Revisão das políticas de segurança da informação.
Organização da segurança da informação	• Organização interna: Papéis e responsabilidades da segurança da informação; Segregação de funções; Contato com autoridades; Contato com grupos especiais de interesse; Segurança da informação na gestão de projetos. • Dispositivos móveis e trabalho remoto: Política de uso de dispositivos móveis; Trabalho remoto.
Gerenciamento de ativos	• Responsabilidade pelos ativos: Inventário de ativos; Propriedade dos ativos; Uso aceitável de ativos; Devolução de ativos. • Classificação da informação: Classificação da informação; Rotulagem da informação; Tratamento da informação. • Manuseio de mídia: Gestão de mídia removível; Descarte de mídia; Transferência física de mídia.
Segurança de recursos humanos	• Antes do emprego: Triagem; Termos e condições de emprego. • Durante o emprego: Responsabilidades de gestão; Conscientização, educação e treinamento em segurança da informação; Processo disciplinar. • Encerramento e mudança de emprego: Responsabilidades no encerramento ou mudança de emprego.
Controle de acesso	• Requisitos de controle de acesso: Política de controle de acesso; Acesso a redes e serviços de rede. • Gestão de acesso do usuário: Registro e cancelamento de usuários; Gestão de direitos de acesso privilegiado; Gestão de direitos de acesso de usuários; Revisão dos direitos de acesso de usuários; Remoção ou ajuste de direitos de acesso. • Responsabilidades do usuário: Uso de senhas; Uso de dispositivos de autenticação. • Controle de acesso ao sistema e à aplicação: Restrição de acesso à informação;

	Procedimentos seguros de login; Sistema de gestão de senhas; Uso de programas utilitários privilegiados; Controle de acesso ao código-fonte do programa.
Criptografia	• Controles criptográficos: Política de uso de controles criptográficos; Gestão de chaves.
Segurança física e ambiental	• Áreas seguras: Perímetro de segurança física; Controles de entrada física; Escritórios, salas e instalações de segurança; Proteção contra ameaças externas e ambientais; Trabalhando em áreas seguras; Áreas de carga e descarga. • Segurança do equipamento: Colocação e proteção de equipamentos; Utilidades de suporte; Segurança do cabeamento; Manutenção de equipamentos; Remoção de ativos; Segurança de equipamentos e ativos fora do local; Reutilização ou descarte seguro de equipamentos; Equipamentos de usuários.
Segurança operacional	• Procedimentos e responsabilidades operacionais: Documentação de procedimentos operacionais; Gestão de mudanças; Capacidade de gestão; Separação dos ambientes de desenvolvimento, teste e operação. • Proteção contra *malware*: Controles contra *malware*. • *Backup*: Cópia de segurança da informação. • Registro e monitoramento: Registro de eventos; Proteção das informações de registro; Registros de administrador e operador; Sincronização do relógio. • Controle de *software* operacional: Instalação de *software* em sistemas operacionais. • Gestão de vulnerabilidades técnicas: Gestão de vulnerabilidades técnicas.
Segurança de comunicações	• Gestão da segurança das redes: Controles de redes; Segurança de serviços de rede. • Troca de informações: Políticas e procedimentos para troca de informações; Acordos sobre transferência de informações; Mensagens eletrônicas; Confidencialidade ou acordos de não divulgação.
Aquisição, desenvolvimento e	• Requisitos de segurança da informação para sistemas de informação: Análise e especificação de requisitos de segurança da informação; Tratamento da segurança da informação nas especificações de requisitos;

manutenção dos sistemas de informação	Segregação do ambiente de desenvolvimento, teste e produção. • Segurança nos processos de desenvolvimento e suporte: Políticas de segurança para desenvolvimento de sistemas; Procedimentos de controle de mudanças no sistema; Revisão técnica das aplicações após mudanças no sistema operacional; Restrições em mudanças de pacotes de *software*; Princípios de engenharia de sistemas seguros; Ambiente de desenvolvimento seguro; Desenvolvimento terceirizado; Teste de segurança de sistemas. • Teste de segurança dos sistemas: Teste de segurança dos sistemas.
Relacionamento com fornecedores	• Segurança da informação em relações com fornecedores: Política de segurança da informação na gestão de fornecedores; Segurança da informação em acordos com fornecedores; Monitoramento e revisão de serviços de fornecedores. • Gestão da entrega de serviços pelo fornecedor: Monitoramento e revisão dos serviços de fornecedores; Gestão de mudanças nos serviços prestados por fornecedores.
Gestão de incidentes de segurança da informação	• Gestão de incidentes e melhorias de segurança da informação: Responsabilidades e procedimentos; Relatório de eventos de segurança da informação; Relatório de fraquezas de segurança da informação; Avaliação e decisão sobre incidentes de segurança da informação; Resposta a incidentes de segurança da informação; Aprendizado com incidentes de segurança da informação; Coleta de evidências.
Segurança da Informação na Gestão da Continuidade do Negócio	• Continuidade da segurança da informação: Planejamento da continuidade da segurança da informação; Implementação da continuidade da segurança da informação; Verificação, revisão e avaliação da continuidade da segurança da informação. • Redundâncias: Disponibilidade dos sistemas de informação.
Conformidade	• Conformidade com requisitos legais e contratuais: Identificação da legislação aplicável e requisitos contratuais; Direitos de propriedade intelectual; Proteção de registros; Privacidade e proteção de dados pessoais; Regulamentação de controles criptográficos. • Revisões de segurança da informação: Revisão independente da segurança da informação; Conformidade com políticas e normas de segurança da informação; Revisão técnica da conformidade.