CESAR *FRAMEWORK* PARA GESTÃO INTEGRADA DE CIBERRISCO E SEGURANÇA OPERACIONAL NA AVIAÇÃO CIVIL

Integração ISMS-SMS através de Inteligência Artificial Explicável para Conformidade com EASA Part-IS

Mestrado em Gestão de Sistemas e Tecnologia da Informação

(Dissertação de Mestrado)

2025

Elaborado por

MARLENE SCHOR - nº 202130016

Orientadora: Professora Doutora Virgínia Maria Da Silva Araújo

Coorientadora: Professora Doutora Luísa Domingues

Barcarena

Novembro, 2025

ATLÂNTICA – INSTITUTO UNIVERSITÁRIO

CESAR *FRAMEWORK* PARA GESTÃO INTEGRADA DE CIBERRISCO E SEGURANÇA OPERACIONAL NA AVIAÇÃO CIVIL

Integração ISMS-SMS através de Inteligência Artificial Explicável para Conformidade com EASA Part-IS

Mestrado em Gestão de Sistemas e Tecnologia da Informação

(Dissertação de Mestrado)

2025

Elaborado por

MARLENE SCHOR - nº 202130016

Orientadora: Professora Doutora Virgínia Maria Da Silva Araújo

Coorientadora: Professora Doutora Luísa Domingues

Barcarena

Novembro, 2025

“Elevo os meus olhos para os montes: de onde me virá o socorro?

O meu socorro vem do Senhor que fez o céu e a terra.

Não deixará vacilar o teu pé: aquele que te guarda não tosquenejará.

Eis que não tosquenejará nem dormirá o guarda de Israel.

O senhor é quem te guarda: O Senhor é a tua sombra à tua direita.

O Sol não te molestará de dia nem a lua de noite.

O Senhor te guardará de todo o mal: ele guardará a tua alma.

O Senhor guardará a tua entrada e a tua saída, desde agora e para sempre.”

(Salmo 121)[1]

[1] *Sociedade Bíblica do Brasil. (2009)*. Bíblia Sagrada: Almeida Revista e Atualizada. *Sociedade Bíblica do Brasil.*

AGRADECIMENTOS

A Deus, pela Sua infinita misericórdia na minha vida. Nos momentos mais difíceis, foi o meu sustento e refúgio; nos momentos mais felizes, a Sua presença encheu o meu coração de alegria e gratidão.

Aos meus pais, que são os meus maiores exemplos de honestidade, determinação, coragem e resiliência, qualidades valiosas que moldaram o meu carácter. O apoio constante, deles, sempre foi fundamental para que eu seguisse em frente sem vacilar, acreditando que o impossível é apenas um lugar onde ninguém ainda chegou.

Aos meus filhos, que são o meu alicerce, a minha fundação e a minha coluna. Cada um deles surgiu num momento único da minha vida para me ensinar o verdadeiro valor do amor. A convivência com eles torna a minha vida mais leve e cheia de sentido. Ao meu filho Marcos, pela dedicação e cuidado constantes comigo; à minha filha Marlene, minha parceira de aventuras e longas conversas filosóficas; à minha filha Maila, cujo abraço tem o dom de curar a alma; à minha neta Júlia, o meu sol da primavera, que ilumina todos os meus dias; e aos meus genros Thiago e Elias, pelo carinho, apoio e presença sempre amorosa.

Aos meus irmãos, porque o amor entre irmãos é o laço invisível que mantém a família unida.

Ao meu melhor amigo, Marcos Justi, por ser o meu porto seguro e o maior incentivador dos meus estudos, sempre acreditando em mim mesmo quando eu duvidava.

Às minhas orientadoras, Prof.ª Doutora Virgínia Araújo e Prof.ª Doutora Luísa Domingues, pelos valiosos ensinamentos, pela dedicação e pela orientação rigorosa e generosa. A vossa ajuda foi essencial para a concretização deste trabalho.

A todos os professores do Mestrado em Gestão de Sistemas e Tecnologias da Informação, pelo conhecimento transmitido e pelo contributo para o meu crescimento académico e profissional

Aos meus antigos líderes e mentores profissionais, Eng.º Euclides Batalha e Cpt. Mário Alvim, pela amizade, incentivo e partilha de conhecimento ao longo da minha trajetória profissional.

A administração da Euroatlantic, que viabilizou esta oportunidade e os colegas pela colaboração, partilha de experiências e constante disponibilidade para o trabalho em equipa.

Por fim, um sincero obrigado a todos que, contribuíram para que esta jornada fosse possível.

LISTA DE ABREVIATURAS E SIGLAS

ACARS – *Aircraft Communications Addressing and Reporting System*

ACM – *Aircraft Condition Monitoring*

ACT / AI Act – *Artificial Intelligence Act* (Regulamento Europeu da IA)

ADS – *Automatic Dependent Surveillance*

AES – *Advanced Encryption Standard*

AI – *Artificial Intelligence /* Inteligência Artificial

AIAA – *American Institute of Aeronautics and Astronautics*

AMCs – *Acceptable Means of Compliance* (EASA)

ANAC – *Autoridade Nacional da Aviação Civil*

AP – *Access Point*

API – *Application Programming Interface*

ARINC – *Aeronautical Radio, Incorporated*

ASRS – *Aviation Safety Reporting System*

ATC – *Air Traffic Control*

ATCO – *Air Traffic Controller*

ATM – *Air Traffic Management*

BMJ – *Best Management Judgment*

BPMN – *Business Process Model and Notation*

BWM – *Best Worst Method*

CAMO – *Continuing Airworthiness Management Organization*

CANSO – *Civil Air Navigation Services Organization*

CAP – *Civil Aviation Publication*

CBM – *Condition-Based Maintenance*

CE – Comissão Europeia

CERT – *Computer Emergency Response Team*

CESAR – *Cyber-Safety Enhanced System for AI-based Risk Management*

CFO – *Chief Financial Officer*

CIA – *Confidentiality, Integrity, Availability*

CISO – *Chief Information Security Officer*

CNCS – *Centro Nacional de Cibersegurança*

CNN – *Convolutional Neural Network*

CNS – *Communication, Navigation and Surveillance*

COTS – *Commercial Off-The-Shelf*

CPS – *Cyber-Physical Systems*

CRI – *Cybersecurity Risk Indicator*

CSIRT – *Computer Security Incident Response Team*

CSRT – *Cybersecurity Response Team*

CVE – *Common Vulnerabilities and Exposures*

DDoS – *Distributed Denial of Service*

DEMATEL – *Decision-Making Trial and Evaluation Laboratory*

DL – *Deep Learning*

DO-326A – *Airworthiness Security Process Specification*

DoS – *Denial of Service*

DSR – *Design Science Research*

EAA – EuroAtlantic Airways

EASA – *European Union Aviation Safety Agency*

EASA Part-IS – *Information Security Regulation* (EU) 2023/203

ED – *Executive Director Decision* (EASA)

EDR – *Endpoint Detection and Response*

EFB – *Electronic Flight Bag*

ENISA – *European Union Agency for Cybersecurity*

ERP – *Emergency Response Plan / Enterprise Resource Planning*

EU – *European Union*

EUDR – *EU Deforestation Regulation*

EUROCONTROL – *European Organization for the Safety of Air Navigation*

FAA – *Federal Aviation Administration* (autoridade de aviação civil dos Estados Unidos)

FDM – *Flight Data Monitoring*

FMS – *Flight Management System*

GM – *Guidance Material*

GRC – *Governance, Risk and Compliance*

HEIMDAL – *Heimdal Security Platform*

IA – *Inteligência Artificial*

IATA – *International Air Transport Association*

ICAO – *International Civil Aviation Organization*

ICCA – *Integrated Cyber-Controlled Architecture*

IDS – *Intrusion Detection System*

IEC – *International Electrotechnical Commission*

IEEE – *Institute of Electrical and Electronics Engineers*

IOSA – *IATA Operational Safety Audit*

IoT – *Internet of Things*

IQSMS – *Integrated Quality & Safety Management System*

IR – *Incident Report*

ISAC – *Information Sharing and Analysis Center*

ISAP – *Information Security Assessment Process*

ISMM – *Information Security Maturity Model*

ISMS – *Information Security Management System*

ISO – *International Organization for Standardization*

IT – *Information Technology*

KPI – *Key Performance Indicator*

KSA – *Knowledge, Skills and Attitudes* (aviação)

LMS – *Learning Management System*

LSTM – *Long Short-Term Memory* (rede neural)

MHIL – *Master Hazard Identification Log*

MITRE ATT&CK – *Adversarial Tactics, Techniques & Common Knowledge*

ML – *Machine Learning*

MoC – *Management of Change*

NIS – *Network and Information Security Directive*

NIS2 – *Network and Information Security Directive* (versão 2)

NLP – *Natural Language Processing*

NVD – *National Vulnerability Database*

ODIN – *Operational Data Integration Network*

OPS – *Operations*

OT – *Operational Technology*

PDCA – *Plan–Do–Check–Act*

PDF – Portable Document Format

PRISMA – *Preferred Reporting Items for Systematic Reviews and Meta-Analyses*

PT – Portugal

QP1–QP5 – Questões de Pesquisa da dissertação

RBAC – *Role-Based Access Control*

RIL – *Risk Identification Log*

RL – *Reinforcement Learning*

RLS – *Risk Level Score*

RPN/RPV – *Risk Priority Number / Value*

RSL – *Risk Severity Level*

RSO – *Responsible Safety Officer*

SAP – *Safety Assessment Process*

SAT – *Security Awareness Training*

SDN – *Software-Defined Networking*

SIEM – *Security Information and Event Management*

SMS – *Safety Management System*

SOC – *Security Operations Center*

SoE – *State of Excellence*

SoK – *Systematization of Knowledge*

SVM – *Support Vector Machines*

SW – *Software*

TAP – Transportes Aéreos Portugueses

TCO – *Total Cost of Ownership*

TCP – *Transmission Control Protocol*

THOR – *Threat Oriented Resilience*

TI – Tecnologia da Informação

TISA – *Technical Information Security Assessment*

TLV – *Threshold Limit Value*

TM – *Technical Manual / Track Monitoring*

UAS – *Unmanned Aircraft System*

UCR – *Unclassified Cyber Report*

UE – União Europeia

UK – *United Kingdom*

USA – *United States of America*

UTM – *Unmanned Traffic Management*

VC – *Venture Capital*

VFR – *Visual Flight Rules*

VHF – *Very High Frequency*

XAI – *Explainable Artificial Intelligence*

XML – *Extensible Markup Language*

RESUMO

A aviação civil europeia enfrenta um desafio crítico, integrar a gestão de cibersegurança (ISMS) com a gestão de segurança operacional (SMS), conforme estabelecido pelo Regulamento EASA Part-IS (UE 2023/203). Este tema ganha relevância num contexto de digitalização crescente, no qual as ameaças cibernéticas intensificam as dependências entre sistemas de informação e processos de segurança operacional no setor aeronáutico. A investigação adota a metodologia *Design Science Research* e inicia-se com uma Revisão Sistemática da Literatura (PRISMA 2020), que analisou quarenta estudos publicados entre 2018 e 2025. Os resultados mostram que apenas 5% das publicações abordam o novo regulamento EASA Part-IS e 10% tratam a integração entre ISMS e SMS. Observa-se igualmente que sistemas de IA com desempenho médio de 92% em domínios isolados descem para 72% quando aplicados a contextos integrados, revelando limitações técnicas das abordagens existentes. Os contributos centrais incluem a proposta do modelo conceptual CESAR *Framework*, orientado à integração regulatória e alinhado aos requisitos IS.I.OR.200-260 e ao ICAO Anexo 19, incorporando inteligência artificial para apoiar a gestão de risco aeronáutico. Conclui-se que a integração ISMS-SMS carece ainda de instrumentos operacionais nos referenciais atuais e que a utilização de IA poderá apoiar esse processo, exigindo validação técnica em ambientes reais.

.

Palavras-chave: EASA Part-IS, *aviation cybersecurity*, *Explainable AI, risk Assessment, safety-security integration.*

Abstract

European civil aviation faces a critical challenge: integrating cybersecurity management (ISMS) with safety management System (SMS), as required by the EASA Part-IS Regulation (EU 2023/203). This issue gains relevance in the context of increasing digitalization, where cyber threats intensify the interdependence between information systems and safety processes within the aviation sector. The research adopts the Design Science Research methodology and begins with a Systematic Literature Review (PRISMA 2020), which analyzed forty studies published between 2018 and 2025. The results show that only 5% of the publications address the new EASA Part-IS regulation, and 10% examine ISMS–SMS integration. It is also observed that AI systems achieving an average performance of 92% in isolated domains drop to 72% when applied to integrated contexts, revealing technical limitations in existing approaches. The central contributions include the proposal of the CESAR Framework, a conceptual model oriented towards regulatory integration and aligned with the IS.I.OR.200-260 requirements and ICAO Annex 19, incorporating artificial intelligence to support aviation risk management. The study concludes that ISMS–SMS integration still lacks operational instruments within current regulatory references and that the use of AI may support this process, subject to technical validation in real operational environments.

.

Keywords: EASA Part-IS, aviation cybersecurity, Explainable AI, risk Assessment, safety-security integration.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

ÍNDICE DE GRÁFICOS

1. INTRODUÇÃO

1.1. Contextualização

A incorporação de tecnologias digitais na aviação, desde a gestão do tráfego aéreo até à manutenção preditiva e aos sistemas administrativos das companhias aéreas, transformou profundamente a forma como as operações são planeadas, executadas e monitorizadas. Contudo, esta interconectividade crescente trouxe novos desafios, nomeadamente o aumento exponencial da superfície de ataque cibernético (Lykou et al., 2019).

As ameaças cibernéticas no setor aeronáutico tornaram-se cada vez mais complexas, abrangendo desde ataques *ransomware* a infraestruturas aeroportuárias até à manipulação de dados de voo e interferências em comunicações aeronáuticas (*spoofing* e *jamming*) (Çevik & Akleylek, 2024). Estas ameaças não comprometem apenas a confidencialidade ou disponibilidade da informação, mas podem afetar diretamente a segurança operacional (*safety*), demonstrando a interdependência entre *safety* e *security*.

Reconhecendo a natureza transversal das ameaças cibernéticas, a Agência Europeia para a Segurança da Aviação (EASA) publicou os Regulamentos (UE) 2023/203 e (EU) 2022/1645, denominado EASA Part-IS, que estabelece requisitos obrigatórios de *Information Security Management System* para operadores aéreos, organizações de manutenção e fornecedores críticos. Paralelamente, a Diretiva (UE)2022/2555 (NIS2) reforça a resiliência cibernética dos setores críticos, incluindo o transporte aéreo, exigindo mecanismos de governação, gestão de risco e notificação de incidentes (UE 2023/203, 2023).

Apesar desses avanços regulatórios, observa-se que muitas organizações aeronáuticas ainda enfrentam dificuldades significativas na implementação prática dessas exigências. Entre os principais obstáculos destacam-se a falta de integração efetiva entre os sistemas de gestão de segurança operacional (SMS) e os sistemas de gestão da segurança da informação (ISMS), a escassez de profissionais especializados em cibersegurança aeronáutica e a ausência de ferramentas automatizadas que apoiem a mitigação contínua de riscos. Soma-se a esses desafios a insuficiente compreensão interdisciplinar entre os domínios de *safety*, *security* e *cybersecurity*, o que frequentemente resulta em abordagens fragmentadas e na incapacidade de traduzir riscos digitais em impactos operacionais concretos. Essa lacuna de conhecimento impede que as equipas de diferentes áreas comuniquem e cooperem de forma eficaz,

comprometendo a eficácia global dos sistemas de gestão integrados (Mizrak & Reyhan Akkartal, 2024).

Face à esta crescente complexidade do ambiente digital da aviação, a Inteligência Artificial (IA) afirma-se como uma aliada estratégica para o fortalecimento da resiliência cibernética no setor aeronáutico. Estudos recentes evidenciam que técnicas avançadas de *machine learning* e *deep learning* têm capacidade para detetar padrões anómalos em redes aeronáuticas, prever vulnerabilidades e apoiar decisões críticas em tempo real (Garcia, 2022; Lakhani, 2025). Estas tecnologias oferecem, assim, uma oportunidade concreta de elevar a maturidade dos sistemas de gestão, tornando-os mais preditivos e adaptativos face às ameaças emergentes. O desafio que se impõe vai além da mera adoção tecnológica, mas reside em integrar a IA de forma ética, transparente e auditável, assegurando a rastreabilidade dos processos decisórios e a conformidade com o quadro normativo europeu, nomeadamente o Regulamento (UE)2023/203 EASA Part-IS e o (UE)AI Act (2024). Tal integração representa não apenas uma evolução tecnológica, mas uma mudança paradigmática na forma como o risco é identificado, avaliado e mitigado no domínio da aviação civil (UE 2023/203, 2023; UE 2024/1689, 2024).

1.2. Objetivo Geral

A presente dissertação tem como finalidade propor uma abordagem integrada para a gestão de riscos de cibersegurança no setor aeronáutico, sustentada na integração entre Inteligência Artificial (IA) e os sistemas de gestão regulatórios europeus. Partindo da análise crítica do enquadramento normativo, em particular do Regulamento EASA Part-IS, da Diretiva NIS2 e do (EU) AI Act, o estudo procura compreender como os requisitos de segurança da informação e de segurança operacional podem ser articulados num modelo único de gestão inteligente e auditável.

Neste contexto, os objetivos da investigação foram definidos de forma a garantir uma progressão lógica entre a fundamentação teórica, a análise normativa e o desenvolvimento do modelo proposto. Inicialmente, a pesquisa aborda o estado da arte da regulamentação normativa e sua evolução no tempo, para perceber o impacto regulatório para o setor e seu processo de implementação, a cibersegurança para compreender seus domínios no setor aeronáutico e por fim os estudos atuais da IA na aviação, explorando as interdependências entre *Safety Management Systems* (SMS) e *Information Security Management Systems* (ISMS). Em seguida, traz-se na conceção do modelo teórico CESAR (*Cyber–Safety Enhanced System for AI-based*

Risk Management), que pretende demonstrar a viabilidade da integração entre *safety*, *security* e *cybersecurity* através de processos de gestão de risco suportados por IA explicável.

Os objetivos gerais e específicos que se apresentam, delineiam a trajetória científica deste trabalho e orientam o desenvolvimento dos capítulos subsequentes, articulando o rigor académico com a aplicabilidade prática no contexto da aviação civil europeia.

1.3. Motivação

A motivação deste estudo assenta na constatação de que o setor aeronáutico se encontra num ponto de inflexão entre a transformação digital e a necessidade de garantir segurança e conformidade. A complexidade dos sistemas interconectados, o aumento de incidentes de cibersegurança e a crescente pressão normativa tornam imperativa uma abordagem que vá além do cumprimento formal de requisitos, é necessário um modelo integrado, inteligente e proativo de gestão de risco.

Do ponto de vista profissional, a experiência no contexto de companhias aéreas europeias demonstra a dificuldade em alinhar práticas de *safety* e cibersegurança sob um mesmo sistema de gestão. Enquanto o SMS é amplamente consolidado, com processos maduros de análise de perigos e mitigação, o ISMS ainda é frequentemente tratado como uma função isolada de TI, sem integração direta com a segurança operacional.

A nível institucional, a introdução do EASA Part-IS representa um marco histórico, ao exigir que operadores e organizações aeronáuticas passem a tratar a segurança da informação como componente essencial da segurança operacional. No entanto, a implementação prática desse regulamento, especialmente em companhias de médio porte, tem revelado desafios de recursos, competências e alinhamento regulatório (UE 2023/203).

A motivação científica emerge, assim, da necessidade de investigar como a Inteligência Artificial pode ser usada para colmatar essas lacunas, automatizando tarefas de monitorização, análise de incidentes e priorização de riscos, enquanto assegura explicabilidade e rastreabilidade, conforme exigido pelo Regulamento (UE)AI Act (2024) (UE 2024/1689).

1.4. Contribuição da Investigação

A principal contribuição desta dissertação reside na proposta do CESAR *Framework* (*Cyber–Safety Enhanced System for AI-based Risk Management*), um modelo conceptual interdisciplinar que integra a gestão de riscos de cibersegurança (ISMS), a gestão de segurança operacional (SMS) e a Inteligência Artificial explicável (XAI), estruturado segundo o ciclo regulatório do EASA Part-IS.

Ao propor essa integração, procura-se dar resposta a um desafio identificado e ainda por resolver aos desafios regulatórios e tecnológicos que emergem da crescente evolução tecnológica no setor da aviação, demonstrando como a utilização de sistemas inteligentes podem reforçar a resiliência ciberoperacional e garantir a conformidade normativa no contexto europeu (Filinovych & Hu, 2021; Monev, 2024; UE 2023/203, 2023).

a) Contribuições Científicas

1. Integração interdisciplinar: desenvolvimento de um modelo teórico que unifica, os domínios de *safety* e *cybersecurity* na aviação civil, estabelecendo um quadro conceptual de interdependência entre a gestão de risco técnico, operacional e organizacional, para atender a nova regulamentação EASA Part-IS (Easy Rules, 2025; UE 2023/203, 2023) .

2. Contribuição centrada na análise normativa: realização de uma análise aprofundada do Regulamento EASA Part-IS, cuja sistematização poderá servir de base metodológica para investigações futuras sobre a integração entre sistemas de gestão regulatórios (UE 2023/203, 2023).

3. Incorporação de mecanismos de Inteligência Artificial explicável (XAI), no modelo teórico: inclusão de elementos de *machine learning*, *federated learning* e Inteligência Artificial explicável em conformidade com o (UE)AI Act *(2024)* (UE 2024/1689), reforçando a transparência, a auditabilidade e a confiança nos processos automatizados de gestão de risco.

b) Contribuições Práticas

1. Proposta de um processo integrado de gestão de riscos: aplicável às companhias aéreas, permitindo alinhar práticas internas de *cybersecurity* e *safety* com os requisitos de conformidade definidos pelo EASA Part-IS e pela Diretiva NIS2.

2. Apoio à implementação normativa: o modelo fornece um guia prático para a adoção harmonizada das normas ISO/IEC 27001:2022 e ISO/IEC 27005:2022, favorecendo a uniformização das práticas de gestão da segurança da informação no setor aeronáutico.

3. Base conceptual reutilizável: criação de uma estrutura teórica que pode ser estendida para o desenvolvimento de futuras soluções tecnológicas, políticas públicas e estratégias organizacionais de cibersegurança na aviação, contribuindo para a construção de uma cultura europeia de resiliência digital.

Em suma, a dissertação propõe um modelo teórico que aborda um paradigma de gestão integrada de riscos para o setor aeronáutico, em que a Inteligência Artificial atua como elemento de ligação entre a segurança operacional, a cibersegurança e a conformidade regulatória, promovendo uma visão sistémica, automatizada e transparente da segurança na aviação civil.

1.5. Estrutura da Dissertação

Esta dissertação está estruturada em nove capítulos principais, organizados de forma a garantir uma progressão lógica desde a fundamentação metodológica até à proposta e validação do modelo.

O Capítulo 1 - Introdução apresenta o enquadramento geral do tema, a relevância do problema de investigação, os objetivos do estudo, as questões de pesquisa e a metodologia global adotada, além de explicar a estrutura da dissertação.

O Capítulo 2 - Metodologia de Investigação apresenta o enquadramento metodológico assente no método *Design Science Research* (DSR), descrevendo as cinco fases do processo investigativo, os métodos de recolha de dados, e a estratégia de validação através de *workshop* com especialistas da aviação.

O Capítulo 3 - Revisão Sistemática da Literatura descreve o protocolo PRISMA aplicado, a estratégia de pesquisa nas bases de dados académicas e regulatórias, os critérios de seleção, e a

síntese dos 40 estudos incluídos. Este capítulo responde às cinco questões de pesquisa que fundamentam teoricamente o modelo proposto.

O Capítulo 4 - Enquadramento Regulatório da Aviação Civil analisa a evolução histórica e normativa dos pilares *Safety*, *Security* e *Cybersecurity*, evidenciando como incidentes críticos moldaram as regulações atuais, com destaque para a convergência entre os três domínios no contexto europeu.

O Capítulo 5 - EASA Part-IS: Análise Técnica aprofunda o Regulamento (UE) 2023/203, examinando detalhadamente os requisitos IS.I.OR.200 a IS.I.OR.260, com foco no processo de gestão de risco de segurança da informação e na integração obrigatória com o SMS (UE 2023/203, 2023).

O Capítulo 6 - Inteligência Artificial no setor Aeronáutico apresenta o estudo sobre IA na aviação, abrangendo tipologias de algoritmos, aplicações operacionais, requisitos de explicabilidade (XAI), e o enquadramento do regulamento (UE)AI Act.

O Capítulo 7 - CESAR *Framework*: Modelo Proposto introduz e descreve o sistema integrado ISMS-SMS com suporte de IA explicável desenvolvido neste estudo, incluindo arquitetura técnica, ciclo de funcionamento, mapeamento regulatório e cenários de aplicação.

O Capítulo 8 - Validação Conceptual e Aceitação Organizacional apresenta a metodologia, execução e resultados do *workshop* realizado com profissionais da EuroAtlantic Airways, discutindo criticamente o *feedback* obtido e as limitações da validação realizada.

O Capítulo 9 - Conclusões e Trabalho Futuro sintetiza os contributos científicos e práticos da investigação, reconhece as limitações do estudo, e estabelece direções para investigação futura e implementação técnica do modelo. A dissertação termina com a Conclusão, onde são apresentados os contributos, limitações e sugestões para investigação futura, seguida pelas Referências Bibliográficas.

2. METODOLOGIA DE INVESTIGAÇÃO

2.1. Introdução

A aviação civil constitui um dos domínios tecnológicos mais complexos e digitalmente interdependentes da atualidade, o que reforça a necessidade de estratégias robustas de cibersegurança e de resiliência digital. A crescente interconectividade entre sistemas aeronáuticos e infraestruturas críticas trouxe ganhos significativos de eficiência e modernização; contudo, introduziu também novos vetores de vulnerabilidade, tornando a cibersegurança um domínio crítico e transversal ao conceito de *safety*.

A integração entre sistemas físicos e digitais tornou cada vez mais ténue a distinção entre falhas técnicas e ataques cibernéticos. Em resposta a estes desafios emergentes, foram desenvolvidos novos marcos regulatórios e normativos. A Europa, em esforço contínuo para reforçar a segurança operacional, instituiu o Regulamento (UE)2023/203 – EASA Part-IS, que estabelece um quadro normativo europeu para o *Information Security Management System* (ISMS) em operadores aéreos, organizações de manutenção e autoridades aeronáuticas. Em paralelo, a Diretiva (UE)2022/2555 – NIS2 reforça a obrigatoriedade de estruturas de governança e gestão de risco cibernético nos setores críticos, incluindo o transporte aéreo (UE 2022/2555, 2022; UE 2023/203, 2023).

Neste contexto, esta dissertação propõe o CESAR *Framework*, um modelo de gestão cognitiva de riscos que integra ISMS e SMS, apoiado por Inteligência Artificial Explicável (XAI), alinhado ao EASA Part-IS (UE 2023/203) (UE 2023/203, 2023).

Para fundamentar o desenvolvimento deste modelo, foi conduzida uma Revisão Sistemática da Literatura (RSL), combinada com uma abordagem metodológica baseada em *Design Science Research* (DSR).

2.2. Abordagem Metodológica

A investigação apresenta carácter qualitativo, exploratório e propositivo, com base na metodologia *Design Science Research* (DSR). Essa abordagem é amplamente utilizada para o desenvolvimento de artefactos tecnológicos e modelos de gestão inovadores, articulando o rigor científico com a relevância prática (Peffers et al., 2007).

A DSR é particularmente adequada a este estudo, pois permite desenvolver um modelo teórico-aplicado (CESAR *Framework*) como resposta a um problema complexo, a integração entre cibersegurança e segurança operacional sob requisitos regulatórios.

2.3. *Design Science Research* (DSR)

2.3.1. Justificação da Escolha do DSR

O *Design Science Research* é um método de investigação em sistemas de informação que visa criar e avaliar artefactos (construtos, modelos, métodos, instanciações) destinados a resolver problemas práticos identificados (Hevner et al., 2004; Peffers et al., 2007). Segundo Peffers et al. (2007), o DSR é particularmente apropriado quando:

- Existe um problema prático relevante para organizações
- A solução requer desenvolvimento de um artefacto inovador
- É necessário demonstrar a viabilidade e utilidade do artefacto
- O conhecimento produzido tem valor tanto académico quanto prático

Estas características alinham-se perfeitamente com os objetivos desta dissertação:

1. Problema Prático Identificado: As organizações aeronáuticas europeias enfrentam dificuldades em integrar ISMS e SMS conforme exigido pelo EASA Part-IS, carecendo de modelos conceptuais que orientem esta integração com suporte de tecnologias emergentes como IA.

2. Artefacto a Desenvolver: O CESAR *Framework* constitui um modelo conceptual que articula processos de gestão de risco de cibersegurança e segurança operacional através de IA explicável.

3. Necessidade de Validação: A utilidade e aceitabilidade do modelo devem ser avaliadas junto de profissionais do setor antes de eventual implementação técnica.

4. Contributo *Dual*: A investigação produz conhecimento académico (publicações, avanço teórico) e conhecimento prático (ferramenta conceptual aplicável).

O DSR foi preferido a outras abordagens (estudo de caso, investigação-ação, *design thinking*) porque enfatiza a criação rigorosa e sistemática de artefactos, exigindo fundamentação teórica sólida (através da revisão da literatura) e validação estruturada (através do *workshop*).

2.3.2. Fases do Processo DSR Aplicadas

Seguindo o modelo processual de Peffers et al. (2007), a investigação desenvolveu-se em cinco fases sequenciais e iterativas, descrito nas Tabelas 1, 2, 3, 4, 5 abaixo:

Tabela 1- Identificação do problema e motivação

FASE 1: IDENTIFICAÇÃO DO PROBLEMA E MOTIVAÇÃO
Objetivo: Definir o problema de investigação e justificar o valor da sua resolução. Atividades: • Análise exploratória da literatura sobre cibersegurança na aviação • Revisão dos regulamentos EASA Part-IS e NIS2 • Identificação da lacuna: ausência de modelos integrados ISMS-SMS com suporte de IA • Contacto preliminar com profissionais da EuroAtlantic para confirmar relevância prática do problema Resultado: Problema delimitado e justificado (Capítulo 1.1-1.3 da dissertação).

Fonte: Fases do Processo DSR Aplicadas

Tabela 2 - Definição dos objetivos da solução

FASE 2: DEFINIÇÃO DOS OBJETIVOS DA SOLUÇÃO

Objetivo: Estabelecer critérios que a solução deve cumprir.
 	
Atividades:
 	
• Definição de objetivos gerais e específicos
• Formulação de questões de pesquisa (5 QPs)
• Estabelecimento de requisitos do artefacto:
  o Integrar processos ISMS-SMS
  o Incorporar IA explicável
  o Alinhar-se com EASA Part-IS
  o Ser compreensível para profissionais da aviação
 	
Resultado: Especificação dos requisitos do CESAR (Capítulo 1.2 e 1.4 da dissertação).

Fonte: Fases do Processo DSR Aplicadas

Tabela 3 - *Design* e desenvolvimento

FASE 3: *DESIGN* E DESENVOLVIMENTO

Objetivo: Criar o artefacto (CESAR *Framework*):
• Revisão Sistemática da Literatura (Capítulo 3):
  o Protocolo PRISMA 2020
  o Análise de 40 estudos sobre IA e cibersegurança
  o Síntese de ameaças, técnicas, desafios
• Análise Documental Regulatória (Capítulos 4-5):
  o Estudo aprofundado do EASA Part-IS
  o Mapeamento de requisitos regulatórios
  o Análise de integração ISMS-SMS
• Revisão de IA na Aviação (Capítulo 6):
  o Tipologias de algoritmos
  o Requisitos de XAI
  o (UE)AI Act e certificação
• Conceptualização do CESAR (Capítulo 7):
  o Definição da arquitetura
  o Especificação do ciclo de 7 fases
  o Mapeamento regulatório
  o Desenvolvimento de diagramas BPMN
Resultado: CESAR *Framework* conceptualmente desenvolvido.

Fonte: Fases do Processo DSR Aplicadas

Tabela 4 - Demonstração

FASE 4: DEMONSTRAÇÃO

Objetivo: Demonstrar a viabilidade do artefacto em contexto.
 	
Atividades:
 	
• Preparação de materiais de apresentação:
  o Apresentação PowerPoint
  o Diagramas de fluxo BPMN
  o Cenários simulados de aplicação
• Realização do *Workshop* (Capítulo 8):
  o Apresentação do CESAR a 10 profissionais da EAA
  o Demonstração de 3 cenários práticos
  o Sessão de perguntas e discussão
 	
Resultado: Modelo apresentado e discutido com *stakeholders*.

Fonte: Fases do Processo DSR Aplicadas

Tabela 5 - Avaliação

FASE 5: AVALIAÇÃO

Objetivo: Avaliar o artefacto face aos objetivos definidos.
 	
Atividades:
 	
• Análise do *feedback* do *workshop*:
  o Identificação de questões levantadas (13)
  o Catalogação de sugestões (2 principais)
  o Avaliação de correções necessárias (2)
• Análise crítica das limitações:
  o Reconhecimento da validação apenas conceptual
  o Identificação de próximos passos (implementação)
 	
Resultado: Validação conceptual obtida com identificação de requisitos para validação técnica futura (Capítulo 8).

Fonte: Fases do Processo DSR Aplicadas

Entre as fases 3 e 4, foram realizados ajustes iterativos no modelo com base em *feedback* recolhidos de orientadores e colegas. Após a fase 5 (*workshop*), foram incorporadas sugestões, de acordo com os *feedbacks* recolhidos, na conceptualização final apresentada no Capítulo 7.

Fase 6 (Comunicação):

A comunicação dos resultados materializa-se através desta dissertação, complementada pela preparação de artigo científico para submissão a revista indexada (em curso).

2.4. Métodos de Recolha de Dados

A investigação utilizou três métodos complementares de recolha de dados, cada um respondendo a objetivos específicos dentro do processo DSR conforme mostrado nas Tabelas 6, 7 e 8.

Tabela 6 - Revisão sistemática da literatura (RSL)

REVISÃO SISTEMÁTICA DA LITERATURA (RSL)
Objetivo: Construir base de conhecimento rigorosa sobre IA, cibersegurança e regulação na aviação. Protocolo: PRISMA 2020 (Kitchenham & Charters, 2007) Bases de Dados: o Academicas: Scopus, IEEE Xplore, ScienceDirect, SpringerLink, Web of Science, ACM Digital Library o Regulatórias: EASA, ICAO, EUROCONTROL, ENISA, ANAC, IATA Período: janeiro 2018 - dezembro 2025 Resultado: 40 estudos incluídos após triagem sistemática Detalhe: O protocolo completo está descrito no Capítulo 3.

Fonte: Fases do Processo DSR Aplicadas

Tabela 7 - Analise documental regulatória

ANÁLISE DOCUMENTAL REGULATÓRIA
Objetivo: Compreender em profundidade os requisitos regulatórios aplicáveis. Documentos Analisados: o Regulamento (UE) 2023/203 (EASA Part-IS) o Regulamento (UE)2019/1583 – *Basic Regulation* o Regulamento (UE)2018/1139 – *Security Aviation* o Regulamento (UE) 2024/1110 - SMS o AMC & GM to Part-IS (*Decision* 2025/014/R) o Diretiva (UE) 2022/2555 (NIS2) o Regulamento (UE) 2024/1689 (EU AI Act) o ICAO Annex 19 (*Safety Management*) o ICAO Annex 17 (*Security Management System*) o ISO/IEC 27001:2022 e ISO/IEC 27005:2022 o *Easy Access Rules for Information Security* (*Regulations* (EU) 2023/203 *and* 2022/1645) o *Acceptable Means of Compliance and Guidance Material to Annex II* (Part-IS.I.OR) to *Commission Implementing Regulation* (UE)2023/203 o *Annex* I e II to ED *Decision* 2025/014/R 'AMC & GM to Part-IS.D.OR – *Issue* 1, *Amendment* 1 o ICAO *Aviation Cybersecurity Strategy* o ICAO *Cybersecurity policy Guidance* o EASA *Detailed specifications and associated AMC and guidance material for AI* Método de Análise: o Leitura integral dos documentos o Extração de requisitos relevantes para ISMS-SMS o Mapeamento de interdependências regulatórias o Criação de tabelas comparativas Resultado: Fundamentação regulatória detalhada (Cap. 4-5).

Fonte: Fases do Processo DSR Aplicadas

Tabela 8 - *Workshop* de Validação

WORKSHOP DE VALIDAÇÃO
Objetivo: Validar conceptualmente o CESAR *Framework*. Formato: Sessão presencial de 4 horas Participantes: 10 profissionais da EuroAtlantic Airways o CISO / *IT Manager* o *Safety Manager* o *Security Manager* o *Chief Pilot* o *Accountable Manager* o CFO o Direção Técnica o *Project Manager* o *Developer* o *Infrastructure Lead* Estrutura: 1. Apresentação conceptual do CESAR (90 min) 2. Demonstração de 3 cenários práticos (60 min) 3. Sessão de perguntas e discussão (90 min) Dados Recolhidos: o 13 questões formuladas pelos participantes o 2 correções identificadas durante demonstração o 2 sugestões de melhoria o Notas de observação sobre reações e *engagement* Resultado: *Feedback* qualitativo sobre aceitação viabilidade do modelo (Cap. 8).

Fonte: Fases do Processo DSR Aplicadas

2.5. Análise e Síntese de Dados

A análise dos dados recolhidos seguiu abordagens distintas consoante a natureza de cada fonte:

Revisão Sistemática da Literatura:

- Análise de conteúdo temática para responder às 5 questões de pesquisa,
- Síntese narrativa dos resultados por categoria (ameaças, regulação, IA, desafios, integração),

Análise Documental Regulatória:

- Análise jurídico-normativa dos requisitos aplicáveis,
- Mapeamento sistemático entre diferentes *frameworks* regulatórios (EASA Part-IS ↔ ISO 27001 ↔ ICAO *Annex* 17 e *Annex* 19),
- Identificação de *gaps* e sobreposições regulatórias

Workshop de Validação:

- Análise de conteúdo das questões levantadas, agrupando-as por temas,
- Catalogação sistemática de sugestões e correções,
- Interpretação qualitativa das reações e nível de aceitação observado.

A triangulação entre as três fontes permitiu construir uma visão integrada que fundamenta a proposta do CESAR *Framework*.

2.6. Considerações Éticas

Esta investigação respeitou os princípios éticos fundamentais da investigação. Todos os participantes do *workshop* foram informados previamente sobre os objetivos da investigação, o uso dos dados recolhidos, e o carácter voluntário da sua participação. Obteve-se consentimento verbal de todos.

Embora a investigação tenha sido conduzida numa organização específica (EuroAtlantic Airways), com conhecimento e apoio da direção, os dados recolhidos não incluem informação sensível sobre sistemas, vulnerabilidades ou incidentes reais da companhia. As perceções dos participantes foram anonimizadas quando reportadas.

A investigação não envolveu qualquer risco para os participantes nem para a organização. O *workshop* teve carácter puramente exploratório e educativo, não afetando operações ou sistemas produtivos.

O modelo CESAR é de autoria da investigadora, desenvolvido no âmbito académico sob orientação da Universidade Atlântica. Não há conflitos de interesse comercial ou financeiro.

2.7. Limitações Metodológicas

Reconhecem-se as seguintes limitações metodológicas desta investigação:

O CESAR *Framework* foi validado apenas conceptualmente através de *workshop* com profissionais de uma única organização. Não houve implementação técnica, testes em ambiente operacional, nem medição de performance real. Assim, a eficácia do modelo permanece como hipótese a validar empiricamente em trabalho futuro.

O *workshop* envolveu 10 profissionais de uma companhia aérea portuguesa. Embora a diversidade de perfis que cobrem ambas as áreas de análise do modelo proposto, esta amostra não é representativa do setor aeronáutico europeu, limitando a generalização das conclusões sobre aceitação organizacional.

A validação baseou-se exclusivamente em *feedback* qualitativo (perguntas, sugestões, observações). Não foram aplicados instrumentos quantitativos (questionários estruturados, escalas de avaliação), o que reduz a robustez da avaliação.

A revisão sistemática cobriu 2018-2025, período que captura o surgimento do EASA Part-IS mas pode excluir desenvolvimentos muito recentes (publicações de 2025 ainda não indexadas).

O modelo foi desenvolvido especificamente para o enquadramento regulatório europeu (EASA, NIS2, (UE)AI Act). A sua aplicabilidade a outros contextos regulatórios (FAA, Transport Canada, autoridades asiáticas) não foi explorada.

A investigadora possui experiência prévia em aviação, o que pode ter influenciado a interpretação dos dados e o *design* do modelo. Procurou-se mitigar este viés através de fundamentação rigorosa na literatura e com a triangulação de fontes, além de validação com orientadoras e profissionais externos.

Embora o DSR seja apropriado para criar artefactos conceptuais, é menos eficaz para validar empiricamente a sua efetividade. O modelo DSR foi seguido até à fase de "demonstração", faltando completar a fase de "avaliação rigorosa" que exigiria implementação técnica.

Estas limitações não invalidam os contributos da investigação, mas delimitam o seu alcance e apontam para direções de investigação futura.

3. REVISÃO SISTEMÁTICA DA LITERATURA

3.1. Introdução

Este capítulo apresenta a Revisão Sistemática da Literatura (RSL) que fundamenta teoricamente a proposta do CESAR *Framework*. Seguindo o protocolo PRISMA 2020 (Page et al., 2021), a revisão examinou sistematicamente a literatura científica e documentação regulatória publicada entre janeiro de 2018 e dezembro de 2025, com o objetivo de identificar o estado da arte sobre gestão de riscos de cibersegurança na aviação, aplicações de Inteligência Artificial voltadas para aviação e os sistemas regulatórios europeus, em particular o novo regulamento (UE)2023/203.

O capítulo está organizado em nove secções: após esta introdução, a secção 3.2 detalha o protocolo metodológico; a secção 3.3 apresenta os resultados quantitativos da seleção; as secções 3.4 a 3.8 respondem sistematicamente às cinco questões de pesquisa; e a secção 3.9 oferece síntese crítica integradora que estabelece as bases para os capítulos subsequentes.

3.2. Protocolo da Revisão Sistemática da Literatura (RSL)

A revisão seguiu as diretrizes metodológicas de Kitchenham & Charters (2007) e o protocolo PRISMA 2020, assegurando rastreabilidade e rigor na identificação, seleção e análise das fontes.

O objetivo da RSL foi identificar e analisar as evidências científicas relacionadas às cinco questões de pesquisa da literatura da dissertação, com foco no Regulamento (UE)2023/203 (EASA Part-IS), no âmbito das organizações, na integração entre SMS e ISMS e no papel da IA na gestão de riscos aeronáuticos.

3.2.1. Questões de pesquisa

As cinco questões de pesquisa foram formuladas após análise exploratória preliminar da literatura, assegurando que cobrem as dimensões essenciais para fundamentar o desenvolvimento do modelo proposto. A Tabela 9 sintetiza as questões e suas finalidades.

Tabela 9 – Questões da pesquisa

QP	Questão	Finalidade
QP1	Quais são as principais ciber ameaças enfrentadas pelo setor aeronáutico atualmente?	Caracterizar o panorama de ameaças para fundamentar a relevância do problema
QP2	Quais são os regulamentos europeus que abordam a cibersegurança na aviação?	Mapear o enquadramento normativo aplicável ao modelo proposto.
QP3	Quais são os principais desafios e limitações da nova regulamentação EASA Part-IS?	Identificar obstáculos práticos que o modelo deve ajudar a superar.
QP4	Quais aplicações de Inteligência Artificial têm sido propostas ou implementadas para mitigar ciber riscos na aviação?	Compreender o potencial e limitações da IA como tecnologia de suporte.
QP5	Como pode ser estruturado um processo integrado de gestão de riscos que contemple segurança operacional, cibersegurança e *compliance* regulatório?	Identificar requisitos e princípios para o *design* do CESAR *Framework*.

Fonte: Perguntas da pesquisa

3.2.2. Bases de dados e *strings* de pesquisa

A pesquisa bibliográfica foi conduzida nas bases Scopus, SpringerLink, ScienceDirect, IEEE Xplore e *Web of Science*, complementadas por fontes regulatórias (EASA, ICAO, ENISA, IATA, EUROCONTROL e FAA).

As combinações de termos utilizadas incluíram:

- ("*cybersecurity*" OR "*information security*") AND ("*aviation*" OR "*aerospace*")

- ("EASA Part-IS" OR "*aviation regulation*") AND ("*cyber threats*" OR "*risk management*")
- ("*artificial intelligence*" OR "*machine learning*") AND ("*cybersecurity*" AND "*aviation*")

Essas *strings* foram ajustadas conforme os operadores booleanos de cada base de dados.

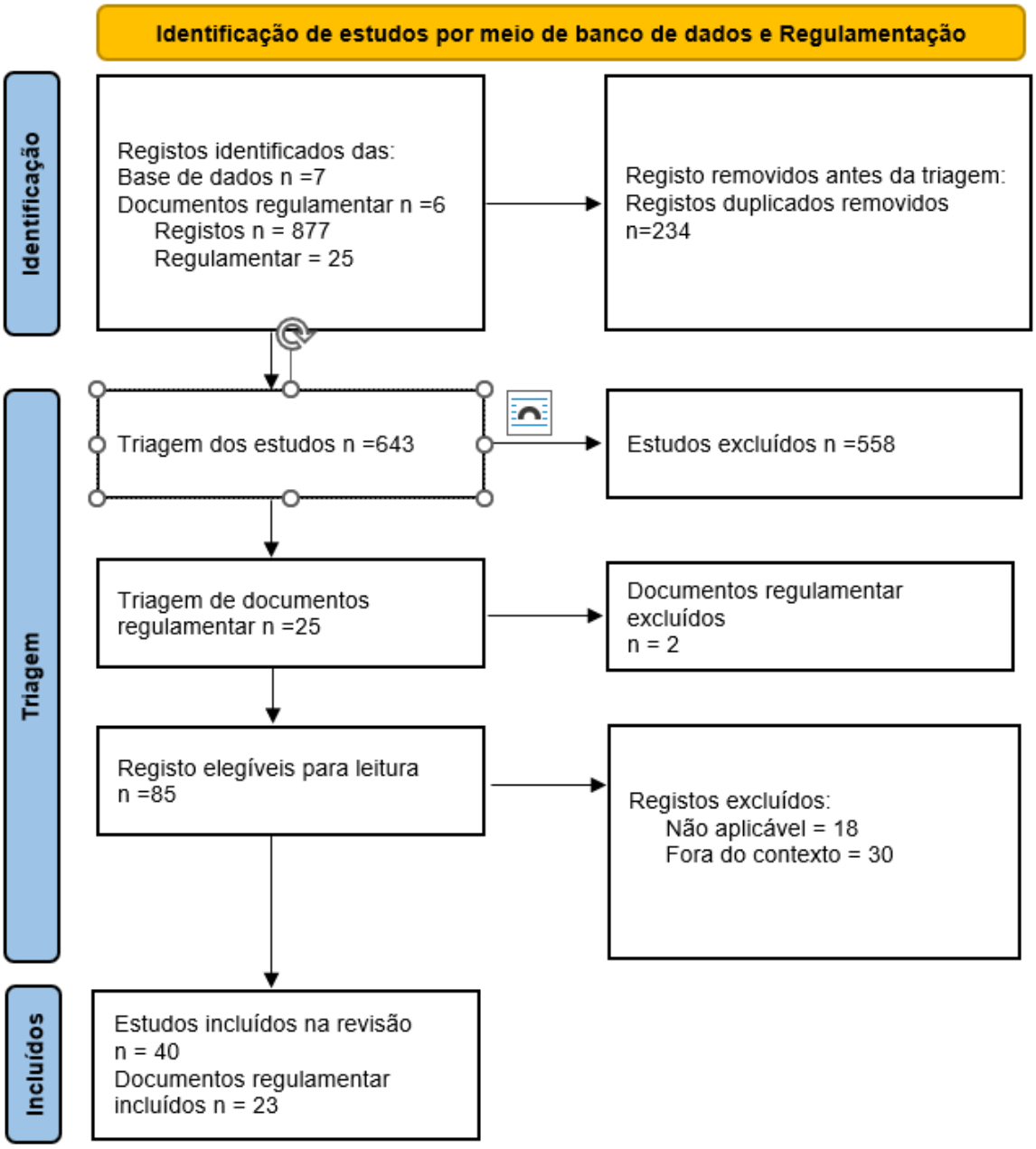
3.2.3. Critérios de inclusão e exclusão

Inclusão: estudos entre 2018–2025, revisados por pares, em inglês ou português, com foco em aviação, cibersegurança, IA e regulação.

Exclusão: artigos duplicados, sem acesso completo, ou que não abordassem o contexto aeronáutico.

Após a triagem inicial de 877 estudos, 85 artigos foram elegíveis para leitura completa e 25 documentos regulatórios. Destes, 40 artigos científicos e 23 documentos regulatórios (EASA, ICAO, ENISA, ISO, CNCS) compuseram a análise final. A Figura 1 ilustra o processo PRISMA adotado.

Fig. 1 - Processo PRISMA



Fonte: Resultado da análise dos Documento analisados

3.3. Resultados da Seleção e Resposta às Questões de Pesquisa

A estratégia de pesquisa identificou inicialmente 877 registos nas bases de dados seleccionadas (Scopus: 324, IEEE Xplore: 198, ScienceDirect: 145, SpringerLink: 112, Web of Science: 98). Após remoção de 234 duplicados, 643 registos foram triados por título e resumo, dos quais 558 foram excluídos por não satisfazerem os critérios de elegibilidade. Os 85 estudos remanescentes

foram avaliados em texto completo, resultando na exclusão de 45 por razões específicas: falta de foco em aviação (18), ausência de componente de IA ou cibersegurança (12), estudos puramente teóricos sem validação (9), e duplicação de conteúdo (6).

O processo culminou na inclusão de 40 estudos na revisão sistemática, conforme ilustrado na Figura 1 (diagrama PRISMA).

Dos 40 estudos analisados, 12 (30%) estudos têm como foco temático a União Europeia; no entanto, apenas 7 deles têm efetivamente origem europeia. A produção científica europeia concentra-se sobretudo em temas ligados à regulamentação (EASA, ENISA, União Europeia e EUROCONTROL), à integração entre *safety* e *cybersecurity*, às infraestruturas críticas, como ATM e aeroportos, e à resiliência e *compliance* regulatória. Em síntese, apesar de a Europa contribuir com um volume menor de publicações, os estudos produzidos são marcadamente especializados e de forte orientação normativa.

Dos 40 estudos analisados, 22(55%) têm foco exclusivo em cibersegurança, constituindo assim a maioria da produção identificada. Dentro deste subconjunto, emergem cinco categorias temáticas centrais: oito estudos concentram-se em redes aeronáuticas, seis abordam a aplicação de IA/ML para deteção de ataques, quatro exploram sistemas ciber-físicos (CPS) e infraestruturas críticas, três analisam vulnerabilidades associadas a aeroportos inteligentes e um estudo dedica-se à *Industry* 5.0, com ênfase em *gap analysis*. Este panorama mostra que, embora tematicamente variados, os estudos mantêm um foco inequívoco na cibersegurança aeronáutica em sentido estrito.

Dos 40 estudos analisados, 5(12,5%) estudos foram classificados como "*safety* puro", por apresentarem foco exclusivo em políticas, *frameworks* e iniciativas europeias relacionadas à segurança operacional, sem abordar cibersegurança ou integração com ISMS, sendo 3 estudos puramente técnicos (IA, Casualidade, NLP) e 2 estudos tem foco regulamentar no contexto europeu.

Dos 40 estudos analisados, 20(50%) estudos abordam inteligência artificial, sendo que 6 estudo de IA tem foco regulatórios, mas somente 3, ou seja, somente 7,5% fala explicitamente sobre o regulamento europeu (UE)IA Act, e 17 estudos falam sobre o uso de *datasets*.

Dos 40 estudos analisados, 15(37.5%) estudos abordam regulamentação, 6(15%) estudos tem foco na regulamentação EASA e apenas 2 (5%) fazem referência explícita à regulamentação europeia da EASA Part IS, revelando uma lacuna significativa na literatura científica sobre enquadramento regulatório aeronáutico. O estudo Stastny & Stoica (2022) aborda regulamentos

europeus de *safety*, incluindo o Regulamento (UE)2017/373, enquanto Lykou et al. (2019) discute o ecossistema regulatório europeu no qual a EASA desempenha papel central.

Abaixo as questões da dissertação e achados dentro dos estudos:

1. **Ameaças (QP1):** aumento de DDoS, *ransomware*, *phishing*, *spoofing* e ataques à cadeia de fornecimento (Çevik et al., 2024; Lykou et al., 2019).
2. **Regulação (QP2):** fortalecimento normativo europeu via EASA Part-IS e NIS2, ainda em fase de maturação (EASA, 2023).
3. **Desafios do Part-IS (QP3):** carência de integração ISMS–SMS e de profissionais especializados (Eleimat & Őszi, 2025; FAYE et al., 2024; Mizrak & Reyhan Akkartal, 2024; Nobles et al., 2022).
4. **Aplicações de IA (QP4):** uso crescente de ML, DL e XAI para deteção de anomalias e apoio à conformidade (Garcia, 2022; Xie et al., 2023).
5. **Integração de gestão de risco (QP5):** consenso sobre a necessidade de modelos cognitivos integrados (Lykou et al., 2018, 2019; Monev, 2024; Stastny & Stoica, 2022).

3.4. Ameaças de Cibersegurança na aviação (Q1)

Durante as últimas duas décadas, a crescente interoperabilidade entre sistemas de tráfego aéreo, aeronaves e infraestruturas críticas, impulsionada por tecnologias baseadas em IP e redes sem fio, ampliou a exposição da aviação a ataques cibernéticos direcionados. Incidentes como o *ransomware* na British Airways (2018), a violação de dados da TAP Air Portugal (2022) e as falhas operacionais na Lufthansa (2023) evidenciam que a cibersegurança passou a ser também uma questão de continuidade operacional e segurança de voo (Lykou et al., 2019).

Esta ampliação da gama de ataques e atores maliciosos exige maior consciencialização e análise aprofundada da indústria (Florido-Benítez, 2024). Atacantes exploram vulnerabilidades de sistemas e protocolos de comunicação, comprometendo integridade, confidencialidade e disponibilidade da informação (Mizrak & Reyhan Akkartal, 2024; Xie et al., 2023).

As motivações incluem cibercrime organizado, *hacktivismo* e ciberterrorismo, incidindo sobre sistemas críticos como plataformas de reservas, comunicações aeronáuticas, gestão aeroportuária, controlo de tráfego aéreo e redes de fornecedores interligadas (Florido-Benítez, 2024). Entre os métodos de ataque predominantes destacam-se *ransomware* e *malware*, capazes de paralisar sistemas essenciais e exigir resgates, bem como vazamentos de dados que expõem

informação sensível de passageiros e transações financeiras (Lykou et al., 2019; Stastny & Stoica, 2022).

Os atacantes exploram também vulnerabilidades humanas através de *phishing* e engenharia social, facilitando acessos remotos não autorizados. Ataques de rede, como negação de serviço distribuída (*DDoS*), sobrecarregam servidores e interrompem operações críticas, desde sistemas de comunicação até funções. Segundo,

Em resposta, as entidades reguladoras intensificaram os esforços para estabelecer obrigações formais de segurança da informação, promovendo uma abordagem integrada de gestão de risco que una *safety*, *security* e *information security*. Este novo enquadramento normativo representa uma mudança paradigmática, na qual a cibersegurança deixa de ser apenas uma função tecnológica e assume um papel central na gestão corporativa e na conformidade regulatória.

Da análise dos 40 estudos, identificaram-se:

- 85 ameaças cibernéticas distintas documentadas,
- 6 categorias principais de ameaças (conforme Figura 2)
- 31 estudos (77,5%) foco em *DDoS/Dos*,
- 29 estudos (72,55%) focam em *ransomware*/*malware*,
- 27 estudos (67,5%) abordam ataques a redes/infraestrutura,
- 25 estudos (62,5%) analisam engenharia social/phishing.
- 22 estudos (55%) analisam *Insider Threat,*
- 19 estudos (47.5%) analisam *Spoofing.*

Esta caracterização fundamenta a necessidade de sistemas inteligentes de deteção, dada a diversidade e sofisticação crescente das ameaças, como podemos verificar na Figura 2 - Ilustra os top 6 tipos de ataques e seus vetores encontrados na análise dos 40 artigos.

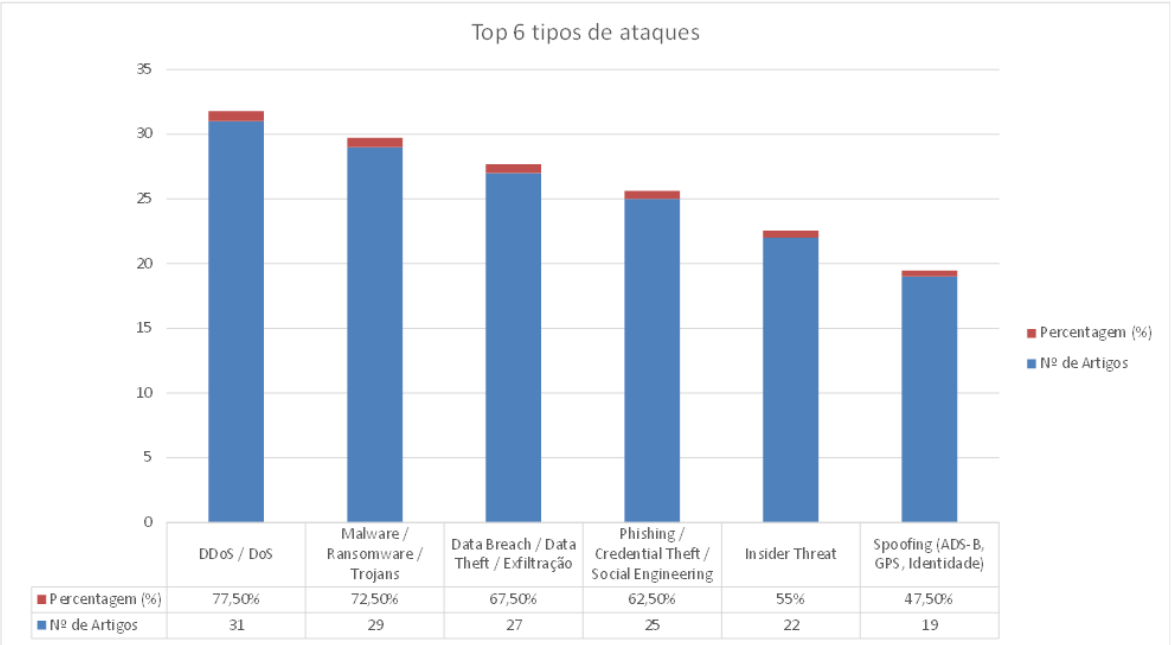
Fig. 2 - Principais tipos de ameaças no contexto da aviação

Tipo de Ataque	Vetores / Mecanismos de Exploração	Impacto no *Safety*	Principais Autores / Estudos
DDoS / DoS	*UDP flood, TCAM exhaustion, signaling flood, IPS mobility attacks, SDN saturation, jamming digital*	Perda de comunicações ATC, interrupção CPDLC, atrasos, perda de separação	Garcia (2022), Lykou (2022), Niraula (2022), SDN-FL (Rawat 2022), ADS-B SoK (2024), Bansal (2021)
Malware / Ransomware / Worms / Trojans	*E-mail, supply-chain, phishing, credential theft, removable media, remote exploitation, APTs*	Paralisação de aeroportos, perda de dados operacionais, indisponibilidade de sistemas críticos	Faye (2024), Bansal (2021), Palmer (2025), Garcia (2022), Aviation CPS (2023), Industry 5.0 (2025)
Data Breach / Data Theft / Exfiltração	*PKI compromise, MITM, spoofing, privilege escalation, APT lateral movement, cloud compromise*	Exposição de planos de voo, manipulação de mensagens, impactos indiretos via espionagem operacional	Stastny & Stoica (2022), Aviation CPS (2023), Industry 5.0 (2025), Niraula (2022), Grygorov (2021)
Phishing / Credential Theft / Social Engineering	*Spear phishing, smishing, MFA bypass, credential reuse, identity fraud*	Alteração não autorizada de dados operacionais; ataques a sistemas críticos via escalada de privilégios	Palmer (2025), Lakhani (2025), Kotadiya (2024), Garcia (2022), Bansal (2021)
Insider Threat (Malicioso ou Acidental)	*Negligência, abuso de credenciais, sabotagem, erro operacional, falhas de manutenção, data mishandling*	Erros diretos em operações (maintenance, ATC, cockpit), sabotagem física, manipulação/proxy para ataques	Palmer SLR (2025), Faye (2024), CPS Resilience (2023), Stastny (2022), Aviation Policy (2021)
Spoofing (ADS-B, GPS, Identidade de Rede)	*ADS-B injection, GPS spoofing, identity usurpation, wormhole attack, rogue router, packet replay*	Alvos falsos ("ghost aircraft"), perda de separação, rotas falsas, comandos manipulados	ADS-B SoK (2024), Xie et al. (2023), Niraula (2022), Lykou (2022), ANS studies

Fonte: Elaboração própria a partir da revisão sistemática (2021–2025).

No Gráfico 1, observa-se a distribuição dos diferentes tipos de ataques identificados, nos estudos:

Gráfico 1 - Top 6 tipos de Ataque na aviação Global



Fonte: Elaboração própria a partir da revisão sistemática (2021–2025).

Dos 31 artigos analisados, obtém-se o seguinte resumo sintético:

- Quatro em cada cinco estudos referem ataques *DDoS/DoS.*
- Quase três em cada quatro mencionam *malware* ou *ransomware*.
- Dois em cada três abordam *data breaches*.
- Mais de metade referem *insider threats*.
- Cerca de metade discutem *spoofing* aeronáutico (GPS/ADS-B).

Em síntese, os resultados da QP1 evidenciam que a literatura convergente identifica um conjunto relativamente consistente de ameaças predominantes no setor aeronáutico. Considerando os 40 estudos analisados verificamos a elevada frequência com que surgem, e como podem ter potencial impacto no *safety*, o que confirma que o ecossistema aeronáutico permanece particularmente vulnerável a ataques que exploram interdependências digitais críticas, fragilidades de redes aeronáuticas legadas e a crescente superfície de ataque decorrente da digitalização. Os achados indicam, portanto, a necessidade de abordagens integradas de segurança, capazes de combinar práticas de cibersegurança, gestão de risco e proteção da informação de forma alinhada com as exigências regulatórias e com a dinâmica operacional do setor.

3.5. Regulamentos de Cibersegurança Europeu. (Q2)

O aprofundamento da interconectividade entre componentes físicos e plataformas digitais na aviação europeia tornou cada vez mais difícil distinguir falhas técnicas de ataques cibernéticos. Essa interdependência tecnológica trouxe novos desafios de segurança, impulsionando o desenvolvimento de normas e regulamentos específicos que visam fortalecer a resiliência do setor. Em resposta, a União Europeia estabeleceu um conjunto de instrumentos regulatórios destinados a harmonizar a gestão da cibersegurança e da segurança operacional (*safety*) em toda a aviação civil (Easy Rules, 2025; Nobles et al., 2022).

Os Regulamentos (UE)2023/203 e (UE)2022/1645 compõem o enquadramento EASA Part-IS da EASA, estabelecendo a obrigatoriedade de um *Information Security Management System* (ISMS) orientado para a identificação, mitigação e monitorização de riscos de segurança da informação com impacto na segurança operacional. O Regulamento (UE)2023/203 aplica-se de forma abrangente às organizações aeronáuticas, operadores e autoridades competentes, enquanto o Regulamento Delegado (UE)2022/1645 possui um âmbito mais restrito, abrangendo

apenas as organizações responsáveis pelo projeto e produção de produtos aeronáuticos e os operadores de aeródromos, incluindo serviços de gestão da placa aviação (UE 2022/1645, 2022; UE 2023/203, 2023).

Em paralelo, a Diretiva (UE) 2022/2555, NIS2, reforça a necessidade de estruturas de governança e de gestão de riscos de cibersegurança nos setores críticos, incluindo o transporte aéreo, exigindo maior responsabilização da gestão executiva, reporte obrigatório de incidentes e mecanismos de auditoria contínua (UE 2022/2555). Na Figura 3 vemos os regulamentos de cibersegurança aplicados na União Europeia.

Fig. 3 - Regulamentos de Cibersegurança aplicados a Aviação

Regulamento / Diretiva	Foco principal	Âmbito de aplicação	Exigências de cibersegurança	Entrada em vigor
(UE) 2019/1583	Proteção técnica da aeronave	Fabricantes e operadores aeronáuticos	Requisitos técnicos contra interferências cibernéticas	2019
(UE) 2023/203 (Part-IS)	Gestão organizacional da segurança da informação	Operadores aéreos, aeroportos e prestadores de serviços aeronáuticos	ISMS integrado, avaliação de riscos, mitigação organizacional	2026
(UE) 2022/1645	Gestão de riscos de segurança da informação com impacto na segurança da aviação	Organizações de projeto e produção de aeronaves; operadores de aeródromos e prestadores de serviços de gestão da placa	Avaliação e tratamento de riscos de segurança da informação, deteção e resposta a incidentes, comunicação interna e externa	2025
(UE) 2017/373	Segurança operacional em ATM/ANS	Prestadores de serviços de navegação aérea	Gestão integrada de segurança da informação e operacional	2017
(UE) 2022/2555 (NIS2)	Cibersegurança geral em infraestruturas críticas	Entidades críticas da UE (incluindo aviação)	Gestão de risco, segurança de rede, reporte obrigatório	2024

Fonte: EASA (EASA, 2023).

Neste quadro normativo, a EASA, a ENISA e a ICAO convergem na definição de uma abordagem integrada entre *safety*, *security* e *cybersecurity*, reconhecendo que a proteção da informação é indissociável da segurança operacional. A ICAO define *safety* "*como o estado no qual o risco de danos é reduzido e mantido em nível aceitável*", e *security* "*como a proteção da aviação civil contra atos ilícitos*" (Annex 17, 2022; Annex 19, 2013). Já a ISO/IEC 27000:2018 descreve *cybersecurity* "*como a proteção da informação no ciberespaço contra o acesso não autorizado, ataques, utilização, divulgação, interrupção, modificação ou destruição*" (ISO/IEC 27000, 2018).

O Regulamento EASA Part-IS amplia esses conceitos ao introduzir o termo *Information Security* como a "*proteção de informações críticas necessárias para garantir a segurança operacional das aeronaves, sistemas e infraestruturas*" UE 2023/203, (2023). Estes elementos,

combinados com princípios como resiliência, mitigação, vulnerabilidade e *compliance*, formam a base da abordagem europeia de gestão integrada de risco, que articula tecnologia, processos e governança sob uma visão única de segurança e continuidade operacional.

Cobertura regulatória nos estudos analisados:

- EASA mencionado: 6 estudos (20%),
- EASA Part-IS com análise detalhada: 2 estudos (5%),
- NIS/NIS2 mencionada: 4 estudos (10%),
- ISO 27001 referenciada: 10 estudos (25%),
- ICAO *frameworks* citados: 6 estudos (20%)

Apenas 5% dos estudos abordam o EASA Part-IS, apesar de ser um regulamento obrigatório para aviação europeia desde outubro 2023. Esta lacuna evidencia o *gap* entre investigação académica e necessidades práticas de *compliance.*

3.6. Desafios na Implementação do EASA Part-IS (Q3)

A implementação do Regulamento EASA Part-IS é um diferencial na segurança operacional (*safety*) e cibersegurança na aviação europeia. No entanto, de acordo com a EASA (2023), um dos principais obstáculos é a falta de maturidade dos operadores aeronáuticos na adoção de estruturas de ISMS integradas aos processos de SMS. Muitas organizações ainda tratam *safety* e *cybersecurity* como domínios isolados, o que dificulta a criação de um ciclo de risco unificado, conforme exigido pelas secções IS.I.OR.200-215 do regulamento.

Monev, (2024) refere que a implementação da EASA Part-IS apresenta diversas dificuldades, principalmente relacionadas à integração do processo de gestão de risco da informação dentro do Sistema de Gestão de Segurança da Informação (ISMS), o que exige um redesenho organizacional para contemplar uma abordagem orientada a ativos com foco na segurança da aviação. Além disso, a recomendação de utilização de ferramentas especializadas de Governança, Risco e Conformidade (GRC) impõe desafios técnicos e demanda conhecimentos específicos para a configuração adequada dos fluxos de trabalho, notificações e atribuições de responsabilidades. A interpretação e operacionalização dos requisitos regulatórios, que muitas vezes são implícitos e envolvem múltiplos atores, como proprietários de risco e gestores responsáveis, também dificultam a implementação. Ademais, a manutenção contínua da conformidade, com avaliações periódicas e ações derivadas de lições aprendidas, pode ser

onerosa, especialmente para organizações com menor maturidade ou recursos limitados. Portanto, a complexidade de adaptação dos processos, o uso de tecnologias específicas e o alinhamento entre diversos requisitos regulatórios e organizacionais constituem os principais obstáculos na adoção da Part-IS.

Como salientam, FAYE et al., (2024) a aviação vem enfrentando uma escassez significativa de profissionais qualificados em cibersegurança, lacuna que compromete a proteção de infraestruturas digitais cada vez mais complexas e interdependentes. Considerando que a implementação do EASA Part-IS exige o envolvimento de múltiplos atores, a escassez de profissionais qualificados constitui um desafio adicional particularmente relevante. A falta de competências técnicas especializadas, que combinem conhecimentos simultâneos em aviação, regulamentação europeia e cibersegurança, torna-se especialmente crítica, dado tratar-se de um perfil ainda raro no mercado.

A este cenário acrescentam-se as dificuldades associadas às barreiras organizacionais, que surgem como um obstáculo adicional à implementação eficaz dos requisitos da Part-IS. Tais barreiras incluem a resistência interna à mudança, a falta de alinhamento entre departamentos, como segurança da informação, operações de aviação e gestão de risco, e a complexidade de integrar os processos de gestão de risco de segurança da informação dentro do Sistema de Gestão da Segurança da Aviação. Esta fragmentação organizacional pode comprometer a correta configuração e automatização dos processos e das ferramentas de identificação, avaliação, tratamento e monitorização dos riscos, dificultando a conformidade contínua e a gestão integrada entre ISMS e SMS. Assim, para além da carência de profissionais qualificados, as barreiras organizacionais intensificam os desafios de implementar uma abordagem de risco eficiente e plenamente alinhada com as exigências regulatórias (Easy Rules, 2025; Lykou et al., 2018; Monev, 2024; Nobles et al., 2022; Ukwandu et al., 2022).

Para Guskova et al., (2025) em operações *U-Space*[2] as principais dificuldades na implementação do EASA Part-IS, incluem a limitação da metodologia *STPA-Sec* (*System-Theoretic Process Analysis for Security*), que identifica vulnerabilidades de segurança, mas não gera medidas mitigatórias específicas, exigindo intensa dependência da expertise dos analistas.

[2] U-Space, refere-se a um conjunto de serviços e procedimentos baseados em sistemas digitais para gerenciar com segurança e eficiência o tráfego de *drones* (veículos aéreos não tripulados) em espaços aéreos controlados ou não controlados (Guskova et al., 2025).

Além disso, a necessidade de integrar outras metodologias, como o STRIDE[3], aumenta a complexidade do processo. A adaptação contínua a mudanças regulatórias e tecnológicas frequentes também representa um desafio, assim como a garantia de que os profissionais envolvidos possuam o conhecimento especializado necessário para desenvolver e implementar medidas eficazes de segurança (Ekstedt et al., 2023).

Importa salientar ainda os desafios de governança e conformidade regulatória, especialmente no que respeita à articulação entre o EASA Part-IS e a Diretiva NIS2. Embora ambas abordem a gestão de riscos de cibersegurança, diferem nos seus objetivos, âmbitos e terminologias, o que pode resultar em sobreposição de requisitos, duplicação de auditorias e potenciais divergências interpretativas entre as autoridades de aviação civil e as entidades nacionais responsáveis pela cibersegurança (UE 2022/2555, 2022; UE 2023/203, 2023).

Por fim, há limitações práticas relacionadas à escassez de dados partilhados sobre incidentes cibernéticos. A confidencialidade inerente ao setor e a ausência de um repositório centralizado de eventos dificultam a análise comparativa e o *benchmarking* regulatório, restringindo a aprendizagem organizacional e o desenvolvimento de métricas de desempenho (FAYE et al., 2024; Garcia, 2022; Sheikhi et al., 2025).

Em síntese, os principais desafios identificados na implementação do EASA Part-IS são:

1. Integração efetiva entre ISMS e SMS dentro de um ciclo único de gestão de risco;
2. Falta de recursos humanos qualificados e formação especializada;
3. Ausência de metodologias harmonizadas para avaliação e mitigação de riscos cibernéticos;
4. Dificuldades de governança e sobreposição normativa com a NIS2 (UE 2022/2555, 2022);
5. Limitações de partilha de informação e reporte de incidentes no ecossistema aeronáutico.

[3] STRIDE é uma metodologia de análise de segurança que classifica as ameaças em seis categoria. Essa abordagem ajuda a identificar e avaliar os riscos de segurança em sistemas, facilitando a adoção de medida específicas para proteger contra cada tipo de ameaça (Guskova et al., 2025).

A literatura analisada demostra que a gestão de risco aeronáutico estava fragmentada, carente de integração *safety-cyber* e necessitada de automação inteligente. O EASA Part-IS surge exatamente como resposta a essas lacunas, sendo visto como a base para uma gestão de risco moderna, integrada e preparada para acolher tecnologias cognitivas e sistemas assistidos por IA (Lykou et al., 2019; Monev, 2024; Niraula, 2022; Stastny & Stoica, 2022).

Este avanço representa um marco na modernização da segurança da aviação europeia, ao estabelecer as bases normativas e operacionais para uma gestão de risco verdadeiramente integrada entre ISMS e SMS, com potencial para evoluir para abordagens cognitivas e assistidas por IA. Esta orientação regulamentar converge diretamente com a proposta desenvolvida neste estudo, materializada no CESAR *Framework*, que operacionaliza esta integração através de mecanismos inteligentes de avaliação, mitigação e evidência.

Tabela 10 - Prevalência de desafios identificados (n=40 estudos):

Categoria de Desafio	Estudos	%
Integração Técnica	18	45%
Restrições de Dados	17	42,5%
Escassez de Competências	12	30%
Incerteza Regulatória	9	22,5%
Barreiras Organizacionais	14	35%

Fonte: Resultado da análise dos Documento analisados

Conforme podemos observar na Tabela 10, a integração técnica emerge como desafio mais prevalente (45%), confirmando a complexidade de harmonizar sistemas legados com soluções modernas de IA.

3.7. Aplicações de IA na Aviação (Q4)

A aplicação de Inteligência Artificial (IA) no setor aeronáutico tem-se expandido para várias áreas, desde manutenção preditiva até ciberdefesa, transformando-se num eixo estratégico para a prevenção e mitigação de riscos. Segundo (Demir et al., 2024), a IA tem demonstrado eficácia na previsão de falhas e otimização de processos de segurança operacional, permitindo antecipar

eventos e reduzir a intervenção humana em tarefas de monitorização. Garcia et al. (2021) acrescenta que, ao utilizar algoritmos de *machine learning* e *deep learning* em dados de tráfego aéreo, *logs* e comunicações, é possível detetar anomalias em tempo real, reforçando a capacidade de resposta do SMS e do ISMS.

A revisão de Delgado-Aguilera et al., (2024) evidencia o papel crescente da IA explicável (XAI) na aviação, especialmente na certificação e auditoria de sistemas inteligentes. O (UE)AI Act (2024) estabelece que sistemas de IA de "alto risco", como os aplicáveis à aviação, devem ser transparentes, rastreáveis e auditáveis, assegurando que o ser humano permanece no controlo das decisões críticas (UE 2024/1689, 2024).

As aplicações mais relevantes identificadas incluem:

a) Manutenção preditiva e *Condition-Based Monitoring* (CBM);
b) Classificação automatizada de relatórios de segurança (ASRS - *Aviation Safety Reporting System*) usando *Natural Language Processing* (New & Wallace, 2025)
c) Deteção de intrusões e anomalias em redes aeronáuticas, com *Deep Learning* (Çevik & Akleylek, 2024; Ukwandu et al., 2022; Xie et al., 2023);
d) Aprendizagem Federada (FL) para partilha segura de modelos entre operadores, sem exposição de dados sensíveis (Ali et al., 2025);
e) IA Generativa para simulações e criação de dados sintéticos em treino de risco (Sai et al., 2025).

Tabela 11 - Técnicas de IA Aplicadas à Cibersegurança Aeronáutica

Técnica de IA	Estudos	%	Foco Regulat.
Supervised Machine Learn	19	47,5%	36,8% (n=7)
Deep Learning	13	32,5%	46.1% (n=6)
Federated Learning	3	7,5%	33.3% (n=1)
Reinforcement Learning	4	10%	25% (n=1)
Natural Language Process	7	17.5%	42.8% (n=3)
IA explicável (XAI)	4	10%	75% (n=3)

Fonte: Resultado da análise dos Documento analisados

Percentagens não somam 100% porque estudos usam múltiplas técnicas. "*Foco Regulat."* indica percentagem de estudos dessa técnica que abordam conformidade regulatória.

Técnicas mais utilizadas (*Supervised* ML: 47,5%) têm uma consideração regulatória (36,8%), enquanto técnicas menos exploradas (IA explicável (XAI): 10%) demonstram maior alinhamento regulatório (75%). Isto sugere *disconnect* entre desenvolvimento técnico e necessidades de *compliance,* conforme demonstrado na Tabela 11.

3.8. Integração da Gestão de Risco (Q5)

A gestão de risco é o eixo central tanto da segurança operacional (SMS) quanto da segurança da informação (ISMS). Na aviação, o Anexo 19 da ICAO define o risco como a combinação entre a probabilidade e a severidade de um evento adverso que possa afetar a segurança operacional (Annex 19, 2013). No domínio da cibersegurança, a ISO/IEC 27005:2022 propõe um processo estruturado de identificação de ativos, ameaças e vulnerabilidades, seguido da avaliação de impacto e da definição de medidas de mitigação (ISO/IEC 27005, 2022).

O EASA Part-IS (Regulamento (UE)2023/203) reforça a necessidade de cada organização aeronáutica implementar um ISMS integrado ao SMS, garantindo que os riscos cibernéticos sejam tratados no mesmo ciclo de gestão dos riscos operacionais. As secções IS.I.OR.200 a 215 estabelecem requisitos para avaliação, mitigação e monitorização contínua de riscos que possam comprometer a segurança de voo (Monev, 2024).

Apesar dos avanços, a literatura indica que a integração entre *safety* e *cybersecurity* ainda é limitada. Lykou et al. (2019) apontam a falta de metodologias conjuntas de avaliação de risco, e Mizrak & Reyhan Akkartal (2024) evidenciam que, mesmo com métodos quantitativos como o BWM e o *Fuzzy DEMATEL*, o setor aeronáutico ainda carece de maturidade operacional.

O EASA Part-IS surge, assim, como um marco na convergência entre segurança operacional e cibersegurança, ao reconhecer que as ciberameaças são também riscos de *safety*. Essa visão reforça a necessidade de uma gestão holística que una ISMS, SMS e *compliance* regulatório, garantindo continuidade operacional, proteção da informação crítica e resiliência organizacional.

Essas lacunas justificam o desenvolvimento do CESAR *Framework*, proposto nesta dissertação, como um modelo de gestão cognitiva de risco baseado em Inteligência Artificial

explicável (XAI) e alinhado às normas EASA Part-IS, ISO/IEC 27005:2022 e diretiva NIS2 (2022/2555).

Abordagem à integração ISMS-SMS nos estudos:

Tabela 12 - Abordagem dos estudos ISMS -SMS

Nível de Integração Abordado	Estudos	%
Integração explícita ISMS-SMS	4	10%
Menção sem metodologia detalhada	11	27,5%
Foco apenas em ISMS	8	20%
Foco apenas em SMS	5	12,5%
Não aborda gestão de risco	15	37,5%

Fonte: Resultado da análise dos Documento analisados

Como podemos ver na Tabela 12, apenas 10% dos estudos propõem integração explícita entre ISMS e SMS, apesar de ser requisito mandatário do EASA Part-IS (IS.I.OR.200). Esta é a lacuna fundamental que justifica o desenvolvimento do CESAR *Framework*.

3.8.1. Performance de Sistemas de IA em Aplicações Integradas

Uma das descobertas mais significativas desta revisão sistemática relaciona-se com a degradação de performance observada quando sistemas de inteligência Artificial tentam endereçar simultaneamente requisitos de múltiplos domínios regulatórios.

A análise dos estudos que reportaram métricas quantitativas de performance (26 dos 40 estudos, 65%) revela padrão consistente. Sistemas optimizados para aplicações *single-domain* (*cybersecurity* isolada OU *safety* isolada) apresentam performance significativamente superior a sistemas que tentam integrar ambos os domínios. A Tabela 13 sintetiza estes resultados.

Tabela 13 -Performance de Sistemas de IA por Complexidade de Integração

Tipo de Sistema	*Accuracy* Reportada	Estudos (n)	% Total
Single-domain (*cybersecurity* OU *safety* isolados)	85-92%	23	57,50%
Cross-domain (*cybersecurity* E *safety* integrados)	72-78%	3	7,50%
Estudos sem métricas quantitativas	n/a	14	35%
Total		40	100%

Fonte: Resultado da análise dos documentos analisados – RSL

Os *ranges* de *accuracy* representam valores mínimos e máximos reportados em estudos que utilizaram metodologias comparáveis. A categoria "*cross-domain*" inclui apenas estudos que explicitamente avaliaram performance em contextos de integração *Safety-Security*. Catorze estudos (35%) não reportaram métricas quantitativas suficientes para inclusão nesta análise.

Sistemas *single-domain* alcançam *accuracy* na ordem dos 85-92%, enquanto sistemas integrados degradam para 72-78%. Esta diferença de aproximadamente 12-15 pontos percentuais representa o limiar entre sistema operacionalmente viável e sistema que gera sobrecarga excessiva de falsos positivos, comprometendo a confiança dos utilizadores.

As causas identificadas na literatura para esta degradação incluem a falta de *datasets* integrados. Estes sistemas são treinados com dados exclusivamente de *cybersecurity* ou *safety*, mas raramente com eventos que atravessem ambos os domínios (Çevik & Akleylek, 2024).

Algoritmos optimizados para confidencialidade (ISMS) tendem a ser conservadores, gerando mais alarmes falsos quando aplicados a critérios de *Safety* que priorizam disponibilidade (Garcia, 2022)

A falta de modelos que integrem nativamente as linguagens técnicas de ambos o domínio força soluções *ad-hoc* que não generalizam adequadamente (Mizrak & Reyhan Akkartal, 2024).

Particularmente revelador é o facto de apenas 3 estudos (7,5%) na literatura analisada abordarem explicitamente integração *Safety-Security*, apesar do EASA Part-IS (UE 2023/203) tornar esta integração obrigatória desde outubro de 2023. Esta lacuna quantitativa combinada com a evidência de degradação de performance, fundamenta empiricamente a necessidade de *frameworks* como o CESAR, concebidos desde o início para integração *cross-domain*, e não como adaptação posterior de sistemas *single-domain*.

3.9. Síntese Crítica e Lacunas Identificadas

A revisão sistemática demonstrou que a aviação se encontra em um ponto crítico de transformação, a segurança operacional e a cibersegurança já não podem ser tratadas como domínios isolados. A literatura evidencia a convergência entre ambos, impulsionada pela digitalização e pelos novos regulamentos europeus (EASA Part-IS, NIS2, UE AI Act).

A análise da literatura científica e técnica evidencia um panorama em evolução ascendente, onde o setor aeronáutico encontra-se no ponto de convergência entre a necessidade de inovação tecnológica e a obrigação de conformidade regulatória. A introdução do EASA Part-IS e da Diretiva NIS2 estabelece as bases normativas para a proteção da informação e a gestão do risco digital, mas a sua aplicação prática depende da capacidade das organizações em integrar tecnologia, processos e cultura de segurança (UE 2022/2555, 2022; UE 2023/203, 2023).

Os estudos analisados confirmam que a cibersegurança na aviação deixou de ser uma função isolada da tecnologia da informação e passou a constituir um domínio transversal à operação e à gestão. As vulnerabilidades digitais podem originar falhas operacionais, interrupções de serviço e até incidentes de *safety*. Da mesma forma, os mecanismos de resposta dependem de uma coordenação eficiente entre *safety managers*, IT *security officers* e autoridades reguladoras.

As aplicações de IA descritas por Lakhani (2025), Kotadiya (2024) e Garcia et al. (2021) demonstram que a aprendizagem automática pode fortalecer esta coordenação, permitindo uma gestão de risco dinâmica e baseada em evidências. A IA atua como camada de inteligência sobre os processos normativos, monitorizando continuamente os dados operacionais e recomendando ações corretivas de forma proativa.

Por fim, observa-se que a maturidade digital das organizações aeronáuticas varia amplamente entre os Estados-Membros da União Europeia. Países com estruturas nacionais de

cibersegurança mais desenvolvidas, como Dinamarca, Finlandia, Estonia e Portugal[4], avançam mais rapidamente na implementação do EASA Part-IS, enquanto operadores menores enfrentam limitações de recursos e de pessoal qualificado. Este desequilíbrio reforça a necessidade de *frameworks* integrados, escaláveis e assistidos por IA, capazes de apoiar a conformidade regulatória sem aumentar a complexidade administrativa[5] .

Em síntese, a cibersegurança na aviação caminha para um novo patamar, da gestão cognitiva de risco, no qual a inteligência artificial atua como mediadora entre o cumprimento normativo e a eficiência operacional. A consolidação deste paradigma exigirá não apenas avanços tecnológicos, mas também um compromisso organizacional contínuo com a cultura de segurança e a ética digital. Neste sentido, onde as práticas atuais de gestão de risco permanecem fragmentadas, e a ausência de um modelo integrador limita a eficácia da conformidade regulatória e a capacidade de resposta das organizações. O modelo conceptual proposto, neste âmbito, denominado CESAR (*Cyber–Safety Enhanced System for AI-based Risk Management*) surge, como uma resposta a essas lacunas, propondo um processo integrado de gestão de risco baseado em IA explicável (XAI), alinhado com o EASA Part-IS, ISO 27005, NIS2 e o EU AI Act (2024) (ACT IA, 2024; EU 2023/203).

3.9.1 Panorama Geral do Setor

Disconnect entre Capacidade Técnica e Integração Regulatória

A descoberta mais significativa desta revisão para a proposta do modelo é a evidência quantitativa de desalinhamento entre investigação técnica e necessidades regulatórias:

- 47,5% dos estudos exploram técnicas de *Supervised* ML, apenas 36,8% destes abordam conformidade regulatória.
- Apenas 5% dos estudos destacam o EASA Part-IS, regulamento obrigatório desde outubro 2023.
- Apenas 10% propõem integração explícita ISMS-SMS, apesar de ser requisito central do Part-IS.

[4] https://www.gov.pt/noticias/comissao-europeia-destaca-portugal-como-lider-na-transformacao-digital.

[5] Nota de delimitação - As observações relativas à maturidade digital dos Estados-Membros e às diferenças na capacidade de implementação do EASA Part-IS não decorrem diretamente dos 40 artigos incluídos na revisão sistemática. Trata-se de inferências críticas baseadas na análise normativa complementar realizada pela autora, uma vez que nenhum dos estudos analisados aborda comparativamente estes aspetos.

Este desalinhamento cria *gap* crítico, organizações dispõem de provas de conceito técnicas, mas carecem de orientação sobre como implementar IA de forma conforme com o enquadramento regulatório Para além de:

a) Ausência de Modelos Integrados ISMS-SMS

Resultado direto do achado de que apenas 10% dos estudos abordam integração ISMS-SMS. Os estudos existentes:

- Tratam cibersegurança e *safety* como domínios paralelos,
- Não especificam mecanismos de correlação entre riscos *cybersecurity* e *safety*,
- Carecem de mapeamento aos requisitos IS.I.OR.200-260 do Part-IS.

b) Falta de Abordagens de IA com *Compliance by Design*

Nenhum dos 40 estudos propõe arquitetura de IA onde conformidade regulatória seja princípio fundador do design. As abordagens existentes:

- Desenvolvem capacidade técnica primeiro, considerando *compliance* depois,
- Não integram requisitos de explicabilidade (XAI) desde a conceção,
- Falham em demonstrar rastreabilidade regulatória (IS.I.OR.215),
- Não abordam gestão de risco do próprio sistema de IA (IS.I.OR.205).

Esta lacuna é particularmente crítica dado o (UE) AI Act (2024) exigir que sistemas de alto risco (categoria que inclui aviação) demonstrem transparência, auditabilidade e controlo humano desde o *design* (UE 2024/1689, 2024).

a) Escassez de Validação em Ambientes Operacionais

Dos 40 estudos, apenas 3 (7,5%) reportam validação em ambientes operacionais reais, de ACARS[6] (*Aircraft Communications Addressing and Reporting System*) de aeronaves, dados de projetos críticos e de ambientes reais OT/ICS. Os restantes baseiam-se em:

- *Datasets* históricos (35%),

[6] ACARS é um sistema digital de comunicação de dados usado entre aeronaves e estações em solo, que permite a troca automática de mensagens operacionais, logísticas, administrativas e de performance durante todas as fases do voo (ARINC 618, 2011).

- Simulações laboratoriais (25%),
- Provas de conceito teóricas (17,5%)

Esta limitação impede avaliar se sistemas de IA mantêm performance prometida quando confrontados com:

- Restrições de latência de sistemas críticos aeronáuticos,
- Diversidade de fontes de dados em organizações reais,
- Requisitos de disponibilidade 99.99% de sistemas ATM/aviónicos,
- Processos de certificação e auditoria regulatória.

b) Ausência de Metodologias de Gestão de Risco Unificadas

A revisão não identificou nenhuma metodologia que unifique:

- Avaliação de risco ISMS (ISO 27005),
- Avaliação de risco SMS (ICAO *Annex* 19),
- *Framework* único que satisfaça EASA Part-IS.

Os 4 estudos (10%) que abordam integração propõem maioritariamente processos paralelos com "pontos de contacto" em vez de metodologia verdadeiramente integrada.

c) Limitada Compreensão de Desafios Organizacionais

Embora 35% dos estudos mencionem barreiras organizacionais, poucos aprofundam:

- Como a cultura de *safety* conservadora da aviação afeta adoção de IA,
- Estratégias de gestão de mudança para implementação,
- Requisitos de competências multidisciplinares (IA + aviação + *cyber*),
- Resistência à "caixa negra" inerente a alguns algoritmos.

3.10. Implicações para o Desenvolvimento do CESAR *Framework*

As lacunas identificadas estabelecem os requisitos fundamentais que o CESAR *Framework* deve endereçar:

Requisito 1: Integração Nativa ISMS-SMS

Responde à Lacuna 1. O CESAR deve integrar processos de gestão de risco de cibersegurança e *safety* desde a conceção, não como sistemas paralelos, mas como ciclo único com pontos de decisão partilhados.

Requisito 2: IA Explicável (XAI) como Princípio Arquitetural

Responde à Lacuna 2. O modelo deve incorporar XAI desde o *design*, garantindo que todas as inferências da IA sejam rastreáveis, justificáveis e auditáveis conforme IS.I.OR.215 e (UE)AI Act.

Requisito 3: Alinhamento Regulatório Estrutural

Responde à evidência de 95% dos estudos não abordarem Part-IS. O CESAR deve mapear explicitamente cada fase do seu ciclo aos requisitos IS.I.OR.200-260, demonstrando *compliance by design.*

Requisito 4: Reconhecimento de Limitações de Validação

Responde à Lacuna 3. Dado que validação operacional completa excede âmbito desta dissertação, o CESAR deve ser posicionado como *framework* conceptual validado junto de *stakeholders*, requerendo implementação técnica futura.

Requisito 5: Abordagem Pragmática à Performance

Responde à evidência de degradação 78% → 72%. O CESAR deve reconhecer que integração regulatória pode implicar *trade-offs* de performance técnica, priorizando conformidade e confiabilidade sobre maximização de *accuracy*.

3.11. Conclusão do Capítulo

A Revisão Sistemática da Literatura cumpriu o objetivo de construir base de conhecimento rigorosa sobre IA, cibersegurança e regulação na aviação. A análise de 40 estudos selecionados através de protocolo PRISMA transparente revelou:

Evidências Quantitativas Chave:

78% → 72%: degradação de performance em sistemas integrados,

5%: estudos que abordam EASA Part-IS (lacuna crítica),

10%: estudos que propõem integração ISMS-SMS (insuficiente),

45%: estudos que reportam desafios de integração técnica.

Lacunas Fundamentais Identificadas:

1. Ausência de modelos integrados ISMS-SMS operacionalizáveis,

2. IA desenvolvida sem *compliance by design,*

3. Escassa validação em ambientes operacionais,

4. Falta de metodologia unificada de gestão de risco,

5. Limitada compreensão de barreiras organizacionais.

A literatura também revela lacunas significativas. Faltam modelos consolidados de integração entre IA, ISMS e SMS, capazes de unir os requisitos técnicos do EASA Part-IS com as práticas de *safety management*. Abozaid & Baydoun (2024) no seu estudo, refere que um dos principais *gaps* identificados na sua pesquisa encontra-se na ausência de abordagens resilientes específicas para sistemas ciber-físicos na aviação, particularmente no que tange à integração efetiva de tecnologias avançadas como a Inteligência Artificial (IA) para a detecção e mitigação de ameaças cibernéticas sofisticadas e essa ausência reforça a necessidade de pesquisas que desenvolvam estratégias integradas de ciber-resiliência alinhadas às especificidades do setor, combinando inovações tecnológicas, políticas de segurança robustas e esforços colaborativos entre *stakeholders* para garantir a segurança e a confiabilidade das operações aéreas.

Estas lacunas justificam e fundamentam a necessidade do CESAR *Framework*, cujo a proposta do modelo será apresentada no Capítulo 7, após estabelecimento do enquadramento regulatório (Capítulos 4-5) e análise de IA aplicada (Capítulo 6). A evidência de degradação sistemática de performance (Tabela 13) e o desalinhamento entre capacidade técnica e integração regulatória constituem os pilares empíricos sobre os quais o modelo proposto se sustenta, demonstrando que abordagens fragmentadas são insuficientes e que *frameworks* integrados como o CESAR são necessários para o setor aeronáutico europeu.

4. ENQUADRAMENTO REGULATÓRIO

4.1. Introdução

Este capítulo estabelece o enquadramento regulatório que contextualiza e justifica a proposta do CESAR *Framework*. A compreensão da evolução normativa da aviação civil é essencial para posicionar o modelo num continuum histórico onde *safety*, *security* e *cybersecurity* convergem progressivamente de domínios distintos para sistema integrado de gestão. A aviação civil é um dos setores mais regulados do mundo, reflexo direto da sua natureza de alto risco e do imperativo de proteger vidas humanas. Esta regulamentação desenvolveu-se historicamente através de resposta reativa a acidentes e incidentes graves, estabelecendo padrão de "aprendizagem através da tragédia" que caracteriza o setor (Reason, 1997).

O capítulo está organizado em seis secções principais. Após esta introdução, a secção 4.2 traça a evolução histórica dos três pilares regulatórios (*safety*, *security* e *cybersecurity*), desde os primórdios da aviação comercial até aos *frameworks* contemporâneos. A secção 4.3 analisa incidentes críticos que catalisaram mudanças regulatórias fundamentais, demonstrando como tragédias impulsionaram avanços normativos. A secção 4.4 examina o IOSA como referencial de excelência operacional internacional. A secção 4.5 detalha a regulamentação europeia atual de cibersegurança (NIS2, Part-IS, (UE)AI Act, ISO/IEC 27001), estabelecendo o contexto normativo direto do CESAR. A secção 4.6 analisa criticamente a convergência entre os três pilares, identificando sinergias e desafios de integração. Finalmente, a secção 4.7 sintetiza o enquadramento regulatório como base para a análise técnica do EASA Part-IS no Capítulo 5 (ISO/IEC 27001, 2022; UE 2023/203, 2023; UE 2024/1689, 2024).

4.2. Evolução Histórica dos Pilares Regulatórios

A aviação moderna[7] nasceu da combinação entre engenho e experimentação, culminando no primeiro voo motorizado dos irmãos Wright em 1903, em Kitty Hawk. O *Flyer*, equipado com motor próprio e um sistema inovador de controlo, demonstrou a viabilidade do voo controlado e inaugurou o rápido desenvolvimento que levou aos sistemas aéreos complexos do século XXI.

[7] Aviation - History of flight - https://www.britannica.com/technology/history-of-flight

A aceleração tecnológica intensificou-se com a Primeira Guerra Mundial (1914–1918), quando as aeronaves passaram de missões de reconhecimento a combate, bombardeio tático e apoio logístico, impulsionando aerodinâmica, propulsão e estruturas metálicas. No período entre guerras[7], o excedente de aeronaves e pilotos favoreceu rotas regulares de correio e passageiros, principalmente nos EUA e na Europa, exigindo instituições para pesquisa e normalização técnica: em 1915, os EUA criaram o NACA, precursor da NASA[8], para fomentar ciência aplicada e apoiar a regulação.

Em paralelo, surgiram as primeiras iniciativas diplomáticas de regulação do espaço aéreo. A Primeira Conferência Internacional de Navegação Aérea (Paris, década de 1910) inaugurou o debate sobre soberania. Em 1919, dois marcos: a *International Air Traffic Association* (precursora da atual IATA) [9] e a Convenção de Paris, primeiro tratado multilateral de navegação aérea, que consagrou a soberania estatal sobre o espaço aéreo e definiu nacionalidade de aeronaves, licenças e regras de tráfego.

A inflexão global veio com a Convenção de Chicago (1944), que criou a ICAO e seus *Standards and Recommended Practices* (SARPs)[10], padrões para operações, certificação, meteorologia, telecomunicações, navegação e investigação de acidentes, instaurando uniformidade e previsibilidade. Em 1945, nasceu em Havana a IATA[9], que passou a coordenar aspetos operacionais, tarifários e técnicos de forma global. A interação ICAO–IATA consolidou uma governança orientada para segurança, interoperabilidade e eficiência, estrutura que permanece central até hoje.

Nos EUA, *o Federal Aviation Act* (1958)[11] criou a FAA, unificando regulação de segurança operacional, ATC (*Air Traffic Control*), certificação de aeronaves e licenças, e influenciando padrões globais em cooperação com a ICAO. Na Europa, a criação da EASA[12] em 2002 (Regulamento (CE) n.º 1592/2002) encerrou gradualmente a JAA, conferindo competência vinculativa à União Europeia e posicionando a Agência como protagonista da harmonização regulatória e voz europeia junto à ICAO.

[8] The First Century of Flight NACA/NASA Contribution to Aeronautics - https://www.nasa.gov/history/centtimeline/pages/nine-15.html

[9] The Founding of IATA / https://www.iata.org/en/about/history/

[10] The Postal History of ICAO – Anexo 17 https://applications.icao.int/postalhistory/annex_17_security_safeguarding_international_civil_aviation_against_acts_of_unlawful_interference.htm

[11] A Brief History of the FAA / https://www.faa.gov/about/history/brief_history

[12] The EASA story so far - https://www.easa.europa.eu/en/20th-anniversary

Esta história não é apenas técnica, é também institucional e jurídica, marcada por cooperação internacional, novas autoridades e padrões globais, um processo que hoje enfrenta desafios de sustentabilidade ambiental, segurança operacional, cibersegurança e automação baseada em IA.

A maturidade normativa da aviação foi forjada por tragédias e eventos críticos que expuseram fragilidades e catalisaram respostas institucionais robustas. Para compreender os avanços regulatórios e os mecanismos de gestão de riscos, distingue-se *safety* e *security*:

"*Safety is the state in which the risk of harm to persons or property is reduced to, and maintained at or below, an acceptable level through a continuing process of hazard identification and safety risk management*" (Annex 19, 2013).

"*Aviation security is the safeguarding of civil aviation against acts of unlawful interference. Such acts include hijacking, sabotage, threats to aircraft, airports, or air navigation facilities, and other related criminal activities*"(Annex 17, 2022).

Fig. 4 - Âmbitos de *Safety* e *Security*

Fonte: ICAO *Annex* 19(Annex 19, 2013) **e ICAO *annex17***(Annex 17, 2022)

A Figura 4, apresenta os âmbitos do *safety* e do *security*, enquanto *safety* previne acidentes decorrentes de falhas operacionais ou técnicas, o *security* protege contra interferência ilícita (sabotagem, terrorismo, ataques cibernéticos). A harmonização global decorre dos SARPs da ICAO[13], organizados em 19 Anexos Técnicos à Convenção de Chicago, aplicados

[13] The Postal History of ICAO – Anexo 19 https://applications.icao.int/postalhistory/annex_19_safety_management.htm

universalmente pelos Estados signatários, promovendo uniformidade, interoperabilidade e eficiência.

4.3. Incidentes Críticos que Moldaram a Regulação

A história da aviação é marcada por um ciclo contínuo de progresso técnico e aprendizado institucional, no qual cada falha grave deu origem a avanços significativos em matéria de segurança operacional (*safety*) e proteção contra interferências ilícitas (*security*). Ao longo das décadas, acidentes e incidentes de grande impacto revelaram vulnerabilidades sistémicas, lacunas regulatórias e deficiências humanas ou tecnológicas que, uma vez analisadas, impulsionaram profundas transformações nos normativos internacionais e nas práticas do setor.

Esses eventos, embora trágicos, funcionaram como verdadeiros pontos de transição, moldando o desenvolvimento de políticas de prevenção, novos padrões técnicos e estruturas de governação global. A partir das investigações conduzidas por organismos como a ICAO[13], a FAA[11] e, mais recentemente, a EASA[12], emergiram regulamentos e programas que definem a atual arquitetura da aviação civil, desde a criação de sistemas de gestão da segurança (SMS) até ao fortalecimento das medidas de *security* e cibersegurança.

Entre os casos mais emblemáticos que impulsionaram essas mudanças estruturais na regulação e nas práticas de segurança da aviação civil, destacam-se os seguintes acontecimentos históricos.

Colisão no Grand Canyon (1956). A colisão aérea entre um Lockheed L-1049 da TWA e um Douglas DC-7 da United Airlines, que resultou em 128 mortes, expôs falhas críticas no sistema de controlo de tráfego aéreo. O desastre levou à criação da *Federal Aviation Administration* (FAA) em 1958, estabelecendo um novo paradigma regulatório nos Estados Unidos[11].

Sequestro do voo 317 (1961)[11]. O desvio do voo da National Airlines de Miami para Havana marcou o início da regulamentação contra interferências ilícitas, conduzindo à criminalização do sequestro aéreo e ao fortalecimento do papel da ICAO na formulação de convenções internacionais de *security*[10].

Tragédia de Tenerife (1977)[14]. A colisão entre dois Boeing 747 no aeroporto de Los Rodeos, com 583 vítimas fatais, revelou falhas de comunicação e pressão operacional, motivando a

[14] Tenerife airport disaster - https://www.britannica.com/event/Tenerife-airport-disaster

criação do *Global Aviation Safety Plan* (GASP) e a institucionalização do *Crew Resource Management (*CRM)[13].

Atentados de 11 de setembro (2001)[15]. Os ataques terroristas contra os Estados Unidos transformaram o conceito de *security* na aviação, levando à criação da TSA[11] (*Transportation Security Administration*), à implementação do *Aviation and Transportation Security Act*[11] e ao reforço global do Anexo 17 da ICAO[10], consolidando o S*ecurity* como um dos pilares estruturais da aviação civil contemporânea, ao lado do *Safety*.

Acidente do voo HCY522 da Helios Airways (2005)[16]. O episódio conhecido como "avião fantasma" destacou falhas humanas e de *design* no sistema de pressurização, influenciando a criação do *Global Aviation Safety Roadmap*[17]*,* por representantes da indústria. Essa iniciativa serviu de base para a reformulação do GASP (*Global Aviation Safety Plan*)[13], que em 2006 deu origem ao *Safety Management Manual* (Doc 9859), reforçando a abordagem proativa da gestão de riscos.

Acidente do Air France 447 (2009)[18]. A perda da aeronave sobre o Atlântico, com 228 vítimas, evidenciou a necessidade de aprimorar treino e sensores de voo. Em 2010 a conferencia da ICAO, com a participação de mais de 600 membros da indústria, deu impulso para o desenvolvimento de um novo anexo dedicado ao *safety*, conduzindo à implementação do Anexo 19 da ICAO[13] e à consolidação dos programas *Safety Management System (*SMS) e *State's Safety Programme (SSP).*

A ICAO reforçou a integração com organismos multilaterais, principalmente para enfrentar ameaças emergentes, sobretudo cibernéticas. Com a Resolução 2309 (2016)[10]**,** emendou-se o Anexo 17 para detetar explosivos, mitigar ameaças internas e fomentar cultura de *security*, além de criar painéis de cibersegurança e *frameworks* de confiança digital.

No *safety*, o GASP 2020–2022[13] definiu metas e iniciativas harmonizadas a nível estatal e regional, clarificando responsabilidades dos *stakeholders* e promovendo cultura de segurança

[15] 9/11: What happened and how many people died in September 11 attacks? https://www.bbc.com/news/articles/c98elnpr0kzo

[16] Boeing 737.300- Helios Airways Flight 52, HCY522 - https://www.faa.gov/lessons_learned/transport_airplane/accidents/HCY522

[17] DOC 10161 Global Aviation Safety Roadmap https://www.icao.int/sites/default/files/safety/GASP/Documents/Doc-10161-Ed-2-Advanced-Version.pdf

[18] Air France crash 'due to pilot and technical failings - https://www.bbc.com/news/world-europe-18720915

alinhada ao crescimento do setor. Na Europa, os requisitos do SMS seguem os elementos centrais do Anexo 19 da ICAO, permitindo integração com outros sistemas (segurança física, saúde ocupacional, ambiente) e evitando sobreposições, inclusive para organizações com múltiplos certificados EASA[19]. A EASA coopera ativamente com a ICAO (com aproximadamente 50 painéis e grupos técnicos) e com a IATA (partilha de informação de segurança), reforçando a harmonização global (Bozena Konecka-Szydelko, 2021).

A aviação é um setor que aprende sistematicamente com incidentes e desastres. ICAO, IATA, EASA e FAA atualizam normas e práticas para responder rapidamente a novas ameaças. De uma base centrada em *safety* e *security*, o ecossistema integra progressivamente cibersegurança, Resolução 2309[10], painéis de cibersegurança da ICAO, EASA Part-IS e diretrizes NIS2 refletem a convergência entre segurança operacional, proteção física e defesa cibernética, rumo a uma gestão de riscos abrangente, proativa e tecnologicamente apoiada (Easy Rules, 2025; ICAO b, 2016; UE 2022/2555, 2022).

4.4. IOSA como Referencial Internacional de *Safety*

Cada nova diretiva exige que a autoridade nacional de cada país, assegure a conformidade das companhias. A IOSA[20] (IATA *Operational Safety Audit*)**,** lançado em 2003 em cooperação com autoridades reguladoras da aviação civil, como CASA (Austrália), EASA**,** FAA e Transport Canada**,** surgiu para avaliar e auditar a conformidade com normas baseadas nos padrões da ICAO e tornou-se requisito de adesão à IATA em 2006. A partir daí, a certificação tornou-se condição de colaboração (*code-share*, alianças), diretamente ligada à segurança operacional, imagem e conformidade.

Resultados recentes reforçam a eficácia da IOSA[20], em 2023, operadores com certificação IOSA tiveram 56% menos acidentes do que não certificados. Entre 19 incidentes reportados, não houve perdas estruturais nem fatalidades. Em 2024, a IOSA ajustou o âmbito das auditorias ao perfil e aos riscos de cada operador. Essa nova abordagem da IOSA baseado no risco, conhecida com *Risk-Based* IOSA, prioriza os ISARPs por criticidade e evidências (p. ex., excursões de pista), considerando histórico e auditorias anteriores. Itens de menor criticidade podem ter frequência reduzida para concentrar recursos nos de maior impacto. Introduziu-se

[19] Safety Management System and Management System - https://www.easa.europa.eu/en/domains/safety-management/safety-management-system-sms

[20] 20 Years of Safety Improvements with IOSA- https://www.iata.org/en/pressroom/2023-releases/2023-09-20-01

ainda a *Maturity Assessment***,** que supera a lógica binária conformidade/não, conformidade, mantendo um nível base obrigatório de ISARPs. O resultado é uma auditoria mais eficaz, focada em riscos relevantes e com ganhos de eficiência.

4.5. Regulamentação Europeia de Cibersegurança da aviação Civil

A regulamentação da cibersegurança no setor da aviação tem evoluído de forma contínua para acompanhar a crescente complexidade dos sistemas críticos que sustentam as operações aéreas modernas. Em nível internacional, a Organização da Aviação Civil Internacional (ICAO) estabeleceu a Estratégia de Cibersegurança para a Aviação, que define diretrizes para a gestão sistemática dos riscos cibernéticos nas operações aéreas e ressalta a importância da proteção das infraestruturas críticas para a segurança do tráfego aéreo. Complementarmente, a Agência Europeia para a Segurança da Aviação (EASA) tem desenvolvido documentos conceptuais que integram a cibersegurança no âmbito mais amplo da segurança da aviação, reconhecendo a urgência de lidar com as vulnerabilidades resultantes da convergência tecnológica e da digitalização crescente (Aghazadeh Ardebili et al., 2024).

Comprometida a consolidar o seu enquadramento jurídico em matéria de cibersegurança aeronáutica, a EASA tem vindo, através do desenvolvimento de instrumentos normativos que atribuem responsabilidades claras a operadores, fabricantes, autoridades nacionais e entidades reguladoras. O Regulamento de Execução (UE) 2023/203 representa um marco essencial nesse processo, ao estabelecer requisitos detalhados para a gestão da segurança da informação com impacto direto na segurança operacional (*Safety)* (UE 2023/203, 2023).

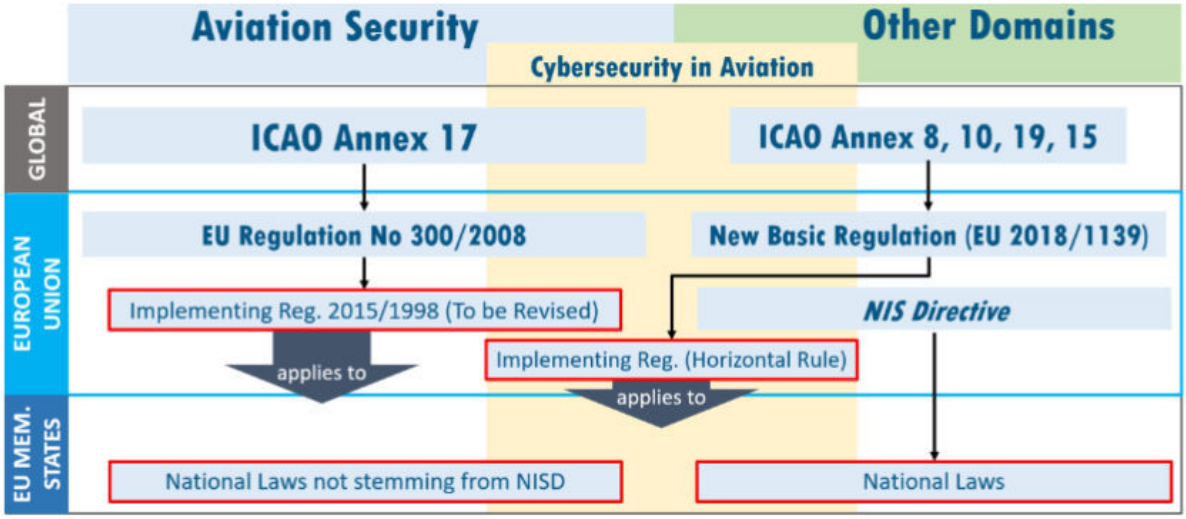
Este diploma impõe às companhias aéreas, operadores aeroportuários e prestadores de serviços aeronáuticos a obrigação de implementar e manter um Sistema de Gestão da Segurança da Informação (ISMS) robusto e formalmente documentado, destinado à identificação, avaliação, mitigação e resposta a riscos cibernéticos que possam comprometer a segurança das operações e a continuidade das atividades críticas da aviação civil (UE 2023/203, 2023).

De forma complementar, o Regulamento Delegado (UE) 2022/1645 amplia o âmbito de aplicação dessas disposições ao incluir as organizações de projeto e produção certificadas, os operadores de aeródromos e os prestadores de serviços de gestão e movimentação em pátio (*ground handling*). Ambos os regulamentos convergem para um modelo integrado de gestão da segurança da informação, em consonância com as boas práticas internacionais, nomeadamente as normas ISO/IEC 27001:2022 e o NIST 2.0 *Cybersecurity Framework*, mas devidamente

adaptadas às particularidades do ecossistema aeronáutico (UE 2022/1645, 2022; UE 2022/2555, 2022).

A Figura 5 ilustra a estrutura jurídica multinível da cibersegurança na aviação, demonstrando como os instrumentos internacionais, europeus e nacionais se articulam para assegurar uma abordagem coerente à proteção dos sistemas aeronáuticos. No nível global, o Anexo 17 da ICAO estabelece as normas de *Aviation Security*, enquanto os Anexos 8, 10, 19 e 15 abrangem domínios técnicos e operacionais relevantes para a cibersegurança na aviação (Annex 17, 2025).

Fig. 5 - Estrutura Jurídica de alto nível da segurança da aviação na EU



Fonte: EASA[21]

No contexto da União Europeia, o Regulamento (UE) n.º 300/2008 e o Regulamento de Base (UE) 2018/1139 constituem os pilares do enquadramento jurídico, complementados por regulamentos de execução e pela Diretiva NIS2, que introduz obrigações específicas de gestão de risco e reporte de incidentes (UE 2018/1139, 2018).

Entre as evoluções mais significativas neste domínio, destaca-se a alteração do Regulamento (UE) 2018/1139, que estabeleceu os princípios gerais do sistema europeu de segurança da aviação e reconheceu formalmente as interdependências entre *Safety*, *Security* e *Cybersecurity*.

[21] EASA https://www.easa.europa.eu/en/domains/cyber-security/main-easa-activities

Esta integração reflete a compreensão de que as ameaças digitais têm potencial para gerar repercussões diretas sobre a segurança operacional, e que falhas de *safety* podem, por sua vez, amplificar vulnerabilidades de *security*, adotando uma postura proativa, colaborativa e sustentada em dados empíricos, promovendo uma cultura de resiliência cibernética e fortalecendo a proteção sistémica da aviação civil europeia (Aghazadeh Ardebili et al., 2024; UE 2018/1139, 2018).

A seguir, apresentam-se os principais diplomas legais que estruturam o enquadramento normativo da cibersegurança aeronáutica na União Europeia, com os respetivos objetivos e áreas de aplicação:

- **Regulamento (UE) 2019/1583:** altera o Regulamento (UE) 2015/1998 (*Security*) e introduz requisitos técnicos para proteger as aeronaves contra interferência ilícita através de meios cibernéticos. Estabelece obrigações para fabricantes e operadores de implementarem defesas técnicas contra ameaças digitais aos sistemas embarcados (UE 2019/1583, 2019).

- **Regulamento (UE) 2023/203:** define requisitos obrigatórios de gestão da segurança da informação e mitigação de riscos cibernéticos para operadores aéreos, operadores aeroportuários e prestadores de serviços aeronáuticos. A sua aplicação plena inicia-se em outubro de 2025 (UE 2023/203, 2023).

- **Regulamento (UE) 2022/1645:** define requisitos obrigatórios de gestão da segurança da informação e de mitigação de riscos com potencial impacto na segurança da aviação para às organizações responsáveis pelo projeto e pela produção de aeronaves, motores, hélices, componentes e peças aeronáuticas, bem como aos operadores de aeródromos e aos prestadores de serviços de gestão da placa de estacionamento, excluindo apenas as entidades dedicadas exclusivamente ao projeto ou produção de aeronaves da categoria ELA2, isto é, aeronaves ligeiras europeias com massa máxima até 1 200 kg e subclasses associadas(UE 2022/1645, 2022).

- **Diretiva (UE) 2022/2555 (NIS2):** harmoniza os requisitos mínimos de cibersegurança para entidades críticas em toda a União Europeia, incluindo o setor dos transportes aéreos, impondo obrigações em matéria de gestão de riscos, reporte de incidentes e continuidade de negócio (UE 2022/2555, 2022).

- **Regulamento (UE) 2017/373:** define requisitos obrigatórios de gestão da segurança da informação e mitigação de riscos cibernéticos para os prestadores de serviços de gestão do tráfego aéreo/de navegação aérea (ATM/NSA) e de outras funções de rede da gestão do tráfego aéreo e respetiva supervisão (UE 2017/373, 2017).

Em síntese, estas iniciativas da EASA consolidam um modelo europeu de governação colaborativa da cibersegurança aeronáutica, assente na integração entre normas regulatórias, mecanismos de coordenação estratégica e ferramentas de apoio à conformidade.

4.6. Convergência do *Safety*, *Security* e *Cybersecurity*

A gestão da segurança operacional na aviação civil (SMS), conforme o Anexo 19 da ICAO, integra-se no sistema de gestão das organizações, permitindo que o *safety* seja promovido de forma transversal. O SMS baseia-se na identificação de perigos, avaliação de riscos e implementação de medidas mitigadoras antes de incidentes ou acidentes, evitando estruturas paralelas e promovendo sinergias internas. Esta abordagem reforça a tomada de decisões baseada na gestão de risco (Annex 19, 2013).

O núcleo do enquadramento exige que as organizações:

1. definam claramente responsabilidades e políticas de segurança;
2. estabeleçam objetivos e procedimentos de reporte;
3. Implementar procedimentos internos de reporte de segurança alinhados com os princípios da *just culture*;
4. identifiquem perigos, avaliem e mitiguem riscos, verificando a eficácia das medidas;
5. monitorizem a conformidade regulatória;
6. mantenham o pessoal competente, treinado e informado e;
7. documentem os principais processos do sistema de gestão.

A eficácia da gestão da segurança na aviação depende de a organização tratar o *safety* como um valor central e transversal, capaz de responder rapidamente a mudanças operacionais e riscos emergentes. Segundo Mizrak & Reyhan Akkartal (2024), a cibersegurança deve integrar-se aos sistemas organizacionais de gestão de risco, como o SMS e o CMS, através de responsabilidades claras, processos partilhados e prioridades definidas pelo impacto operacional e pelos requisitos regulamentares. O SMS permanece o principal veículo para políticas e práticas internacionais de segurança operacional (Stastny & Stoica, 2022).

A literatura destaca a necessidade de sinergia entre segurança operacional e cibersegurança, Lykou et al. (2019) defendem uma integração metodológica em que *safety* e cibersegurança se reforçam mutuamente, enquanto Stastny & Stoica (2022) afirmam que a gestão integrada deve contemplar ameaças físicas e digitais, alinhando requisitos normativos. A crescente digitalização, sistemas críticos de voo, dados sensíveis, comunicações ar–solo e sistemas embarcados, tornou a cibersegurança um componente essencial do *safety*, exigindo proteção física e virtual coordenada para assegurar continuidade e resiliência das operações (Filinovych & Hu, 2021).

Nesse contexto, o ISMS é definido como o conjunto de ferramentas, políticas, salvaguardas, abordagens de gestão de risco, formação e tecnologias destinadas a proteger o ambiente cibernético e os ativos organizacionais (Lykou et al., 2019), funcionando como complemento direto ao SMS.

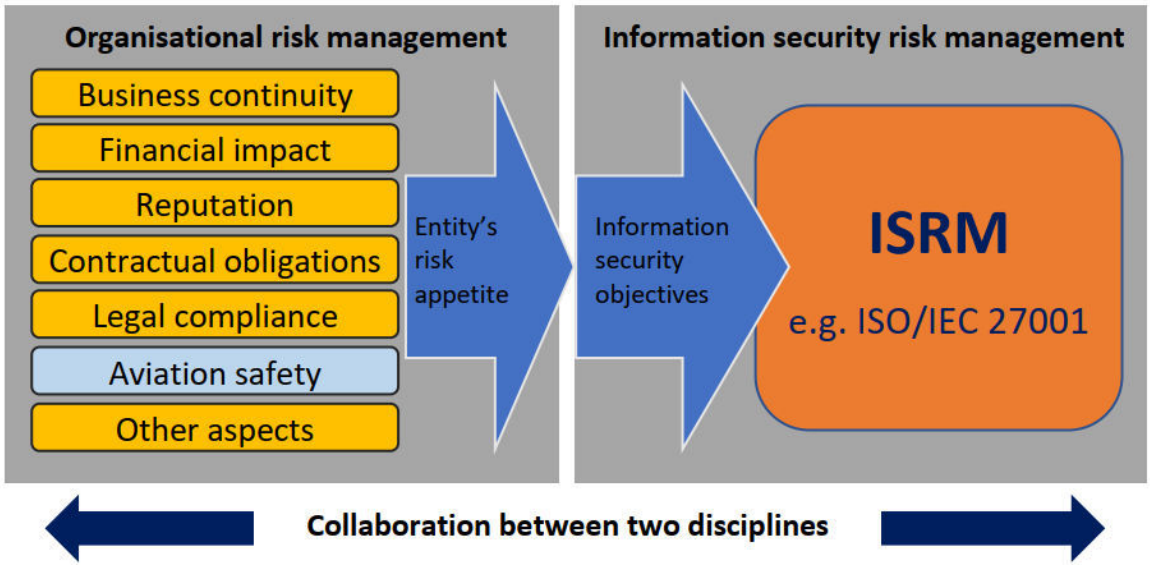
O regulamento EASA Part-IS (Regulamento (UE) 2023/203) estabelece a obrigatoriedade de integrar a gestão da segurança da informação (ISMS) com o sistema de gestão global da organização, indicando que:

"*The information security management system (ISMS) shall be integrated into the organisation's management system, including the safety management system (SMS), to ensure coordinated risk assessment and mitigation*" (EASA, 2023, AMC1 IS.GEN.200(a)).

O EASA Part-IS estabelece um processo estruturado de gestão de riscos de segurança da informação alinhado às melhores práticas internacionais, adotando uma abordagem orientada a ativos sem impor uma norma específica, e assegurando que a avaliação e o tratamento de riscos considerem o impacto na segurança operacional (Monev, 2024).

A integração entre gestão de risco organizacional e de segurança da informação, ilustrada na Figura 6, garante que os objetivos do ISMS, como os definidos na ISO/IEC 27001, estejam alinhados com o apetite ao risco da organização e com domínios críticos como continuidade de negócio, conformidade e segurança da aviação.

Fig. 6 - Integração dos ciclos de gestão de risco (SMS–ISMS)



Fonte: Adaptado de EASA (2023), AMC & GM to Part-IS.I.OR.

Em síntese, a gestão integrada de riscos na aviação exige que o *safety* e cibersegurança sejam tratados como domínios complementares, cada um preservando sua especialização, mas conectados por mecanismos de coordenação, troca de informação e alinhamento regulatório. O SMS, estruturado conforme o Anexo 19 da ICAO (Annex 19, 2013).

4.7. Sinergias, Benefícios e Desafios

A harmonização entre *safety* e cibersegurança gera benefícios tangíveis em três dimensões principais:

1. Eficiência organizacional - A integração evita redundâncias de processos, reduz custos de auditoria e permite o aproveitamento de mecanismos já existentes (por exemplo, canais de reporte, planos de contingência e controlos operacionais).

2. Gestão holística do risco - Ao correlacionar vulnerabilidades cibernéticas com consequências operacionais, as organizações podem quantificar o impacto real de um ciberataque sobre o *safety*. Por exemplo, um ataque ao *flight dispatch system* ou ao *Electronic Flight Bag* pode interromper comunicações e comprometer a tomada de decisão da tripulação.

3. Conformidade e resiliência - Um ISMS alinhado ao SMS assegura conformidade simultânea com normas ISO e regulamentos EASA, fortalecendo a postura de

compliance e a capacidade de resposta a incidentes complexos (Lykou et al., 2018; Monev, 2024).

Além disso, a integração promove transparência e cultura de segurança, pilares do conceito de *Just Culture*, fundamental à aviação. A gestão partilhada do risco cibernético incentiva a comunicação interna de vulnerabilidades sem punição, reforçando o *awareness* e a confiança institucional.

Apesar dos avanços, a integração enfrenta obstáculos significativos. A literatura identifica a escassez de profissionais especializados, a dispersão de responsabilidades e a resistência organizacional à mudança como fatores críticos (Filinovych & Hu, 2021). Além disso, a sobreposição conceptual entre segurança operacional e digital pode gerar ambiguidades de competência e conflitos na priorização de controlos.

Stastny & Stoica (2022) alertam que a co-asseguração total (*full co-assurance*) tende a diluir responsabilidades e reduzir a eficácia. Assim, a integração deve ocorrer por sincronização e cooperação estruturada, e não por fusão de sistemas. Cada domínio deve preservar a sua especialização, mantendo pontos de convergência claros, como a gestão de riscos, o reporte de incidentes e a comunicação entre CISO e *Safety Manager*.

Mizrak & Reyhan Akkartal (2024) acrescentam que a integração efetiva requer priorização baseada em impacto operacional, de modo que os recursos de segurança cibernética se concentrem nas vulnerabilidades com maior potencial de afetar a segurança de voo. Essa priorização é coerente com o princípio de aceitação condicionada de risco previsto no *AMC1 IS.I.OR.205(d)* do EASA Part-IS, que exige revisão contínua sempre que haja mudanças significativas no contexto tecnológico ou organizacional (Easy Rules, 2025).

A integração entre ISMS e SMS é reforçada pela convergência metodológica entre normas internacionais. A ISO/IEC 27005 fornece a base para avaliação e tratamento de riscos de segurança da informação, enquanto a ISO 31000 e o EUROCAE ED-201A descrevem abordagens compatíveis com o ambiente aeronáutico. A EASA Part-IS, ao exigir o alinhamento entre gestão de riscos de informação e gestão de *safety*, transforma essas boas práticas em requisitos jurídicos obrigatórios, criando um sistema coerente e verificável de segurança integrada (Monev, 2024).

O uso de plataformas de Governança, Risco e Conformidade (GRC), conforme recomendado por Monev (2024), permite automatizar processos, atribuir responsabilidades, monitorizar eficácia e documentar evidências de conformidade. Tais ferramentas também facilitam a correlação entre incidentes cibernéticos e eventos operacionais, criando uma visão sistémica dos riscos e reforçando a resiliência organizacional.

A convergência entre *safety* e cibersegurança representa uma evolução inevitável no setor aeronáutico. O SMS continua a garantir a identificação e mitigação proativa de perigos operacionais, enquanto o ISMS assegura a proteção dos sistemas e dados críticos. Quando operam de forma integrada, estes sistemas permitem avaliar o risco de forma multidimensional, combinando critérios técnicos (CIA) e operacionais (severidade, probabilidade, impacto no voo) (Monev, 2024).

Delgado-Aguilera et al. (2024) sublinham que a integração metodológica de *safety* e cibersegurança reforça a capacidade de resposta a ameaças emergentes e reduz a fragmentação regulatória. Assim, o EASA Part-IS surge como o elo regulatório que unifica essas disciplinas, enquanto promove uma abordagem proativa de gestão de risco baseada em evidência.

Em conclusão, a harmonização entre *Safety*, *Security* e Cibersegurança transcende o âmbito técnico e representa uma transformação estrutural na forma como o setor aeronáutico concebe e gere o risco. A EASA consolida esse avanço ao introduzir um quadro regulatório que institucionaliza a integração entre o ISMS e o SMS, promovendo uma cultura de segurança informacional e operacional baseada em dados, colaboração e melhoria contínua. Ao alinhar-se com os referenciais internacionais, *ISO/IEC 27001, ISO/IEC 27005, ISO 31000* e EUROCAE ED-201A, o modelo europeu assegura coerência metodológica e governança comum para riscos tecnológicos e operacionais. No entanto, o verdadeiro êxito dessa integração depende da maturidade organizacional, da capacitação técnica e da adesão cultural a um paradigma de segurança integrada, em que a informação e a operação são tratadas como elementos indissociáveis da mesma missão: preservar a continuidade, a confiabilidade e a segurança da aviação. Assim, a integração entre SMS e ISMS não apenas responde às exigências regulatórias atuais, mas estabelece os alicerces de uma aviação resiliente, digital e segura, preparada para enfrentar os desafios cibernéticos e operacionais das próximas décadas.

5. EASA PART-IS: ANÁLISE TÉCNICA

5.1. Introdução

O Regulamento (UE)2023/203, em conjunto com o Regulamento (UE)2022/1645 da EASA, conhecido como EASA Part-IS - *Information Security*, onde o elemento central do ISMS é a gestão integrada da governança, risco e conformidade **(***Governance, Risk and Compliance* - *GRC***)**, que fornece às organizações uma estrutura para alinhar políticas de segurança da informação com os objetivos estratégicos, gerir riscos de forma contínua e assegurar a conformidade com regulamentações nacionais e internacionais.

Dessa forma, o EASA Part-IS não se limita à cibersegurança técnica, mas institucionaliza um sistema de gestão da segurança da informação (ISMS), interoperável com o *Safety Management System* (SMS) definido pelo ICAO *Annex* 19, onde as organizações devem ainda demonstrar à autoridade competente que os seus sistemas estão em conformidade, inclusive com requisitos transversais como formação de pessoal, integração com o SMS (*Safety Management System*) e proteção contra ameaças internas (Annex 19, 2013; Easy Rules, 2025) .

A EASA descreve o Part-IS como um "sistema de defesa em profundidade" (*defence-in-depth*), que abrange políticas, processos, tecnologia, competências humanas e reporte regulatório.

O regulamento EASA Part-IS complementa o Regulamento (UE)2018/1139, que estabelece as bases comuns para a aviação civil europeia. Para apoio na implementação, a EASA disponibiliza material para decisões interpretativas, designada *Easy Access Rules for Information Security,* com os mínimos aceitáveis para a implementação do regulamento através do documento *Acceptable Means of Compliance* (AMC) *e Guidance Material* (GM) (EASA Cyber, 2025).

5.2. Análise das Cláusulas IS.I.OR.200 a IS.I.OR.260

O presente capítulo dedica-se à análise aprofundada do Anexo II – Part-IS.I.OR, que estabelece os requisitos organizacionais do Sistema de Gestão da Segurança da Informação (ISMS) aplicáveis aos operadores aéreos e demais entidades do setor aeronáutico europeu. O objetivo é oferecer uma visão estruturada e interpretativa de cada elemento normativo, destacando de forma especial o processo de gestão de risco, reconhecido como o núcleo central do regulamento e como o alicerce conceptual do modelo proposto nesta dissertação.

A análise foi desenvolvida com base nos documentos oficiais da EASA, nomeadamente o *Easy Access Rules for Information Security*, os *Acceptable Means of Compliance* (AMC) e o *Guidance Material* (GM), que complementam o regulamento com orientações práticas e meios aceitáveis de conformidade. Estes instrumentos fornecem a estrutura técnica e metodológica necessária para compreender a aplicação real dos requisitos do EASA Part-IS no contexto operacional das organizações aeronáuticas, permitindo identificar as sinergias entre cibersegurança, segurança operacional (*Safety*) e gestão integrada de riscos (Easy Rules, 2025).

a) IS.I.OR.200 – Estabelecimento do ISMS

O ponto de partida do EASA Part-IS é a criação formal do *Information Security Management System* (ISMS).

A organização deve estabelecer, documentar e manter um sistema proporcional à sua dimensão e complexidade, definindo políticas, objetivos e responsabilidades claras para a proteção da informação crítica. A alta direção tem responsabilidade direta pela aprovação das políticas e pela provisão dos recursos necessários.

b) IS.I.OR.205 – *Risk Assessment*

A cláusula 205 constitui o núcleo operativo do EASA Part-IS, pois define o processo formal de identificação e avaliação de riscos de segurança da informação. A organização deve reconhecer ameaças e vulnerabilidades que possam afetar os ativos críticos, avaliar o impacto em termos de confidencialidade, integridade e disponibilidade (CIA) e, principalmente, analisar como esses impactos podem comprometer a segurança operacional (*safety*). A EASA exige que a avaliação de risco considere a relação direta entre *cybersecurity* e *safety*, o que obriga a integrar a metodologia do ISMS com o processo do SMS definido no ORO.GEN.200.

c) IS.I.OR.210 – *Risk Treatment*

O EASA Part-IS não se limita a exigir a avaliação dos riscos, ele obriga também à definição e implementação de medidas de mitigação adequadas. O IS.I.OR.210 estabelece que a organização deve elaborar um plano de tratamento de risco (*Risk Treatment Plan* – RTP), documentando ações, responsáveis, prazos e indicadores de eficácia. Essas medidas podem incluir controlos técnicos (por exemplo, *firewalls*, segmentação de rede), controlos administrativos (políticas, segregação de funções) e controlos humanos (formação e

sensibilização). O AMC 1 IS.I.OR.210 determina que o RTP deve ser revisto periodicamente, garantindo que as ações continuam eficazes.

d) IS.I.OR.215 – *Internal Reporting Scheme*

O regulamento prevê um mecanismo interno de comunicação, designado *Internal Reporting Scheme*, que permite reportar vulnerabilidades, fraquezas ou incidentes de segurança da informação. Este sistema tem dois objetivos principais: promover uma cultura de reporte e transparência, onde qualquer colaborador possa comunicar ocorrências sem receio de sanções; garantir que tais relatórios alimentem o processo de gestão de risco e a aprendizagem organizacional.

e) IS.I.OR.220 – *Incident Detection, Response and Recovery*

Esta cláusula obriga a organização a estabelecer procedimentos de deteção, resposta e recuperação de incidentes de segurança da informação. O processo deve cobrir todas as fases: identificação, contenção, erradicação, recuperação e *lessons learned*. Os incidentes devem ser analisados de forma estruturada, e as conclusões utilizadas para reforçar o ISMS.

f) IS.I.OR.225 – *External Reporting Scheme*

Complementando o requisito anterior, o IS.I.OR.225 introduz a obrigatoriedade de reporte externo de incidentes às autoridades competentes, sempre que estes tenham impacto real ou potencial na segurança operacional. A norma harmoniza-se com o Regulamento (UE)376/2014, relativo à notificação obrigatória de ocorrências na aviação civil. As organizações devem definir procedimentos claros sobre o que reportar, quando e a quem. Este requisito reforça a cultura de transparência e aprendizagem coletiva.

g) IS.I.OR.230 – *Contracting of Information Security Management Activities*

As organizações que subcontratem partes do seu ISMS devem garantir que os prestadores de serviços externos cumprem os mesmos níveis de segurança exigidos internamente. O EASA Part-IS determina que os contratos incluam cláusulas específicas de segurança, mecanismos de auditoria e processos de monitorização.

h) IS.I.OR.235 – *Personnel Requirements*

A segurança da informação depende não apenas de sistemas técnicos, mas sobretudo de pessoas competentes e conscientes dos riscos. O IS.I.OR.235 exige que todas as funções

com responsabilidades de segurança recebam formação adequada e contínua, e que as competências sejam mantidas e verificadas. A EASA recomenda que esta formação esteja alinhada com as funções desempenhadas, incluindo técnicos, gestores, tripulações e pessoal de manutenção. Este requisito corresponde ao Elemento 4.2 do SMS ("*Safety Training and Education*").

i) IS.I.OR.240 – *Record-Keeping*

O EASA Part-IS requer a manutenção de registos completos e protegidos de todas as atividades do ISMS, avaliações de risco, incidentes, auditorias, planos de tratamento e comunicações. A integridade e disponibilidade desses registos devem ser garantidas, servindo como evidência durante auditorias EASA ou Autoridades competentes.

j) IS.I.OR.245 – *Information Security Management Manual* (ISMM)

A organização deve consolidar a estrutura do ISMS num Manual de Gestão da Segurança da Informação (ISMM), descrevendo políticas, procedimentos, responsabilidades e interfaces com outros sistemas de gestão.

k) IS.I.OR.250 – *Changes to the ISMS* (*Management of Change*)

Qualquer alteração tecnológica, organizacional ou de processo que possa afetar a segurança da informação deve ser analisada previamente quanto ao risco. Esta cláusula introduz o princípio de *Management of Change* (MoC) no contexto da cibersegurança, garantindo que mudanças não criam vulnerabilidades inesperadas.

l)* IS.I.OR.255 – *Contracting of* ISMS *Activities

Este requisito reforça as disposições do IS.I.OR.230, especificando que atividades críticas do ISMS realizadas por terceiros devem ser supervisionadas pela organização certificada. A responsabilidade final pela segurança permanece sempre com o operador.

m)* IS.I.OR.260 – *Continuous Improvement and Maturity

A cláusula 260 encerra o ciclo do EASA Part-IS, exigindo que o ISMS seja monitorizado, avaliado e continuamente melhorado. A organização deve definir indicadores de desempenho (KPIs), realizar auditorias internas e revisões de gestão, e utilizar lições aprendidas para aperfeiçoar controlos e processos. O *Guidance Material* da EASA

recomenda que o progresso seja medido com base em níveis de maturidade (de 1 a 5), indo de um sistema inicial até um ISMS otimizado e plenamente integrado com o SMS.

A análise detalhada do EASA Part-IS evidencia a consolidação de um quadro regulatório robusto e harmonizado, que visa integrar a gestão da segurança da informação (ISMS) às práticas tradicionais de segurança operacional (SMS), promovendo uma abordagem unificada para a mitigação de riscos técnicos, humanos e organizacionais. Este regulamento reforça a interdependência entre *safety*, *security* e cibersegurança, traduzindo em requisitos jurídicos os princípios já delineados pela ICAO no *Annex 19* e pelas normas internacionais da série ISO/IEC 27000. Assim, o EASA Part-IS representa a materialização prática da filosofia de gestão integrada do risco, ao alinhar os processos de identificação, avaliação e mitigação de ameaças digitais com os mecanismos de reporte, monitorização e melhoria contínua do SMS (Annex 19, 2013).

No seguimento desta análise, apresenta-se a Tabela 14, que sintetiza as correlações fundamentais entre os elementos estruturais do EASA Part-IS, da ISO/IEC 27001 e do ICAO *Annex* 19, evidenciando os pontos de convergência, complementaridade e reforço mútuo entre os sistemas de gestão, com vista à construção de um modelo coerente de segurança integrada na aviação civil europeia (Annex 19, 2013; EASA Cyber, 2025).

Tabela 14 - Mapeamento Comparativo EASA Part-IS × ISO 27001/27005 × SMS (*Annex* 19)

Cláusula EASA Part-IS	Tema principal	Equivalência ISO	Correspondência SMS (Annex 19 / Part-CAMO.A.200)
IS.I.OR.200	*ISMS Scopo*	ISO 27001 (4–10) - Contexto, liderança, planeamento	*SMS Element 1-Safety Policy & Objectives*
IS.I.OR.205	*Risk Assessment*	ISO 27005 (6) - Avaliação de riscos	*SMS Element 2- Safety Risk Management*
IS.I.OR.210	*Risk Treatment*	ISO 27005 (7) - Tratamento de risco	*SMS Element 2.3- Risk Mitigation*
IS.I.OR.215	*Internal Reporting Scheme*	ISO 27001 (10.1) - Comunicação interna	*SMS Element 3.1- Safety Reporting*
IS.I.OR.220	*Incident Detection, Response & Recovery*	ISO 27035 (8–10) - Gestão de incidentes	*SMS Element 3.2- Safety Investigation*
IS.I.OR.225	*External Reporting Scheme*	Reg. (UE) 376/2014 - *occurrence reporting*	*SMS Element 3.3- External Reporting-*
IS.I.OR.230	*Contracting of ISM Activities*	ISO 27036 - *Security in Supplier Relationships*	*SMS Element 1.4- Safety Accountabilities*
IS.I.OR.235	*Personnel Requirements*	ISO 27002 (6) - Competências e treino	*SMS Element 4.2 – Safety Training & Education*
IS.I.OR.240	*Record-Keeping*	ISO 27001 (9.2 / 9.3) - Avaliação e registos	*SMS Element 4.3- Safety Documentation -*
IS.I.OR.245	*IS Management Manual (ISMM)*	ISO 27001 (7.5) - Informação documentada	*SMS Element 4.3- Manual SMS*
IS.I.OR.250	*Changes to the ISMS (MoC)*	ISO 27001 (8.1) - Controlo de mudanças	*SMS Element 2.2 - (MoC)- Management of Change*
IS.I.OR.255	*Contracting of ISMS Activities*	ISO 27036 (5) - Gestão de fornecedores	*SMS Element 1.4- Accountability e Oversight*
IS.I.OR.260	*Continuous Improvement and Maturity*	ISO 27001 (10.2) - Melhoria contínua	*SMS Element 4.1- Safety Performance Monitoring & Measurement*

Fonte: Elaboração com base no *EASA Part-IS (Regulamento UE 2023/203)*, *ICAO Annex 19* e *IS/ 27001*

5.3. O Coração do Regulamento: A Gestão de Risco no EASA Part-IS

A perspetiva de risco constitui um elemento central do ISMS no contexto da segurança da aviação, servindo como base para a tomada de decisões transparentes e para a priorização dos controlos e opções de tratamento de riscos. Neste sentido, compreender a avaliação, o tratamento e a monitorização dos riscos de segurança da informação, em articulação com a gestão dos riscos do *Safety,* assegura que eventuais vulnerabilidades com impacto na segurança de voo serão devidamente tratadas. Esta dimensão envolve principalmente: (EASA Cyber, 2025)

a) Identificação de ameaças (*Identify Threats*): compreender as ameaças específicas enfrentadas pela organização, desde ciberataques até erros humanos e vulnerabilidades sistémicas;

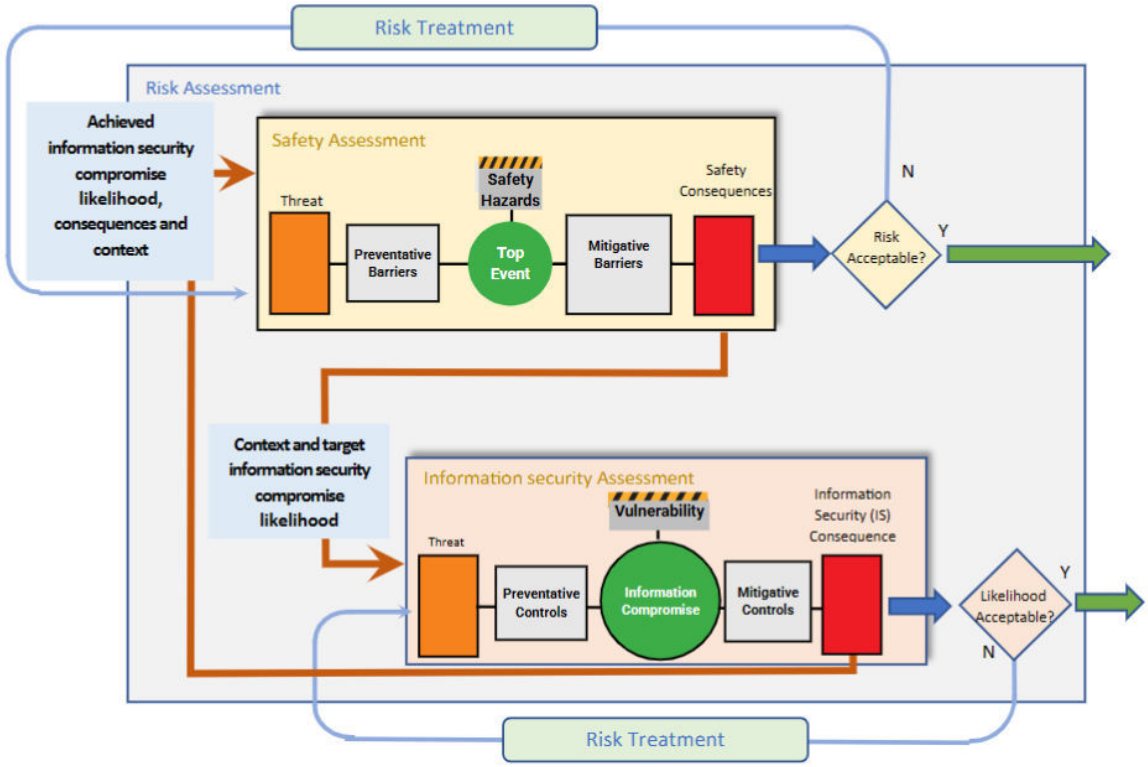
b) Avaliação de vulnerabilidades (*Assess Vulnerabilities*): analisar fragilidades em sistemas de TI, processos operacionais e fatores humanos que possam ser explorados;

c) Avaliação de impactos (*Evaluate Impacts*): determinar de que forma as ameaças identificadas podem afetar as operações, a segurança e a conformidade regulatória;

d) Priorização de riscos (*Prioritize Risks*): concentrar-se nos riscos mais críticos, aplicando uma abordagem sistemática que assegure a alocação de recursos onde estes são mais necessários.

A perspetiva de risco integra requisitos de proteção, níveis de exposição e critérios de aceitação, orientando estratégias de resposta consistentes e alinhadas com padrões reconhecidos, o que reforça a interdependência entre cibersegurança e segurança da aviação. Assim, o processo de gestão de riscos combina avaliações de *safety* com níveis de aceitação de riscos de segurança da informação, permitindo tratar vulnerabilidades que possam afetar a segurança operacional. A Figura 7 ilustra essa articulação entre os processos de avaliação de *safety* (SAP) e de segurança da informação (ISAP), evidenciando como um compromisso da informação pode impactar diretamente o risco operacional.

Fig. 7 - Representação *Bow-tie* da gestão dos riscos de segurança operacional da aviação decorrentes de ameaças à segurança da informação



Fonte: ***AMC & GM to Part-IS.I.OR Issue 1, Amendment 1***[22]

O diagrama demonstra que o SAP e o ISAP partilham a mesma lógica de avaliação de risco, baseada na identificação de ameaças, vulnerabilidades, eventos críticos e barreiras mitigadoras. Enquanto o ISAP avalia compromissos de confidencialidade, integridade e disponibilidade, o SAP analisa o impacto dessas falhas na segurança de voo. O ciclo de retroalimentação entre ambos reflete a melhoria contínua prevista no Part-IS: o ISAP fornece dados sobre incidentes de informação e o SAP devolve o impacto operacional e medidas necessárias. Esta interação iterativa mantém o risco num nível aceitável e evidencia a perspetiva integrada de *safety* e *cybersecurity*, que fundamenta as etapas de identificação, avaliação, tratamento e aceitação descritas nos pontos IS.I.OR.205 e IS.I.OR.210.

5.3.1. Avaliação de Riscos de Segurança da Informação segundo o IS.I.OR.205

[22] https://www.easa.europa.eu/en/document-library/acceptable-means-of-compliance-and-guidance-materials/amc-gm-part-isior-issue-1-0

O EASA Part-IS não impõe a utilização de um *framework* específico de segurança da informação, como a ISO, o NIST ou outros, para o desenvolvimento da avaliação de riscos ou para a implementação geral da gestão de riscos. A EASA reconhece que cada *framework* possui benefícios distintos e nenhum deles é, por si só, totalmente adequado a todas as organizações, devendo ser adaptado e personalizado para atender às necessidades globais da organização e, especificamente, às exigências relacionadas com a segurança operacional da aviação (*Safety*) (EASA Cyber, 2025).

Além disso, as organizações cujos *frameworks* de segurança da informação sejam certificados por normas da indústria podem apresentar estas certificações como artefactos de suporte, mas devem demonstrar claramente a aplicabilidade dessas certificações ao âmbito deste Regulamento, conforme previsto no GM1 IS.I.OR.200.

Como destacado por Monev (2024) é crucial empregar uma ferramenta especializada de gestão de riscos de segurança da informação, evitando-se o uso de ferramentas genéricas, como planilhas Excel, que não oferecem controle automatizado nem integração com processos regulatórios. Esta ferramenta especializada deve ser configurada para gerar automaticamente tarefas e alertas baseados nos requisitos normativos aplicáveis, facilitando a conformidade contínua com o EASA Part-IS.

5.3.2. Estabelecer o âmbito - AMC1 IS.I.OR.205(a)

Para a gestão de risco, a identificação do âmbito e dos limites constitui uma etapa fundamental para a implementação e execução eficaz desse processo, exigindo da organização uma compreensão clara e abrangente de suas atividades e serviços aeronáuticos, dos processos associados, dos sistemas de informação relevantes, bem como dos fluxos de dados e trocas de informação. Essa definição estabelece a base para a delimitação do âmbito do ISMS e para a condução da avaliação de riscos.

Na gestão de risco, a definição do âmbito e dos limites é essencial para compreender as atividades, processos, sistemas e fluxos de informação da organização, constituindo a base do ISMS e da avaliação de riscos. A identificação estruturada de ativos, processos, ambientes operacionais e recursos garante rastreabilidade e coerência ao longo do ciclo de vida dos ativos, assegurando que todos os elementos com impacto potencial na segurança da informação e na segurança operacional sejam devidamente controlados. Esta abordagem sistematizada mantém o ISMS alinhado aos requisitos do EASA Part-IS.

6.1.2. Risco na partilha de informação - IS.I.OR.205(b)

A identificação e caracterização das interfaces entre organizações, como companhias aéreas, aeroportos, prestadores de serviços de navegação aérea, manutenção e meteorologia, constitui um elemento essencial na avaliação de riscos de segurança da informação. Estas interconexões operacionais envolvem o intercâmbio contínuo de dados críticos, que sustentam a segurança e a eficiência das operações aeronáuticas, mas que também representam potenciais vetores de vulnerabilidade cibernética.

Este tipo de mapeamento, base do IS.I.OR.205(b) do EASA Part-IS, reforça a importância da gestão colaborativa do risco e da integração entre os Sistemas de Gestão da Segurança da Informação (ISMS) das diferentes entidades do ecossistema aeronáutico europeu, promovendo a visibilidade e a rastreabilidade necessárias para prevenir incidentes e fortalecer a resiliência cibernética setorial.

5.3.3. Avaliação do Risco - AMC1 IS.I.OR.205(c)

Como o EASA Part-IS não impõe uma metodologia específica para a gestão de riscos de segurança da informação, as organizações devem adotar abordagens estruturadas que permitam identificar, avaliar e tratar riscos de acordo com critérios qualitativos e quantitativos. O processo deve considerar os ativos identificados nos pontos IS.I.OR.205(a) e (b) e classificar o risco em níveis, alto, médio ou baixo, segundo a probabilidade de ocorrência e as potenciais consequências sobre a segurança operacional (*Safety*).

A probabilidade é determinada com base na robustez dos controlos existentes, na eficácia das medidas de deteção e mitigação, e na capacidade técnica dos potenciais atacantes, avaliada com apoio de dados provenientes de entidades especializadas como CERTs[23], CSIRTs[24] e ISACs[25]. Já a severidade das consequências deve refletir o impacto operacional e de segurança: alta (quando há risco de fatalidades ou danos estruturais), moderada (quando há incidentes operacionais) ou baixa (com efeitos negligenciáveis).

[23] *Computer Emergency Response Team* (*CERT*) - é uma equipa especializada em resposta a incidentes.

[24] *Computer Security Incident Response Team* (*CSRT*) - É uma equipa formal responsável por gerir e responder a incidentes de segurança informática dentro de uma organização ou a nível nacional/setorial.

[25] *Information Sharing and Analysis Center* (*ISAC*) - É uma entidade colaborativa criada para partilha de informação sobre ciberameaças entre organizações de um mesmo setor

Os resultados da análise devem ser documentados e classificados conforme os critérios de aceitação de risco, que podem ser: aceitável, condicionalmente aceitável ou inaceitável. Os riscos condicionalmente aceitáveis devem estar associados a medidas compensatórias, planos de mitigação e revisão contínua, de acordo com o princípio de melhoria permanente estabelecido no GM1 IS.I.OR.260(a).

A aceitação condicional deve considerar fatores como a duração da exposição, compromissos futuros de tratamento e a maturidade da estrutura de gestão de riscos da organização, que deve englobar avaliação, tratamento e monitorização contínua. Apenas organizações com processos repetíveis e reprodutíveis de gestão de riscos, conforme GM1 IS.I.OR.260(a) (que diz respeito a melhoria continua), devem recorrer a essa categoria, garantindo a governança adequada ao longo do tempo. Segundo Monev, (2024), "*na aviação os riscos não podem ser transferidos*".

Fig. 8 - Matriz de Risco para comparação – ICAO *Annex* 13

ICAO Annex 13 >	Negligible effect	Incident	Accident
Threat scenario — potential of occurrence	**Low safety consequences**	**Moderate safety consequences**	**High safety consequences**
High	Conditionally acceptable	**Not acceptable**	**Not acceptable**
Medium	Acceptable	Conditionally acceptable	**Not acceptable**
Low	Acceptable	Acceptable	Conditionally acceptable*

Fonte EASA Easy Rules Part-IS

A estrutura desta matriz, Figura 8, baseia-se em dois eixos fundamentais: o eixo vertical, que representa a probabilidade de ocorrência de um cenário de ameaça (alta, média ou baixa), e o eixo horizontal, que reflete a gravidade das consequências sobre a segurança operacional (*negligible effect*, *incident* ou *accident*). De acordo com o modelo do *ICAO Annex 13*, que esta no AMC GM da EASA, mesmo eventos raros, quando associados a consequências graves, não podem ser considerados aceitáveis sem a implementação de medidas de mitigação. Essa premissa é particularmente relevante para riscos relacionados à integridade e disponibilidade

de sistemas digitais críticos, cuja falha pode gerar condições inseguras e, em casos extremos, contribuir para acidentes (EASA Cyber, 2025).

A gestão de riscos, neste contexto, deve assentar numa abordagem metodológica, rigorosa e contínua, garantindo que as avaliações sejam repetíveis, assegurando consistência e comparabilidade ao longo do tempo, e reprodutíveis, permitindo que diferentes especialistas, operando sob as mesmas condições, obtenham resultados equivalentes. Essa característica reforça a credibilidade, a robustez e a rastreabilidade do processo analítico.

O ciclo de gestão de riscos deve ainda ser iterativo, possibilitando o refinamento progressivo dos cenários à medida que novas vulnerabilidades e vetores de ataque são identificados. Este dinamismo requer monitorização contínua de indicadores-chave de risco, revisões sistemáticas de ameaças emergentes e avaliação periódica da eficácia dos controlos implementados. A integração com fornecedores, prestadores de serviços e parceiros da cadeia de valor é igualmente essencial, dado que fragilidades externas podem ter repercussões diretas sobre a segurança da informação e, por consequência, sobre o *Safety*.

A etapa de identificação dos cenários de ameaça visa descrever as possíveis formas de materialização de ataques, considerando a fonte, o vetor, as vulnerabilidades, os controlos existentes e as consequências potenciais para a segurança da aviação. O resultado esperado é uma lista de cenários representativos que sirva de base para a avaliação e o tratamento do risco.

Entre os principais elementos dessa caracterização destacam-se:

- **Fonte da ameaça**: origem do ataque (ex.: ator interno, *hacker* externo, fornecedor comprometido);
- **Vetor de ataque**: método e caminho de exploração do ativo (ex.: *phishing*, acesso remoto, rede sem segurança);
- **Controlos de mitigação**: medidas existentes que possam reduzir a probabilidade ou o impacto do incidente;
- **Consequências**: efeitos diretos ou indiretos sobre a segurança da aviação (ex.: falha de sistemas críticos, interrupção de serviços, degradação operacional).

Por fim, a identificação de cenários deve apoiar-se em catálogos e referências reconhecidas, mas deve igualmente ser atualizada à luz das ameaças emergentes e das tendências observadas nos setores tecnológicos e aeronáuticos. Essa prática assegura que o processo de avaliação permaneça relevante, atualizado e alinhado com a evolução do panorama global de cibersegurança.

5.3.4. Avaliação periódica do Risco IS.I.OR.205(d)

A frequência das revisões da avaliação de riscos deve considerar o nível de risco, a criticidade e a complexidade dos ativos envolvidos. O objetivo é permitir a reavaliação da probabilidade e do impacto, sempre que houver mudanças relevantes que possam alterar os resultados anteriores.

Desta forma é possível assegurando a melhoria contínua da qualidade das análises, a eficácia dos controlos existentes e a identificação de novas ameaças, além de atualizar o plano de tratamento dos riscos com a identificação das alterações organizacionais, mantendo assim uma visão panorâmica global dos riscos emergentes. Para tal, as revisões e suas periodicidades devem ser documentadas, envolver os responsáveis pelo risco e alinhar-se com os processos de gestão de mudanças e de governação da segurança da informação da organização.

5.3.5. Tratamento do Risco IS.I.OR.210(a)

Os riscos classificados como inaceitáveis, conforme o disposto no ponto IS.I.OR.205 do EASA Part-IS, exigem a implementação de um processo formal de tratamento de risco, que contemple medidas específicas de segurança da informação aplicáveis a todas as fases do ciclo de vida dos ativos. Este processo deve materializar-se num plano de tratamento de risco, no qual sejam claramente definidos os objetivos, os métodos, as prioridades e os prazos de execução, bem como os responsáveis pela sua implementação e monitorização.

A gestão de topo deve validar e aprovar o plano, garantindo o alinhamento com a estratégia organizacional e a adequada comunicação com a autoridade competente, sobretudo nos casos em que os riscos residuais possam resultar em condições inseguras para as operações aeronáuticas. Qualquer atraso na execução das medidas previstas deve ser devidamente justificado e documentado, podendo ser temporariamente aceite apenas mediante a adoção de controles compensatórios ou medidas reativas que assegurem um nível de proteção equivalente.

O plano de tratamento deve igualmente funcionar como instrumento de comunicação e evidência regulatória, demonstrando à autoridade competente e às organizações parceiras o estado de implementação das ações corretivas e o controlo efetivo dos riscos partilhados. Este mecanismo reforça a transparência e a responsabilização interorganizacional, essenciais à gestão integrada da cibersegurança no setor aeronáutico.

Em conformidade com o ponto IS.I.OR.205(d), o plano de tratamento deve ser objeto de revisão regular ou condicional, sempre que ocorrerem alterações significativas no contexto tecnológico, organizacional ou operacional, garantindo que as medidas continuam eficazes e adaptadas à evolução das ameaças.

Importa sublinhar que as ações de mitigação implementadas não devem, em hipótese alguma, originar novos riscos para o *Safety*. Esta premissa traduz o princípio da *co-assurance* entre segurança operacional e cibersegurança, assegurando que o fortalecimento dos controlos digitais não compromete a integridade, a disponibilidade ou a fiabilidade dos sistemas críticos da aviação.

5.3.6. Comunicação dos Riscos IS.I.OR.210(b)

Nos termos do ponto IS.I.OR.240 do EASA Part-IS, a comunicação eficaz dos resultados da avaliação de riscos constitui um elemento essencial da governança da segurança da informação na aviação. É imperativo que tanto os responsáveis designados nas alíneas (a) e (b), quanto todo o pessoal operacional e técnico potencialmente impactado, sejam devidamente informados sobre as conclusões da análise conduzida em conformidade com o IS.I.OR.205.

O regulamento estabelece a necessidade de comunicação externa estruturada com organizações com as quais existam interfaces funcionais ou tecnológicas, de modo a garantir uma abordagem coordenada à gestão de riscos partilhados. Esta cooperação interorganizacional é um dos pilares da ciber-resiliência sistémica preconizada pela EASA, uma vez que assegura a continuidade da proteção ao longo de toda a cadeia de valor aeronáutica.

Dessa forma, a transparência e a reciprocidade na partilha de informação tornam-se instrumentos centrais para a eficácia do Sistema de Gestão da Segurança da Informação (ISMS), contribuindo simultaneamente para a preservação da segurança operacional (*Safety*) e para a conformidade regulatória europeia.

5.4. Integração entre ISMS-SMS: Fundamentos, desafios e direções de implementação

Para facilitar a implementação da EASA Part-IS, o ISMS no setor aeronáutico pode beneficiar significativamente da integração com sistemas de gestão já existentes na organização. Esta abordagem permite reduzir esforços duplicados, otimizar recursos e garantir coerência entre as diferentes áreas de gestão. Esta integração beneficia as áreas envolvidas, colocando-as em sinergias que podem ser exploradas através da integração do ISMS com outros sistemas de gestão existentes:

- **Aproveitamento de políticas e procedimentos já existentes:** a organização pode utilizar as suas políticas e procedimentos atuais como base para o ISMS, garantindo coerência e reduzindo a necessidade de documentação adicional.
- **Alinhamento do ISMS com outros sistemas de gestão:** o ISMS pode ser alinhado com outros sistemas, como o **Sistema de Gestão da Segurança Operacional (SMS)**, assegurando consistência com a estratégia global da organização.
- **Utilização dos processos de gestão de riscos já existentes:** a organização pode aplicar os seus processos de gestão de riscos atuais para identificar e avaliar riscos de segurança da informação que possam gerar impactos na segurança operacional da aviação.
- **Reutilização de controlos existentes:** controlos já implementados, como os de controlo de acessos ou gestão de incidentes, podem ser adaptados para satisfazer os requisitos de segurança da informação exigidos pelo ISMS.
- **Processo de melhoria contínua:** a organização pode aplicar os processos de melhoria contínua dos seus sistemas de gestão existentes para evoluir e otimizar continuamente o ISMS.

A análise detalhada dos requisitos IS.I.OR.200 a IS.I.OR.260 revela que o EASA Part-IS estabelece "o quê" deve ser implementado, mas fornece orientação limitada sobre "como" operacionalizar a integração ISMS-SMS exigida.

Requisitos Claros (O Quê):

- IS.I.OR.200: ISMS deve estar integrado com SMS.
- IS.I.OR.205: Avaliação de risco deve considerar impacto em *safety*,
- IS.I.OR.210: Tratamento de risco deve ser coordenado,

- IS.I.OR.215: Reporte interno deve fluir entre domínios,
- IS.I.OR.260: Melhoria contínua deve abranger ambos.

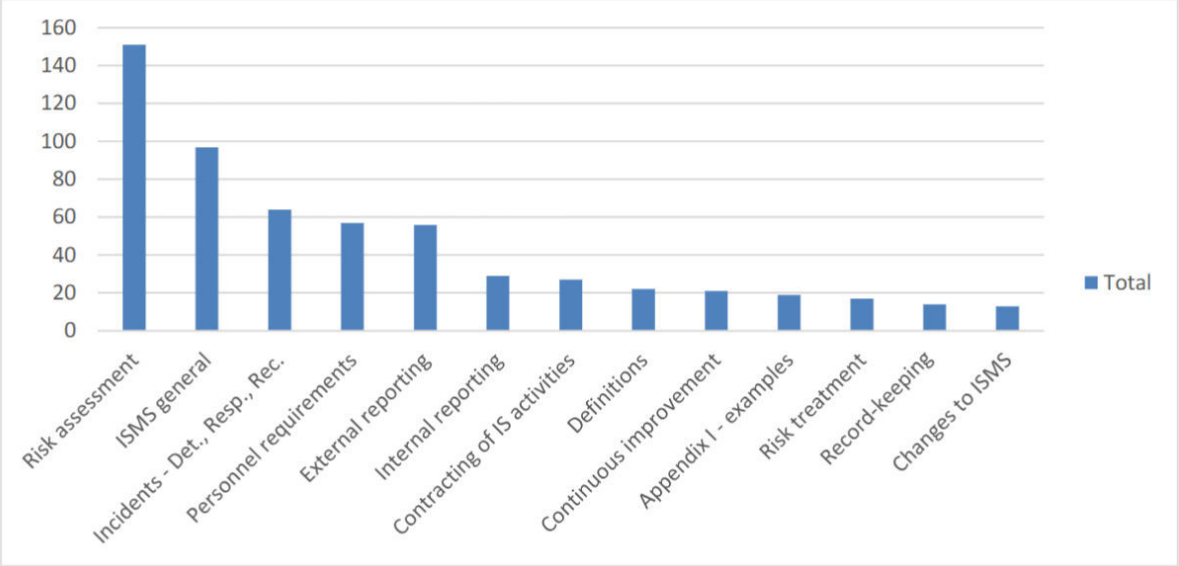
Lacunas Metodológicas (Como):

- Qual o processo específico de correlação entre risco *cyber* e *safety*?
- Como garantir que avaliação de risco *cyber* considera critérios SMS?
- Que mecanismos técnicos suportam comunicação CISO ↔ *Safety Manager*?
- Como automatizar identificação de riscos com impacto cruzado?
- Como demonstrar *compliance* de forma auditável e rastreável?

Em termos globais, a análise normativa evidencia um ecossistema regulatório robusto, porém marcado por assimetrias na implementação, sobreposição de obrigações e ausência de mecanismos de harmonização entre diferentes domínios da aviação. A introdução do EASA Part-IS representa um avanço significativo ao estabelecer requisitos claros para a gestão da segurança da informação, mas a sua integração com outras estruturas, como o SMS, a NIS2 e os referenciais internacionais, continua a exigir clarificação e uniformidade operacional.

A revisão dos regulamentos demonstra igualmente que, apesar da evolução normativa, persistem desafios estruturais: interpretações divergentes entre operadores, maturidade desigual entre Estados-Membros, escassez de orientações práticas para a articulação entre *safety* e *security* e ausência de instrumentos que suportem a implementação contínua de processos de gestão de risco alinhados com as exigências europeias. Esta constatação é reforçada pelos próprios materiais de apoio às *Explanatory Note ED Decisions* 2023/008/R, 2023/009/R e 2023/010/R, nos quais a EASA identifica elevados volumes de comentários sobre definições, âmbito do *risk assessment*, responsabilidades organizacionais, reporte, *incident handling* e integração com processos existentes, evidenciando a necessidade de clarificação, harmonização e apoio adicional para garantir uma aplicação consistente do Part-IS em toda a aviação europeia. A EASA recebeu um total de 865 comentários de 26 diferentes *stakeholders*, sobre a implementação, na Figura 9 abaixo, vemos a distribuição dos comentários por tipo (EASA, 2024).

Fig. 9 - Distribuição de comentários por área



Fonte: EASA - *Explanatory Note to ED Decisions* 2023/008/R, 2023/009/R and 2023/010/R(EASA, 2024)

Estes resultados reforçam a necessidade de modelos conceptuais capazes de traduzir os requisitos regulamentares em mecanismos claros, consistentes e aplicáveis ao contexto operacional das organizações aeronáuticas. As lacunas identificadas constituem, assim, a base para o desenvolvimento, nos capítulos seguintes, de uma proposta que procure responder de forma integrada às exigências regulatórias e às necessidades práticas das entidades reguladas.

6. INTELIGÊNCIA ARTIFICIAL APLICADA À AVIAÇÃO

6.1. Introdução e Contextualização

Este capítulo examina o estado da arte sobre aplicação de Inteligência Artificial (IA) na aviação, com foco em gestão de risco e cibersegurança, estabelecendo a fundamentação tecnológica do CESAR *Framework*. Este capítulo não é uma revisão genérica de IA, mas análise direcionada de técnicas aplicáveis à:

a) Correlação automática de riscos *cybersecurity* e *safety*,
b) Processamento de grandes volumes de dados operacionais,
c) Explicabilidade e auditabilidade (XAI),
d) Conformidade com EU AI Act.

A aviação civil atravessa uma das mais significativas revoluções tecnológicas desde a introdução da automação digital. A Inteligência Artificial (IA) emergiu como catalisadora desse processo, incorporando-se de forma transversal às operações aeronáuticas, à manutenção, à cibersegurança e à gestão de tráfego aéreo. Mais do que uma inovação técnica, a IA representa uma mudança de paradigma no modo como o setor gere informação, risco e decisão (Ahmed, 2025; Demir et al., 2024).

O carácter multidimensional da IA, combinando computação avançada, análise preditiva e aprendizagem automática, permite às organizações aeronáuticas responder à crescente complexidade dos sistemas digitais e das interações homem-máquina. A aviação moderna é hoje um ecossistema ciberfísico, composto por aeronaves altamente conectadas, sistemas de controlo de tráfego baseados em dados e redes digitais que integram operadores, autoridades e infraestruturas críticas (Xie et al., 2023). Cada elemento desse sistema produz um fluxo contínuo de dados, sensores de voo, relatórios de manutenção, registos de tráfego aéreo e *logs* de rede. A análise manual desses dados tornou-se impraticável, abrindo espaço para a automação inteligente como ferramenta de decisão estratégica (Ahmed, 2025; Demir et al., 2024).

Os avanços em *Machine Learning* (ML) e *Deep Learning* (DL) redefiniram a capacidade das organizações de prever falhas, otimizar processos e mitigar riscos cibernéticos. Essas técnicas permitiram o desenvolvimento de sistemas que aprendem padrões de comportamento e detetam desvios antes que causem impacto operacional (Kotadiya, 2024; Taleqani et al., 2018). No

domínio da segurança operacional (*Safety*), algoritmos de ML e DL processam relatórios de segurança e identificam causas subjacentes a incidentes, enquanto, no domínio da cibersegurança (*Security*), são capazes de reconhecer comportamentos anómalos em redes aeronáuticas e comunicações de satélite (Çevik & Akleylek, 2024; Xie et al., 2023).

A adoção de IA na aviação responde também à necessidade de resiliência e conformidade regulatória, num contexto em que a dependência tecnológica expõe operadores a novas vulnerabilidades. Regulamentos europeus como o EASA Part-IS (Regulamento (UE) 2023/203) e a Diretiva NIS2 (2023/2555) exigem abordagens dinâmicas de gestão de risco baseadas em evidência e monitorização contínua. A IA oferece uma camada adicional de proteção e eficiência, atuando simultaneamente como ferramenta de segurança e de *compliance* (Delgado-Aguilera et al., 2024; Sheikhi et al., 2025).

A integração de sistemas inteligentes em ambientes críticos exige atenção à explicabilidade e rastreabilidade das decisões algorítmicas. A confiabilidade desses sistemas está condicionada não apenas pela sua precisão, mas pela sua capacidade de justificar o raciocínio que conduz às decisões (Delgado-Aguilera et al., 2024). Por esse motivo, a aviação adota progressivamente os princípios da IA Explicável (*Explainable Artificial Intelligence* – XAI) e do controlo humano significativo (*Human-AI Teaming* – HAT), conforme definidos pela Agência Europeia para a Segurança da Aviação (UE 2024/1689, 2024).

Neste contexto, a inteligência artificial deixa de ser apenas uma tecnologia emergente para se tornar um elemento transformador da cultura organizacional e da governança aeronáutica, influenciando profundamente a forma como segurança, risco e responsabilidade são concebidos. Embora aumente a eficiência operacional, a IA também introduz desafios epistemológicos, éticos e regulamentares que exigem novas abordagens de análise e controlo. Kabashkin et al., (2023) reconhecem que o desenvolvimento de sistemas de IA para a aviação depende fortemente da disponibilidade, qualidade e correta manipulação de *datasets*, fator essencial para a criação de soluções que melhorem a operação, a segurança e a eficiência do setor. Contudo, o estudo não aprofunda aspetos técnicos relacionados com tipos, dimensão, curadoria ou limitações desses *datasets (Jiang et al., 2023)* .

Este capítulo explora, de forma técnica e crítica, as principais tipologias, aplicações e implicações da IA no setor aeronáutico, com base nas evidências científicas mais recentes.

6.2. Evolução e Tipologias da Inteligência Artificial na Aviação

A evolução da IA na aviação decorre de um processo gradual de digitalização iniciado com os sistemas automatizados de navegação e manutenção e consolidado pela convergência entre dados massivos (*Big Data*), computação cognitiva e aprendizagem automática. As suas tipologias mais relevantes, *Machine Learning* (ML), *Deep Learning* (DL), Aprendizagem Federada (FL), IA Generativa e IA Explicável (XAI), representam etapas sucessivas na maturidade da automação inteligente (Demir et al., 2024).

a) *Machine Learning* (ML)

O *Machine Learning* constitui o núcleo funcional da IA aplicada à aviação. Baseia-se na capacidade dos algoritmos de aprender a partir de dados históricos para reconhecer padrões, prever comportamentos e tomar decisões com base em evidências.

De acordo com Demir et al., (2024) a aprendizagem supervisionada, como *Random Forest*, *Support Vector Machines* (SVM) e *Gradient Boosting*, permite identificar relações complexas entre variáveis de segurança, detetar anomalias em séries temporais e prever falhas antes da sua ocorrência.

Estes métodos são amplamente utilizados em monitorização de motores, previsão de manutenção e análise de incidentes. Kotadiya, (2024) enfatiza que a integração de ML nos sistemas de gestão de segurança (ISMS e SMS) melhora a capacidade das equipas em detetar vulnerabilidades emergentes e reduzir tempos de resposta a ameaças.

b) *Deep Learning* (DL)

O *Deep Learning* expande a lógica do ML, recorrendo a redes neuronais artificiais com múltiplas camadas para representar relações de elevada complexidade. No estudo de Dong et al., (2021), modelos *Long Short-Term Memory* (LSTM) foram aplicados ao *Aviation Safety Reporting System* (ASRS) para analisar mais de 180 mil relatórios de incidentes.

Os resultados demonstraram que o DL consegue identificar fatores causais e padrões latentes em texto livre, apoiando a identificação de falhas organizacionais e técnicas. New & Wallace, (2025) utilizaram técnicas de *Natural Language Processing* (NLP) baseadas em BERT, obtendo mais de 90% de precisão na classificação de relatórios de segurança operacional. Esses resultados comprovam o valor do DL e do NLP como instrumentos para automatizar a

aprendizagem organizacional, transformando dados textuais em conhecimento aplicável à prevenção de incidentes.

c) Aprendizagem Federada (*Federated Learning* – FL)

A Aprendizagem Federada (FL) é uma das evoluções mais relevantes no campo da IA aplicada à aviação conectada. Ali et al., (2025) propuseram um modelo descentralizado em redes *Software-Defined Networking* (SDN) aeronáuticas, permitindo que múltiplos nós, aeronaves, estações de solo e sistemas de controlo, treinem algoritmos localmente, sem partilhar dados sensíveis.

Este paradigma assegura privacidade, integridade e colaboração, reduzindo a exposição a ciberataques e fortalecendo a resiliência das comunicações aeronáuticas. O FL é particularmente compatível com as exigências do EASA Part-IS e da Diretiva NIS2, que requerem segregação e proteção de dados críticos (UE 2022/2555, 2022; UE 2023/203, 2023).

d) IA Generativa e Modelos de Linguagem (LLMs)

A nova geração de modelos generativos, descrita por Kirwan, (2024), amplia o espectro cognitivo da IA. Baseados em *Large Language Models* (LLMs) e Redes Adversárias Generativas (GANs), estes sistemas são capazes de criar dados, simular cenários operacionais e gerar explicações linguísticas. Na aviação, estas tecnologias têm aplicações em simulações de risco, treino de pessoal, análise de incidentes e gestão preditiva de tráfego aéreo. Kirwan, (2024) destaca o conceito de *Human-AI Teaming* (HAT), em que modelos generativos funcionam como assistentes inteligentes capazes de interagir com pilotos, engenheiros e controladores, reforçando a segurança operacional através de apoio cognitivo em tempo real. Estas aplicações, embora ainda em fase experimental, apontam para uma aviação cada vez mais colaborativa entre homem e máquina.

e) IA Explicável (XAI)

Com a crescente complexidade dos modelos, surge a necessidade de garantir transparência e auditabilidade. A IA Explicável (XAI), analisada por Delgado-Aguilera et al. (2024) representa o esforço de tornar o raciocínio algorítmico inteligível para humanos, sobretudo em ambientes regulados. Na aviação, a XAI permite compreender por que razão um algoritmo classifica um evento como anómalo, validar as variáveis determinantes e documentar decisões automatizadas em auditorias de conformidade. A explicabilidade é requisito central do (EU) AI Act (2024) e

do EASA AI *Roadmap* (2023), sendo fundamental para a certificação de sistemas baseados em IA e para a aceitação institucional da automação cognitiva (EASA AI, 2025; Easy Rules, 2025).

6.3. Aplicações Operacionais da Inteligência Artificial na Aviação

A implementação da Inteligência Artificial (IA) em sistemas aeronáuticos reflete um movimento contínuo de transformação operacional, no qual o ser humano passa de executor para supervisor cognitivo. As aplicações práticas abrangem desde a prevenção de falhas e incidentes operacionais até à melhoria da eficiência e fiabilidade dos sistemas de manutenção e tráfego aéreo. A literatura científica recente demonstra que a IA se tornou um componente essencial para a modernização da aviação, integrando as dimensões de segurança, manutenção, controlo e decisão (Demir et al., 2024; Dong et al., 2021).

a) Prevenção de incidentes e apoio à decisão

A IA permite identificar, em tempo real, anomalias e tendências de risco que seriam impossíveis de detetar apenas com análise humana. No estudo conduzido por Dong et al. (2021), foram utilizados algoritmos de *Deep Learning* baseados em redes *Long Short-Term Memory* (LSTM) para processar mais de 180 mil relatórios do *Aviation Safety Reporting System* (ASRS), extraindo automaticamente fatores causais e contributivos para incidentes. Esta abordagem revelou que padrões linguísticos e contextuais podem antecipar falhas humanas e organizacionais, oferecendo suporte à prevenção proativa.

De forma complementar, New & Wallace, (2025) aplicaram *Natural Language Processing* (NLP) supervisionado através do modelo BERT, alcançando mais de 90% de precisão na classificação de relatórios de *safety*. Os autores sublinham que este tipo de IA melhora a consistência das análises e reduz significativamente o tempo de processamento de dados, permitindo que as equipas de segurança operacional se concentrem em interpretação e mitigação. Tais aplicações demonstram que a IA não substitui o julgamento humano, mas amplifica a capacidade analítica das organizações.

b) Manutenção preditiva e otimização de operações

Outra área de aplicação consolidada é a manutenção preditiva (*Predictive Maintenance*), onde sensores e algoritmos inteligentes permitem detetar padrões de degradação em motores e sistemas de bordo. Kondala & Patibandla, (2024) mostra que o uso de IA associada a sensores IoT reduziu em 20% as falhas não programadas e em 15% os custos corretivos em operadores

comerciais.

Essa abordagem, conhecida como *Condition-Based Maintenance* (CBM), representa uma transição da manutenção reativa para a manutenção baseada em condição e dados (*Data-Driven Maintenance*). Segundo o autor, "*a capacidade da IA em correlacionar parâmetros de desempenho, vibração e temperatura cria uma rede de diagnóstico contínuo que aumenta a disponibilidade da frota e reduz custos operacionais*".

c) Gestão de tráfego e operações cognitivas

A IA também desempenha um papel emergente na gestão de tráfego aéreo (ATM) e em operações cognitivas. Niraula, (2022) descreve a integração de IA em sistemas de *Safety Service Ecosystems*, com foco na interoperabilidade entre controladores, aeronaves e sistemas de solo. O estudo destaca a aplicação de algoritmos de aprendizagem automática para otimizar rotas, reduzir atrasos e detetar anomalias em comunicações ATM, permitindo uma coordenação mais eficiente e segura.

Os modelos cognitivos aplicados à gestão de tráfego utilizam técnicas de fusão de dados (*data fusion*) para combinar informações meteorológicas, geoespaciais e operacionais, resultando em decisões mais precisas e contextualizadas.

d) Cultura de segurança e interação homem–máquina

A integração da IA não se limita ao domínio técnico: transforma também a cultura de segurança e o papel humano na operação. Kirwan, (2024) explora este aspeto sob a ótica da segurança futura da aviação, defendendo que a IA pode tanto fortalecer como fragilizar a cultura de *safety*, dependendo do modo como é implementada.

O autor introduz o conceito de *Human–AI Teaming* (HAT), em que a IA atua como colaborador cognitivo, um sistema que aprende com o humano e o auxilia na tomada de decisão sob pressão. Nos níveis mais avançados de autonomia, esta colaboração exige ética, explicabilidade e confiança mútua, de modo que a IA complemente, e não substitua, o raciocínio humano. Essa visão é reforçada pelo EASA AI *Roadmap* (2023), que define a confiança algorítmica e o controlo humano significativo como princípios fundamentais para a certificação de sistemas inteligentes em contextos aeronáuticos (EASA AI, 2025).

6.4. Aplicações de Inteligência Artificial na Cibersegurança Aeronáutica

A cibersegurança aeronáutica é um domínio particularmente sensível da aviação moderna, dada a natureza interconectada das suas infraestruturas digitais. Os sistemas de bordo, redes de comunicação e plataformas de controlo são alvo crescente de ataques de *ransomware*, *spoofing*, DDoS e interferências em sinais ADS-B (*Automatic Dependent Surveillance–Broadcast*). Nesse contexto, a IA surge como uma camada adaptativa de defesa, capaz de detetar, prever e mitigar riscos com uma rapidez e precisão inatingíveis por métodos convencionais (Çevik & Akleylek, 2024; Kotadiya, 2024; Xie et al., 2023).

a) Deteção de anomalias e ameaças em tempo real

A utilização de IA para *anomaly detection* tem sido amplamente estudada no contexto dos sistemas ADS-B. realizaram uma *Systematisation of Knowledge* (SoK) sobre técnicas de *Machine Learning* e *Deep Learning* aplicadas à deteção de anomalias em sinais ADS-B. Os autores concluíram que modelos de redes neuronais profundas (CNN e LSTM) alcançam taxas de deteção superiores a 98%, superando métodos tradicionais baseados em regras (Çevik & Akleylek, 2024).

Esses resultados demonstram a viabilidade da IA como segunda camada de segurança operacional, complementando os mecanismos de criptografia e autenticação existentes. De forma complementar, Xie et al., (2023) analisam o uso de aprendizagem não supervisionada para identificar ataques de *spoofing* e *jamming* em sinais de navegação.

O estudo mostra que os algoritmos de IA podem distinguir ruído legítimo de interferências maliciosas, permitindo que o *Flight Management System* (FMS) reconheça comportamentos incoerentes e execute ações corretivas automáticas.

Essa capacidade de resposta adaptativa é essencial para proteger aeronaves contra-ataques que visam manipular dados de posicionamento e controlo de voo.

b) Ciberdefesa industrial e resposta automatizada

A literatura também identifica iniciativas de integração de IA em plataformas de ciberdefesa operacional. Sheikhi et al., (2025) descrevem o projeto IDUNN, que combina módulos de deteção (THOR), resposta automatizada (HEIMDAL) e gestão de vulnerabilidades (ODIN), utilizando algoritmos de *Machine Learning* e *Natural Language Processing* (NLP).

Este sistema exemplifica o conceito de ciber-resiliência explicável, no qual as decisões tomadas pelos modelos de IA são rastreáveis e auditáveis, característica alinhada com os princípios de IA Explicável (XAI). Embora aplicado ao contexto industrial, o IDUNN é um modelo de referência para a aviação, demonstrando como a IA pode reduzir o tempo de resposta a incidentes e garantir transparência e responsabilidade nas decisões automatizadas.

c) Avaliação e mitigação de riscos cibernéticos

Para além da deteção, a IA tem sido aplicada na avaliação e mitigação de riscos de segurança da informação, em conformidade com os princípios do EASA Part-IS (IS.I.OR.205 e IS.I.OR.210). Zhou et al. (2020) propuseram um modelo preditivo que combina *Machine Learning* e *data analytics* para identificação e previsão de riscos em aeronaves civis, utilizando análise de dados do sistema ACARS para melhorar a precisão e rapidez da identificação e predição de perigos. O estudo utiliza métodos supervisionados para identificação e predição de riscos. De forma semelhante, Faruk et al., (2025) defendem que os modelos de IA podem recomendar ações de mitigação automáticas, otimizando a alocação de recursos e reduzindo redundâncias de controlo.

Essas abordagens antecipam a visão de gestão de risco assistida por IA, na qual os sistemas aprendem continuamente com novos dados e ajustam automaticamente o nível de proteção. Kotadiya, (2024) reforça esta perspetiva, argumentando que a IA deve ser vista como uma camada inteligente de conformidade dentro dos sistemas de gestão de segurança. Segundo o autor, algoritmos de *Machine Learning* podem analisar relatórios de auditoria, identificar não conformidades e sugerir melhorias de controlo em alinhamento com normas como a ISO/IEC 27001:2022 e a ISO/IEC 27005:2022. Essa automatização não apenas melhora a eficiência das equipas de segurança, mas garante rastreabilidade documental, como as exigida pela EASA.

6.5. Explicabilidade, Ética e Certificação de Sistemas de Inteligência Artificial

A crescente integração da Inteligência Artificial (IA) na aviação levanta desafios complexos no que respeita à explicabilidade, ética e certificação regulatória dos sistemas inteligentes. Ao contrário das tecnologias determinísticas, os algoritmos de aprendizagem automática são frequentemente opacos no modo como processam e interpretam dados, o que gera o chamado problema da caixa negra (*black-box problem*). Em setores de alto risco, como a aviação, essa falta de transparência pode comprometer tanto a confiança operacional quanto a conformidade regulatória (Delgado-Aguilera et al., 2024).

A Agência Europeia para a Segurança da Aviação (EASA), no seu *Artificial Intelligence Roadmap* (2023), estabelece que a certificação de sistemas baseados em IA deve assentar nos princípios da explicabilidade, rastreabilidade e supervisão humana. Esta orientação foi posteriormente reforçada pelo Regulamento Europeu de Inteligência Artificial (UE 2024/1689, 2024), que classifica a aviação civil como um domínio de alto risco e impõe exigências rigorosas de transparência algorítmica e controlo humano significativo. Em ambos os documentos, a explicabilidade é vista não apenas como requisito técnico, mas como garantia de segurança e responsabilidade ética (EASA AI, 2025).

a) O papel da IA Explicável (XAI) na segurança aeronáutica

A IA Explicável (*Explainable Artificial Intelligence* – XAI) surge como uma resposta científica e regulatória à necessidade de tornar as decisões algorítmicas compreensíveis e auditáveis. Segundo Delgado-Aguilera et al. (2024), a XAI visa permitir que pilotos, engenheiros e auditores entendam o processo de decisão dos modelos inteligentes, identificando as variáveis determinantes em cada resultado. Os autores propõem uma metodologia de certificação baseada em rastreabilidade, integrando requisitos de segurança civil e militar para validar algoritmos em sistemas críticos. Essa abordagem demonstra que a transparência algorítmica é condição essencial para a confiança institucional e para o cumprimento das normas de segurança aeronáutica.

No contexto operacional, a XAI pode, por exemplo, justificar por que razão um sistema de IA classificou determinado sinal como anómalo, permitindo verificação cruzada humana antes da adoção de ações corretivas automáticas.

Essa rastreabilidade não só reforça a resiliência organizacional, como também facilita auditorias no âmbito do EASA Part-IS.I.OR.215, que exige evidências documentadas de conformidade e de funcionamento seguro dos sistemas de informação.

b) Ética e confiança no ecossistema homem–máquina

A relação entre humanos e sistemas inteligentes evolui para um modelo de cooperação cognitiva, em que a IA atua como agente assistido, e não como substituto do operador. Kirwan, (2024) defende que a confiança na IA depende da sua capacidade de justificar decisões e de preservar a autonomia humana nas operações críticas.

O autor introduz o conceito de *Human–AI Teaming* (HAT), que descreve uma interação colaborativa na qual ambos os agentes, humano e máquina, aprendem mutuamente e partilham responsabilidade decisória.

Este modelo é particularmente relevante em cenários de elevada carga cognitiva, como o controlo de tráfego aéreo, a gestão de incidentes e a resposta a emergências. A ética algorítmica, nesse sentido, não se resume à conformidade legal, mas envolve também valores organizacionais, cultura de segurança e responsabilidade social.

A EASA e o (UE)AI Act estabelecem que todo sistema inteligente deve operar sob o princípio de "controlo humano significativo" (*meaningful human control*), o que implica que as decisões automáticas possam ser contestadas, explicadas e supervisionadas.

Esses requisitos são fundamentais para evitar automatismos cegos, garantindo que a automação sirva para ampliar a perceção situacional humana, e não para substituí-la.

c) Certificação e integração regulatória

A certificação de sistemas de IA na aviação é um processo que combina validação técnica, demonstração de segurança e comprovação ética.

Delgado-Aguilera et al. (2024) defendem a adoção de normas conjuntas entre a EASA e as autoridades militares, de modo a padronizar a avaliação de algoritmos com base em critérios de rastreabilidade, explicabilidade e verificabilidade. O estudo destaca que o ciclo de certificação deve incluir fases iterativas de teste, documentação e avaliação humana, assegurando que o comportamento do sistema se mantenha consistente ao longo do seu ciclo de vida operacional.

De igual forma, Sheikhi et al., (2025) salientam que a convergência entre IA Explicável e Ciberdefesa Adaptativa é essencial para enfrentar o novo paradigma de ameaças digitais. Ao permitir que os sistemas justifiquem suas ações defensivas, por exemplo, a mitigação automática de um ataque *spoofing*, a XAI transforma a cibersegurança aeronáutica num processo de gestão de conhecimento e evidência, em conformidade com o EASA Part-IS e o (UE)AI Act. Essa integração normativa é o que diferencia a aviação de outros setores industriais: aqui, a confiança algorítmica é uma exigência regulatória, e não apenas técnica (EASA AI, 2025; Easy Rules, 2025).

6.6. EASA AI Act e o enquadramento europeu da Inteligência Artificial na aviação

O avanço da Inteligência Artificial (IA) na aviação civil europeia trouxe benefícios expressivos em termos de eficiência operacional, manutenção preditiva e segurança. Contudo, também levantou preocupações éticas, jurídicas e técnicas relativas à fiabilidade, explicabilidade e responsabilidade dos sistemas inteligentes. Em resposta a esses desafios, a Comissão Europeia aprovou o Regulamento (UE) 2024/1689, conhecido como (UE)AI Act, o primeiro quadro legislativo global destinado a regular o desenvolvimento, a implementação e a utilização da IA no espaço europeu (UE 2024/1689, 2024).

O (UE)AI Act estabelece uma abordagem baseada no risco, classificando os sistemas de IA em quatro categorias, risco inaceitável, alto, limitado e mínimo, e impondo obrigações proporcionais à criticidade de cada aplicação. Os sistemas de alto risco, categoria que abrange diretamente o setor aeronáutico, devem cumprir requisitos rigorosos de governança algorítmica, explicabilidade, auditoria e supervisão humana. Isso inclui a necessidade de validação contínua de desempenho, documentação técnica transparente, gestão de dados de treino e avaliação de conformidade antes da certificação e colocação no mercado (UE 2024/1689, 2024).

No domínio aeronáutico, a Agência Europeia para a Segurança da Aviação (EASA) foi incumbida de integrar os princípios do (UE)AI Act ao seu quadro regulatório setorial. Assim, em 2023, a agência publicou o documento EASA *Artificial Intelligence Roadmap* 2.0, que define a visão estratégica para a certificação e supervisão de sistemas baseados em IA utilizados em aeronaves, sistemas de gestão de tráfego aéreo, manutenção e operações. O documento propõe uma transição progressiva em três níveis de maturidade regulatória (*Level 1 a Level 3*), que vão desde aplicações assistidas por IA sob supervisão humana até sistemas altamente automatizados com autonomia operacional parcial (EU IA, 2023; UE 2024/1689, 2024).

De acordo com a EU IA (2023), os sistemas de IA de nível 1 e 2 já podem ser implementados no contexto aeronáutico, desde que cumpram requisitos de explicabilidade (XAI), rastreabilidade e verificabilidade. Esses princípios são essenciais para garantir que o ser humano permaneça no centro do processo decisório e possa compreender as justificações geradas pelos algoritmos. Além disso, a EASA exige que as organizações demonstrem a robustez e a resiliência cibernética dos sistemas inteligentes, articulando a avaliação de risco da IA com a gestão de risco de segurança operacional (SMS) e com o sistema de gestão da segurança da informação (ISMS) (ACT IA, 2024).

A sinergia entre o (UE)AI Act e o EASA Part-IS é, portanto, inevitável, ambos os regulamentos partilham a visão de que a confiança nos sistemas digitais críticos só pode ser alcançada através da transparência, responsabilidade e governança contínua. Enquanto o EASA Part-IS regula a segurança da informação e a mitigação de riscos cibernéticos, o (UE)AI Act assegura que as soluções de IA que apoiam esses processos sejam seguras, éticas e auditáveis.

Nesse contexto, a aplicação de IA explicável (XAI) torna-se central para o setor aeronáutico, pois possibilita a integração entre dados operacionais, riscos cibernéticos e processos de decisão humana, assegurando conformidade com os princípios de segurança, fiabilidade e transparência definidos pelo quadro europeu. Essa convergência normativa constitui o alicerce para modelos teóricos, como o CESAR *Framework*, que propõem a utilização de IA como ferramenta de apoio à gestão integrada de riscos, alinhada com o EASA Part-IS e o EU AI Act (UE 2024/1689, 2024).

6.7. Síntese Crítica e Tendências Futuras

A revisão sistemática e teórica da literatura permite identificar que a Inteligência Artificial já deixou de ser uma promessa para tornar-se um elemento estruturante da aviação contemporânea. As suas aplicações, inicialmente restritas a processos isolados de monitorização e manutenção, expandiram-se para abranger gestão de tráfego, cultura de segurança, manutenção preditiva, deteção de anomalias e ciberdefesa automatizada.

Esta expansão reflete uma mudança epistemológica no setor: a aviação não apenas usa IA, mas depende dela para manter a sua eficiência, segurança e conformidade regulatória (Demir et al., 2024; Kotadiya, 2024; Xie et al., 2023).

Em termos práticos, a aviação caminha para um paradigma de "gestão cognitiva do risco", no qual os sistemas inteligentes não apenas processam dados, mas interpretam contextos e aprendem com as próprias decisões.

Essa transição exige a consolidação de três pilares fundamentais:

a) explicabilidade técnica,
b) ética operacional, e
c) interoperabilidade regulatória entre os sistemas de IA e os requisitos do EASA Part-IS.

Em síntese, a Inteligência Artificial representa hoje o núcleo transformador da aviação do século XXI, combinando inovação tecnológica, responsabilidade ética e robustez regulatória. O desafio, daqui em diante, será equilibrar o poder cognitivo da automação com o juízo humano, assegurando que a IA continue a servir o propósito maior da aviação: a segurança, a fiabilidade e a confiança pública.

6.8. Requisitos de IA para o CESAR *Framework*

A análise do estado da arte sobre IA na aviação, combinada com os requisitos regulatórios estabelecidos nos Capítulos 4-5, define os princípios tecnológicos que o CESAR *Framework* deve incorporar:

Requisito Técnico 1: IA Explicável (XAI) Obrigatória

- Fundamentação: EU AI Act Art. 13 + cultura *aviation safety,*
- Implicação: Algoritmos "*black-box*" (*deep neural networks* complexos) inadequados,
- Solução CESAR: *Hybrid approach* - ML interpretável + regras explicáveis.

Requisito Técnico 2: Supervisão Humana Significativa

- Fundamentação: EU AI Act Art. 14 + EASA Part-IS *governance*,
- Implicação: IA não pode tomar decisões finais sobre riscos críticos,
- Solução CESAR: IA recomenda, humano (*Safety Mgr*/CISO) decide e aprova.

Requisito Técnico 3: Processamento de Linguagem Natural (NLP)

- Fundamentação: Necessidade de ler relatórios FDM (*Flight Data Monitoring*), *logs*, documentos regulatórios,
- Implicação: Correlação semântica entre eventos técnicos e operacionais,
- Solução CESAR: NLP para extração de entidades e correlação de contextos.

Requisito Técnico 4: *Federated Learning* (Opcional, mas desejável)

- Fundamentação: NIS2 Art. 32 (*information sharing*) + confidencialidade

- Implicação: Partilha de *threat intelligence* sem expor dados sensíveis,
- Solução CESAR: Arquitetura permite FL futura para colaboração inter-org.

Requisito Técnico 5: Rastreabilidade Completa

- Fundamentação: Part-IS IS.I.OR.240 (*record-keeping*) + AI Act Art. 12,
- Implicação: Toda inferência da IA deve gerar *audit trail*,
- Solução CESAR: *Logging* estruturado de cada decisão com justificativa.

Requisito Técnico 6: Gestão do Meta-Risco (*AI Risk)*

- Fundamentação: Part-IS IS.I.OR.205 (*own system must be risk-assessed*),
- Implicação: CESAR como sistema de informação crítico deve ter riscos avaliados,
- Solução CESAR: *Self-assessment module* + validação humana periódica.

Com a base tecnológica estabelecida, o próximo capítulo apresenta o modelo conceptual completo, demonstrando como os princípios de IA explicável aqui descritos são aplicados aos requisitos regulatórios do EASA Part-IS para criar sistema integrado de gestão de risco ISMS-SMS.

7. CESAR *FRAMEWORK*

7.1. CESAR (*Cyber–Safety Enhanced System for AI-based Risk Management*)

O CESAR (*Cyber-Safety Enhanced System for AI-based Risk Management*) emerge como resposta integrada às lacunas identificadas ao longo desta dissertação:

Da Revisão Sistemática (Cap. 3):

No âmbito dos estudos analisados na revisão sistemática, nesta dissertação, observou-se que a literatura permanece fragmentada entre os domínios de cibersegurança, segurança operacional (*safety*) e gestão de risco, apesar das exigências de integração estabelecidas pelo Regulamento (UE) 2023/203 (EASA Part-IS). Embora tenham sido identificadas mais de 80 ameaças cibernéticas e operacionais nos 40 estudos considerados, apenas 4 estudos (10%) abordam simultaneamente a relação entre *cybersecurity* e *safety*, evidenciando que ISMS e SMS continuam a ser tratados como sistemas isolados.

Verificou-se ainda que 18 estudos (45%) apontam desafios de integração técnica e 17 estudos (42,5%) mencionam limitações de dados, fatores associados à redução de *performance* quando modelos passam de contextos *single-domain* (*accuracy* média entre 85–92%) para contextos *cross-domain* (72–78%). Além disso, somente 26 dos 40 estudos (65%) apresentam métricas quantitativas de performance, e nenhum deles propõe mecanismos formais para assegurar explicabilidade, auditabilidade ou alinhamento com requisitos regulatórios como o EU AI Act.

A ausência de abordagens que incorporem princípios de *compliance by design*, especialmente no que se refere à integração estruturada entre processos ISMS–SMS, governança da informação, rastreabilidade e requisitos de IA de alto risco, reforça a lacuna entre as soluções propostas na literatura e as exigências operacionais e regulatórias da aviação europeia. Estes resultados justificam o desenvolvimento do CESAR *Framework*, concebido para articular segurança operacional, cibersegurança, inteligência artificial explicável e conformidade normativa num modelo unificado de gestão de riscos para o setor aeronáutico.

Do Enquadramento Regulatório (Cap. 4-5):

O Regulamento (UE) 2023/203 estabelece que todas as organizações abrangidas pelo EASA Part-IS devem implementar, aplicar e manter um sistema de gestão da segurança da informação (IS.I.R.200), que lhe permita assegurar um processo estruturado de gestão de riscos de

informação que considere explicitamente os impactos potenciais sobre a segurança operacional (IS.I.OR.205 e IS.I.OR.210).

A formulação do IS.I.OR.200 torna evidente que a gestão de riscos de informação (IS.I.OR.205 e IS.I.OR.210) deve ser coerente, compatível e integrada com o sistema de gestão da segurança operacional da organização, conforme o enquadramento do Regulamento (UE) 376/2014 e do Anexo 19 da ICAO.

Isto significa que o IS.I.OR.200 funciona como um ponto de intersecção regulatória entre *information security* e *aviation safety*, determinando que eventos de cibersegurança capazes de afetar a operação segura devem ser identificados, avaliados, mitigados e monitorizados dentro de um ciclo comum de risco

Assim, o regulamento define "**o que"** deve ser alcançado, a articulação entre cibersegurança e *safety*, mas não determina "**como"** essa integração deve ser implementada. Assim, cabe às organizações desenvolver métodos, processos e estruturas que operacionalizem essa ligação entre ISMS e SMS.

O (EU) AI Act acrescenta uma camada adicional de exigência. Para sistemas de IA utilizados em ambientes aeronáuticos, classificados como alto risco, o *Act* define condições operacionais específicas: supervisão humana ativa, explicabilidade, rastreabilidade, e controlo contínuo do risco.

Em conjunto, o EASA Part-IS define o objetivo (integração *Cyber*-S*afety*) e o AI *Act* define os critérios de funcionamento da IA(*IA-Based*). Essa combinação estabelece as regras para a definição do modelo conceptual CESAR *Framework (System)*, que operacionaliza a integração e incorpora desde a origem princípios de *compliance by design (Enhanced).*

A Tabela 15 apresenta o mapeamento entre os requisitos do EASA Part-IS e a estrutura do ciclo de vida processual do modelo conceptual CESAR, demonstrando como cada exigência normativa é abrangida e operacionalizada no âmbito das diferentes fases do *framework*.

Tabela 15 - Mapeamento Part-IS → CESAR *Framework*

Requisito Part-IS	Exigência Part-IS	Fase CESAR Correspondente
IS.I.OR.200	Estabelecer ISMS integrado com SMS	Arquitetura geral
IS.I.OR.205(a)	Identificar riscos *info security*	IDENTIFICAR
IS.I.OR.205(c)	Avaliar riscos com impacto *safety*	AVALIAR
IS.I.OR.210(a)	Tratar riscos inaceitáveis	MITIGAR
IS.I.OR.210(b)	Comunicar resultados da avaliação	COMUNICAR
IS.I.OR.205(d)	Revisão periódica + aceitação de risco	ACEITAR
IS.I.OR.215 / 240	Reporte interno / *Record-keeping*	EVIDENCIAR
IS.I.OR.260	Melhoria contínua e maturidade	MELHORAR

Fonte: Mapeamento regulatório do ciclo de vida do CESAR

Da Análise de IA (Cap. 6):

O uso de IA na aviação permanece fragmentado, com aplicações isoladas em domínios específicos (*cybersecurity*, *safety*, manutenção ou análise de incidentes), mas com potencial evidente para suportar processos integrados de gestão de risco. A viabilidade técnica e a necessidade regulatória de XAI, a eficácia dos *Hybrid ML approaches* e a capacidade do NLP para produzir correlação semântica entre fontes de dados heterogéneas configuram-se como elementos críticos que se identifica como habilitadores de integração. No entanto, os estudos analisados não apresentam um modelo operacional que combine estes elementos de forma estruturada, auditável e alinhada com os requisitos do EASA Part-IS e do (EU) AI Act. Assim, a consolidação destas evidências cria a base conceptual para o CESAR, que procura transformar estas capacidades técnicas em mecanismos cognitivos integrados, capazes de suportar a interligação entre ISMS e SMS, reforçar a deteção precoce de riscos e assegurar conformidade por *design* com as obrigações regulatórias europeias. Em síntese, as limitações das abordagens

atuais, orientam e fundamentam a criação do modelo conceptual CESAR como solução integrada para a gestão inteligente de riscos na aviação.

A Tabela 16 descreve as cinco camadas da Arquitetura de IA do CESAR, abrangendo processos de ingestão e pré-processamento de dados, análise semântica por NLP, modelos interpretáveis (XAI), supervisão humana e mecanismos de auditoria e evidência regulatória.

Tabela 16 - Arquitetura de IA do CESAR

Camada	Nome / Função	Principais Elementos e Funções
Camada 1	*Data Ingestion & Preprocessing*	• *Logs* (*firewall*, IDS, *network*)
		• Relatórios (FDM, IQSMS, *occurrence reports*)
		• Fontes externas (ENISA, MITRE ATT&CK, CNCS)
Camada 2	*NLP & Semantic Analysis*	• Extração de entidades (ativos, ameaças, impactos)
		• Correlação contextual (eventos *cyber* ↔ *safety*)
Camada 3	*Interpretable ML (XAI)*	• Classificação de risco (*Random Forest* / *Decision Tree*)
		• Avaliação de impacto (Redes *Bayesianas*)
		• Mecanismo de recomendação (híbrido Regra + ML)
Camada 4	*Human Oversight & Decision*	• *Dashboards* com relatórios explicáveis
		• Fluxos de aprovação (*Safety Manager* ↔ CISO)
Camada 5	*Audit Trail & Compliance Evidence*	• *Logs* imutáveis (*hashing* estilo *blockchain*)
		• Mapeamento regulatório (cláusulas Part-IS)

Fonte: Arquitetura conceptual do CESAR

A evolução normativa e tecnológica analisada nos capítulos anteriores revela um desafio persistente, embora a EASA Part-IS tenha introduzido um enquadramento robusto para a segurança da informação na aviação, a sua implementação prática continua a ser dificultada pela fragmentação entre domínios de *safety* e cibersegurança. Esta lacuna cria o risco de abordagens paralelas, em que cada área avalia e mitiga riscos de forma isolada, perdendo a visão sistémica necessária à mitigação de ameaças que cruzam fronteiras operacionais e digitais.

O CESAR *Framework* (*Cyber–Safety Enhanced System for AI-based Risk Management*) nasce da constatação de que o risco aeronáutico são, cada vez mais ciberfísico, onde os sistemas digitais e operacionais coexistem numa relação de interdependência funcional, em que vulnerabilidades informacionais podem originar falhas operacionais e vice-versa (Abozaid et al., 2024; Filinovych et al., 2021).

Nesse sentido, a separação tradicional entre *safety* e *cybersecurity* torna-se anacrónica e contraproducente. O CESAR *Framework* materializa a convergência destes elementos num modelo operacional de gestão integrada de risco. Concebido a partir dos princípios do EASA Part-IS, o modelo propõe uma estrutura unificada de gestão de riscos (*Risk Management*), que articula os processos do ISMS e do SMS, sustentando-se em tecnologias de inteligência artificial explicável (XAI) para apoiar decisões e evidenciar conformidade regulatória.

7.2. Premissas do Modelo Conceptual

A conceção do modelo baseia-se em três premissas fundamentais:

1. **Integração regulatória e técnica**

   O CESAR alinha os requisitos do EASA Part-IS com os princípios do SMS (ICAO *Annex* 19) e das normas ISO/IEC 27001:2022 e ISO/IEC 27005:2022, garantindo que ambos os sistemas partilham o mesmo ciclo de risco e linguagem operacional.

2. **Inteligência operacional assistida**

A utilização de IA explicável que permite reforçar a rastreabilidade das decisões, automatizar a correlação entre eventos de risco e apoiar a gestão documental exigida pelos pontos IS.I.OR.205–210– 215- 260 do EASA Part-IS.

3. **Resiliência baseada em dados**

O modelo promove a criação de uma memória organizacional digital, capaz de aprender continuamente com incidentes, auditorias e dados regulatórios.

Em síntese, a conceção do modelo conceptual do CESAR reflete a convergência entre integração regulatória, inteligência operacional assistida e resiliência baseada em dados. Estas três premissas estruturantes permitem que o modelo avance de uma abordagem tradicional de gestão de risco para um paradigma de "gestão cognitiva do risco", no qual os sistemas inteligentes deixam de atuar apenas como mecanismos de processamento e passam a interpretar contextos complexos, identificar interdependências e aprender com incidentes, auditorias e evidências regulatórias. Tal evolução exige que a automação permaneça alinhada com três pilares essenciais: uma ética operacional que salvaguarde valores humanos fundamentais; uma explicabilidade técnica que possibilite auditorias algorítmicas rigorosas; e uma interoperabilidade regulatória que assegure a compatibilidade entre a atuação dos sistemas inteligentes e os requisitos do EASA Part-IS.

Assim, o CESAR estabelece uma arquitetura onde o poder cognitivo da IA e o juízo humano crítico coexistem de forma complementar, garantindo que a modernização digital do setor aeronáutico não compromete a segurança nem a conformidade, mas antes as reforça - como ilustrado na Figura 10.

Fig. 10 - Modelo CESAR de gestão cognitiva de risco

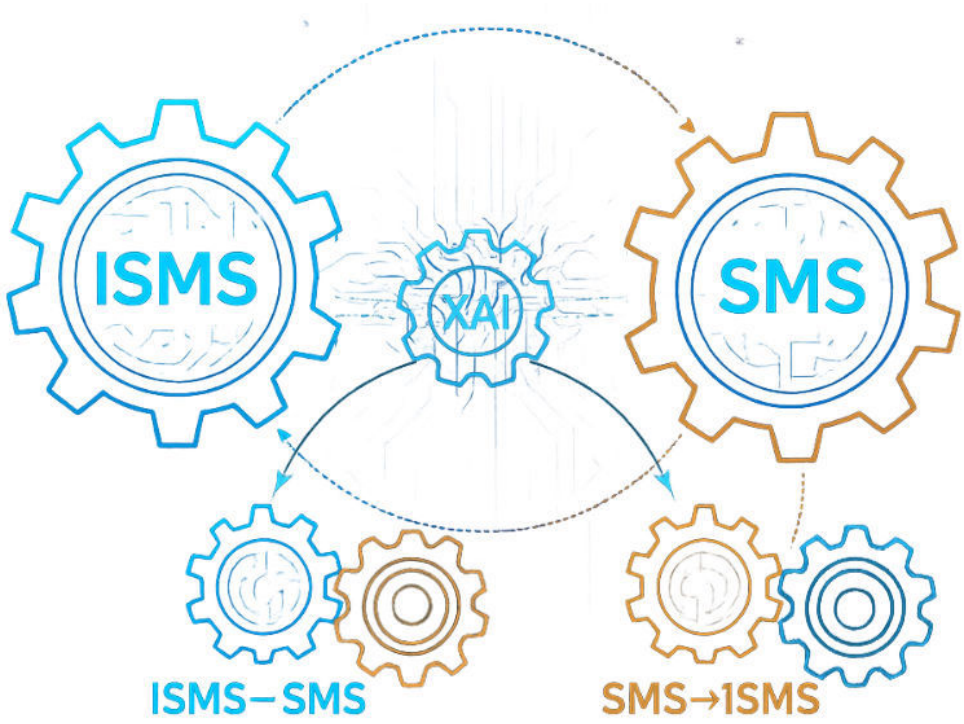
Fonte: Modelo CESAR

7.3. Abordagem Conceptual do Modelo da Gestão de Risco

Diferentemente de abordagens que procuram fundir o ISMS e o SMS num único sistema de gestão, o CESAR adota uma arquitetura dual e independente, ilustrada na Figura 11. Nesta estrutura, cada domínio, ISMS e SMS, mantém os seus processos autónomos de identificação, avaliação e tratamento de riscos, preservando a especificidade metodológica de cada sistema.

A singularidade do CESAR reside na criação de uma ponte de interdependência inteligente, visível no eixo central da figura 11, que se ativa apenas quando existe correlação material entre riscos de natureza operacional e informacional. Essa ponte cognitiva é mediada por um módulo de IA explicável (XAI), responsável por interpretar padrões, analisar dependências e suportar decisões integradas sem comprometer a autonomia dos dois sistemas de gestão. Assim, a Figura 11 representa de forma clara o modelo *dual*-operacional: dois domínios independentes ligados apenas quando necessário por uma camada cognitiva que suporta a integração regulatória exigida pelo EASA Part-IS.

Fig. 11 – Modelo CESAR Estrutura *dual* de Gestão de Risco



Fonte: CESAR - Definição do Modelo

No CESAR, os fluxos de risco são estruturados de forma a preservar a autonomia dos domínios, enquanto permitem integração seletiva sempre que ocorre interdependência material. O **fluxo ISMS isolado** concentra-se na proteção da informação e na continuidade tecnológica, aplicando o ciclo de risco exclusivamente sob a perspetiva da cibersegurança. De modo análogo, o **fluxo SMS isolado** foca-se na integridade operacional e na segurança de voo, avaliando *hazards* e condições de risco exclusivamente no domínio *safety*.

A integração ocorre apenas quando necessária: no **fluxo ISMS → SMS**, um risco de cibersegurança com impacto potencial em sistemas de voo, manutenção, comunicações ou operações é automaticamente correlacionado para o domínio SMS, onde passa a ser analisado sob a ótica de segurança operacional. No sentido inverso, o **fluxo SMS → ISMS** é ativado quando um *hazard* operacional, identificado no SMS, pode gerar ou expor vulnerabilidades de segurança da informação, exigindo correção ou mitigação complementar no ISMS.

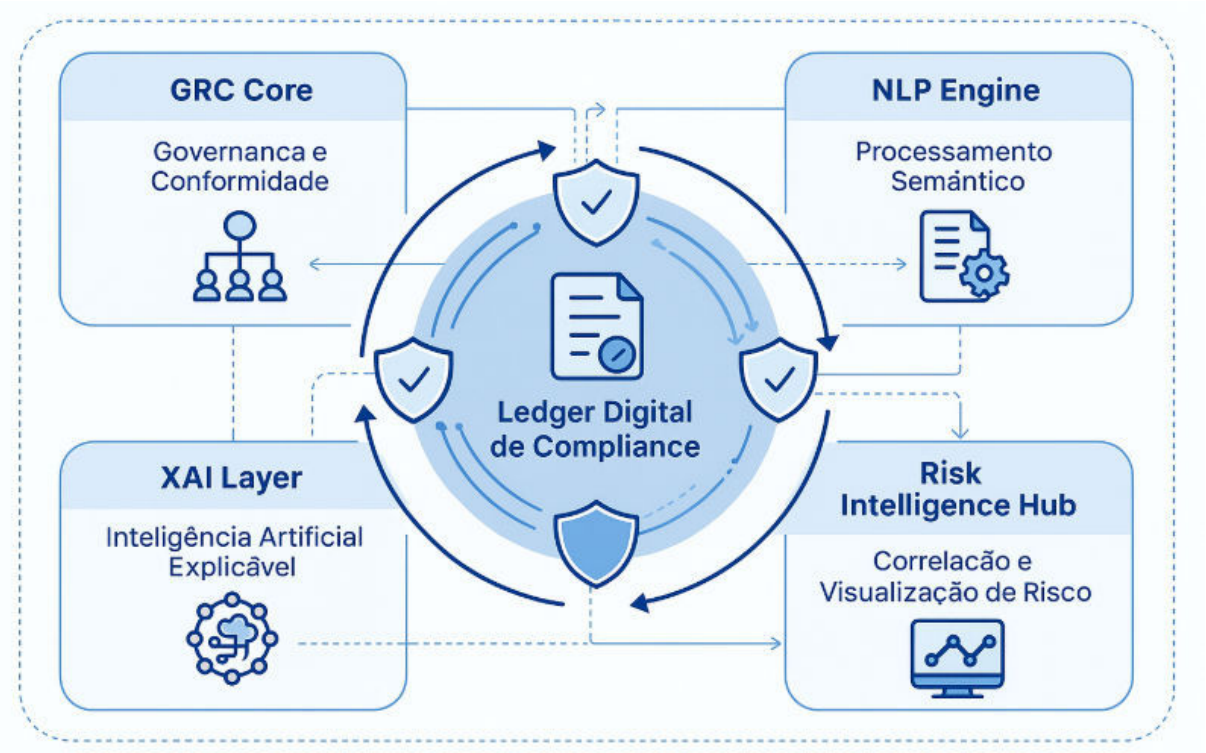
Este mecanismo assegura integração seletiva e rastreável, evitando redundâncias e garantindo que apenas riscos com impacto cruzado são avaliados conjuntamente. A esta lógica acresce a dimensão cognitiva do CESAR, inspirada em abordagens como as de Garcia et al., (2021 e Zhou et al., (2020) onde o modelo incorpora mecanismos de análise de dados e inferência que permitem às organizações detetar, interpretar e priorizar riscos de forma automatizada para antecipar e gerir riscos em ambientes operacionais complexos.

7.4. Arquitetura Técnica do CESAR *Framework*.

A operacionalização do CESAR *Framework* apresenta uma arquitetura técnica capaz de articular governança regulatória, inteligência analítica e rastreabilidade digital. Concebido como um *middleware* inteligente, o CESAR funciona como uma camada integradora entre o ISMS e o SMS, correlacionando dados, interpretando contextos e gerando conhecimento em conformidade com o EASA Part-IS (UE 2023/203) e o EU AI Act (2024).

A arquitetura técnica interna conforme podemos ver na Figura 12 é composta por quatro módulos interdependentes, Governança e Conformidade (GRC *Core*), Processamento Semântico (NLP *Engine*), *Inteligência Artificial Explicável* (XAI *Layer*) e Correlação e Visualização de Risco (*Risk Intelligence Hub*), que em conjunto, asseguram a convergência entre segurança operacional, cibersegurança e conformidade normativa

Fig. 12 - Arquitetura Técnica Interna do CESAR



Fonte: CESAR - Definição do Modelo

7.4.1. Módulo de Governança e Conformidade (GRC *Core*)

O GRC *Core* constitui o eixo de governança do CESAR, garantindo controlo, rastreabilidade e alinhamento regulatório. Baseado nas cláusulas IS.I.OR.200–210–260 do EASA Part-IS, na ISO/IEC 27001:2022 e na Diretiva NIS2, este módulo:

- mantém o inventário normativo e correlaciona requisitos com controlos e evidências;
- gere o mapa de responsabilidades, atribuindo funções a cada papel (CISO, *Safety Manager*, *Compliance Officer*, DPO);
- e monitoriza a conformidade contínua, gerando alertas para auditorias internas e externas.

A integração com o SMS permite associar eventos de cibersegurança a ocorrências operacionais, estabelecendo uma ligação documental direta entre ISMS e SMS. Este princípio de *traceability by design* garante coerência e elimina redundâncias, cumprindo as exigências de auditoria da EASA e da ANAC.

Conforme Zhou et al. (2020) a governança de sistemas críticos depende da articulação entre conformidade, risco e segurança operacional, tríade materializada no *ledger digital* de *compliance* do CESAR, que regista e contextualiza cada ação de forma auditável.

7.4.2. Módulo de Processamento Semântico e Extração de Conhecimento (NLP *Engine*)

O NLP *Engine* constitui a base cognitiva do sistema. Utilizando técnicas de Processamento de Linguagem Natural, lê e interpreta automaticamente documentos técnicos e normativos, como AMC & GM to Part-IS, *Annex* II ED *Decision* 2025/014/R, relatórios da ENISA, boletins da ICAO e alertas do CNCS, relatórios de *Safety*, extraindo entidades como ameaça, ativo, impacto e regulamento associado.

Este processo gera uma base de conhecimento dinâmica, que relaciona vulnerabilidades reais com requisitos regulatórios. Por exemplo, uma vulnerabilidade (CVE) num servidor aeronáutico é correlacionada ao IS.I.OR.205(b) e encaminhada para avaliação pelo módulo XAI. Segundo Garcia et al. (2021) essa leitura semântica melhora a correlação entre dados técnicos e contextuais no ecossistema aeronáutico. O CESAR amplia essa abordagem ao integrar fontes regulatórias e operacionais, assegurando rastreabilidade e validação humana em conformidade com o (UE)AI Act.

7.4.3. Módulo de Inteligência Artificial Explicável (XAI *Layer*)

O XAI *Layer* transforma dados dispersos em recomendações compreensíveis e auditáveis. Alinhado ao (UE)AI Act, privilegia modelos transparentes e supervisionáveis, substituindo abordagens *black box*.

A camada tem duas funções centrais:

- Apoiar a decisão operacional, com recomendações de mitigação e priorização de riscos;
- Demonstrar conformidade, apresentando a lógica e as evidências de cada inferência.

Emprega algoritmos híbridos, *machine learning* supervisionado, redes *bayesianas* e árvores de decisão explicáveis, para inferir relações causais entre ameaças, vulnerabilidades e impactos.

Por exemplo, o CESAR pode detetar falhas em ligações SATCOM, associá-las a ataques de *spoofing* reportados pela ENISA (2023) e propor medidas técnicas e operacionais justificadas.

Como defendem Ajayi et al. (2025), a IA em infraestruturas críticas deve ser interpretável e sujeita a revisão humana, exatamente o princípio adotado pelo CESAR, em que a IA amplifica, e não substitui, o decisor.

7.4.4. Módulo de Correlação e Visualização de Risco (*Risk Intelligence Hub)*

O *Risk Hub* é a interface de integração e visualização dos resultados analíticos. Reúne as perspetivas técnica e operacional, fornecendo uma visão consolidada e dinâmica do risco organizacional.

O *dashboard* principal apresenta:

- a matriz integrada ISMS + SMS com classificação automática de risco;
- o mapa de dependências ciberfísicas entre ativos digitais e funções críticas;
- indicadores de desempenho e conformidade em tempo real;
- e linhas de tempo de mitigação, que demonstram a eficácia das ações.

De acordo com Werthwein & Annighoefer (2024), a visualização da informação reduz a carga cognitiva e favorece decisões mais rápidas e fundamentadas. O CESAR aplica esse princípio ao permitir a exportação automática de relatórios compatíveis com os requisitos da EASA e da ANAC. Adicionalmente, o *Risk Hub* implementa um ciclo de aprendizagem contínua, retroalimentando o GRC *Core* com dados provenientes de incidentes e auditorias, em conformidade com o requisito de melhoria contínua estabelecido no IS.I.OR.260.

7.4.5. Segurança, Ética e Conformidade da IA

O CESAR adota desde a conceção os princípios de IA, garantindo:

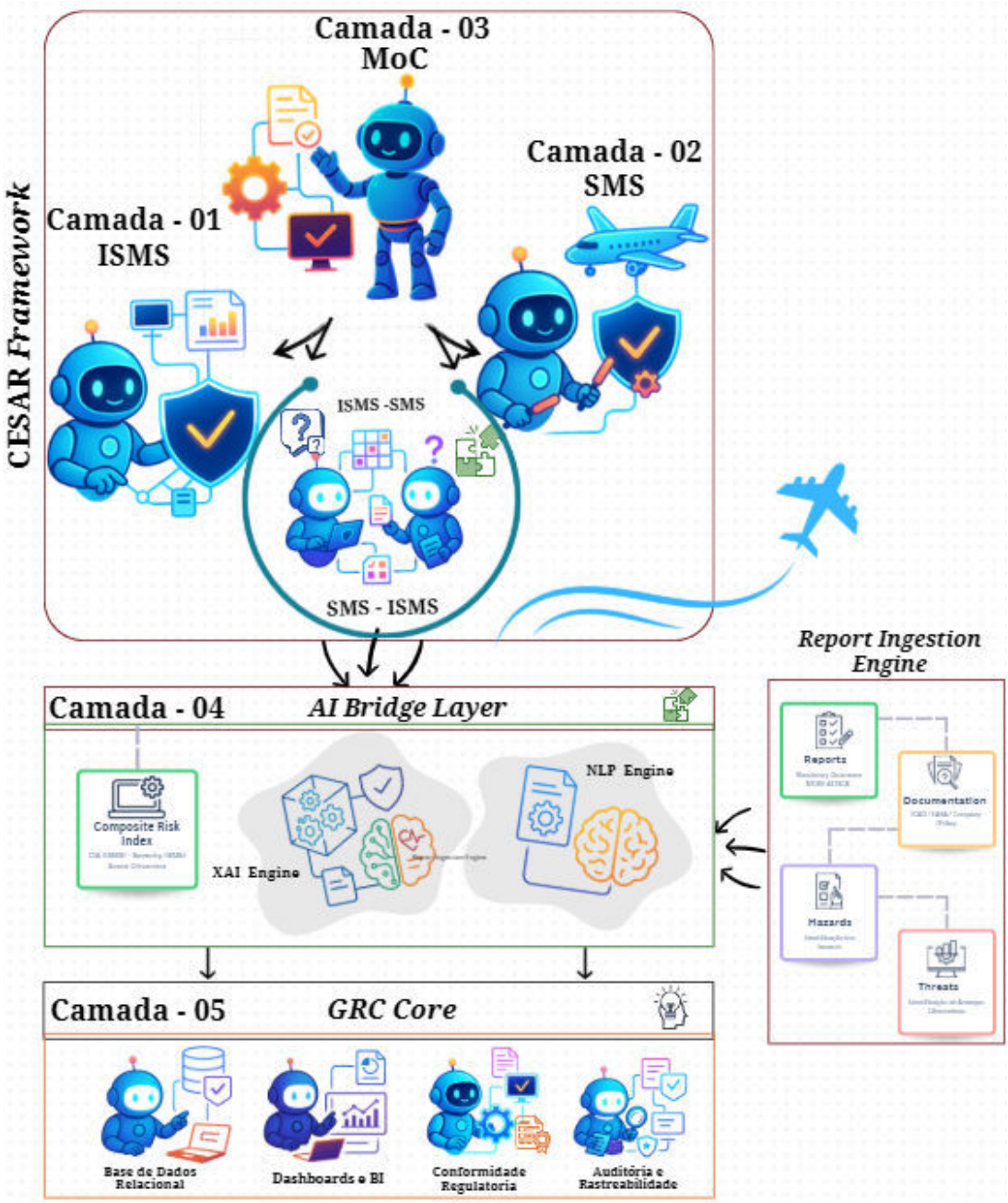
- supervisão humana efetiva,
- rastreabilidade e explicabilidade total,
- robustez técnica contra manipulação adversária,
- e imparcialidade na avaliação de risco.

Dessa forma, a IA torna-se um instrumento de transparência e *compliance*, assegurando ética e conformidade. O CESAR é um sistema inteligente de informação, sujeito aos mesmos princípios de gestão de risco das infraestruturas críticas.

O uso inadequado ou não supervisionado de IA pode gerar riscos à segurança operacional. Por isso, o CESAR exige avaliação contínua de riscos, transparência algorítmica e validação ética, seguindo o UE 2024/1689 (2024) e padrões ISO/IEC 27001 e 27005. Essas diretrizes garantem que a IA apoie decisões sem substituir o julgamento humano, promovendo responsabilidade e conformidade no setor aeronáutico.

A arquitetura técnica, Figura 13, foi concebida para suportar a integração seletiva, inteligente e reguladoramente rastejável entre os domínios ISMS e SMS, assegurando que ambos operem autonomamente, mas com interoperabilidade garantida sempre que existam impactos cruzados.

Fig. 13 - Arquitetura Técnica do CESAR *Framework* representa o ciclo integrado:



Fonte: Definição da arquitetura CESAR

7.4.6. Descrição das Camadas Arquiteturais

Camada 1 - Domínio ISMS

Responsável pela gestão de riscos de cibersegurança, abrangendo todos os ativos digitais e processos tecnológicos críticos:

- Inventário de ativos com classificação CIA

- Integração com *feeds* MITRE ATT&CK, ENISA, CNCS, EASA
- Identificação de riscos com potencial impacto operacional
- Norma associada: IS.I.OR.205(a–c), IS.I.OR.210

Camada 2 - Domínio SMS

Gestão de riscos operacionais e de *Safety*, alinhado com ICAO *Annex* 19:

- Identificação de *hazards* e condições inseguras
- Integração com MHIL e *Mandatory Occurrence Reports*
- Identificação de riscos com potencial impacto na segurança da informação
- Norma associada: IS.I.OR.205(d–f), IS.I.OR.210(c)

Camada 3 - Módulo MoC

Management of Change como gatilho de convergência dinâmica:

- Deteção automática de mudanças tecnológicas/organizacionais
- Avaliação semântica de impacto por IA
- Acionamento da ponte ISMS↔SMS quando necessário
- Norma associada: IS.I.OR.205(g), IS.I.OR.220

Camada 4 - Ponte Cognitiva ISMS↔SMS

- Coração analítico do CESAR, ativado apenas quando há interdependência:
- Correlação causal usando modelos *bayesianos* e grafos de conhecimento
- Cálculo do *Composite Risk* Index (CRI)
- Explicabilidade automática via XAI (LIME/SHAP)
- Norma associada: IS.I.OR.210, IS.I.OR.215

Camada 5 - Repositório Integrado

- Repositório único de rastreabilidade e auditoria:
- Base de dados relacional com metadados Part-IS
- *Dashboards* BI e alertas automatizados
- Conformidade RGPD/NIS2 com cifragem AES-256
- *Audit Trail* inviolável com *hashing* SHA-256

- Norma associada: IS.I.OR.215

Eixo Transversal - IA Semântica & XAI

Camada cognitiva que percorre todas as demais:

- NLP Regulatório: Interpretação de normas EASA/ICAO/CNCS
- Análise Preditiva: Identificação de tendências e padrões
- Fusão de Dados: Integração ISMS + SMS
- XAI *Engine*: Explicabilidade conforme EU AI Act
- Retroalimentação: Aprendizagem contínua

7.5. Estrutura do Fluxos Operacionais

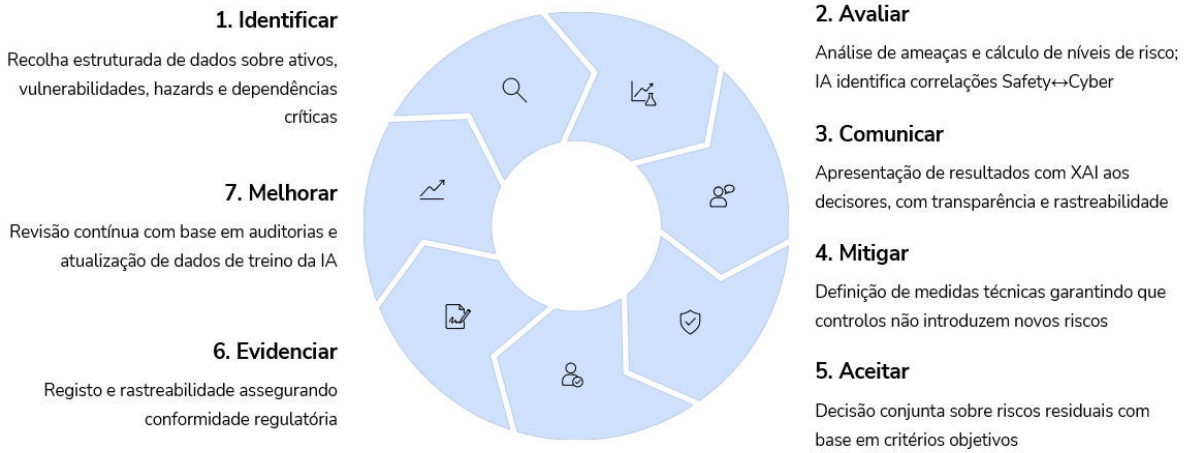
O CESAR *Framework* estrutura-se em sete fases sequenciais - (1) identificar, (2) avaliar, (3) comunicar, (4) mitigar, (5) aceitar, (6) evidenciar e (7) melhorar - que operacionalizam um ciclo PDCA (*Plan-Do-Check-Act)* contínuo aplicado de forma integrada aos domínios ISMS e SMS.

Cada fase funciona como um módulo analítico dentro de um *pipeline* de decisão, assegurando recolha sistemática de dados, avaliação probabilística, comunicação rastreável, definição de controlos proporcionais, aceitação fundamentada e documentação auditável. Esta estrutura de ciclo de vida, Figura 14, garante aderência direta aos requisitos do EASA Part-IS, que estabelece a necessidade de processos consistentes de identificação, análise, comunicação, tratamento e verificação de riscos de segurança da informação com impacto na aviação, e alinha-se igualmente com o ICAO *Annex* 19, que exige mecanismos formais de gestão de riscos operacionais, monitorização contínua, tomada de decisão informada e melhoria permanente do sistema de *safety*.

Ao combinar estes princípios num fluxo técnico-operacional único, o CESAR assegura que os riscos cibernéticos e operacionais são tratados por critérios harmonizados e evidenciáveis, permitindo que a "ponte cognitiva" *Safety↔Cyber* seja ativada sempre que a IA identifica correlações materialmente relevantes entre ameaças, vulnerabilidades e *hazards*. O resultado é um ciclo fechado de gestão integrada de risco que cumpre simultaneamente as obrigações regulamentares europeias e internacionais, reforçando a coerência metodológica, a rastreabilidade e a melhoria contínua, de acordo com as melhores práticas de gestão de ISMS,

conforme a ISO/IEC 27001:2022, e de gestão de risco, seguindo as diretrizes da ISO/IEC 27005:2022 (e, de forma complementar, os princípios da ISO 31000:2018).

Fig. 14 - Fase do *Framework* do CESAR



Fonte: CESAR - Definição do Modelo

A seguir especifica-se cada uma das sete fases que estruturam o fluxo do CESAR *Framework*, descrevendo os processos, responsabilidades e interações essenciais entre ISMS e SMS.

Fase 1 - Identificar

Objetivo: Detetar, estruturar e compreender todos os elementos que influenciam o risco, ativos, vulnerabilidades, ameaças, *hazards*, relatórios FDM e de *Safety*, mudanças (MoC), documentação organizacional e requisitos regulamentares. Cinco Dimensões Complementares

Dimensões de Identificação

1. Inventário de Ativos:
2. Vulnerabilidades e Ameaças:
3. *Hazard Identification* (SMS):
4. Gestão de Mudança (MoC):

5. Documentação Técnica e Organizacional:
6. Requisitos Legais e Regulamentares:
7. Inteligência Externa:

Aplicação da IA

- Recolha e correlação automática de dados
- Deteção de padrões de ameaça
- Mapeamento de interdependências *Safety*↔*Cyber*
- Priorização inteligente de riscos

Nesta fase, a IA atua como motor semântico de análise, utilizando *Natural Language Processing* (NLP) e modelos contextuais para interpretar documentação técnica, políticas internas, relatórios de ocorrências e bases regulatórias. Essa análise permite identificar automaticamente ativos, vulnerabilidades, *hazards* e alterações relevantes, bem como mapear dependências entre *safety* e *cybersecurity*. A IA correlaciona eventos, deteta padrões e prioriza riscos com base em significado operacional e criticidade, tornando o processo de identificação mais rápido, consistente e abrangente.

Fase 2 - Avaliar

Objetivo

Analisar, quantificar e priorizar o nível de risco considerando probabilidade, severidade, impacto cruzado e aceitabilidade regulatória.

Três Níveis de Análise

1. **Avaliação Individual:** ISMS (CIA) e SMS (Prob×Sev×Detet) separadamente
2. **Avaliação Cruzada Bidirecional**: Mesmo sem impacto direto, avaliação recíproca
3. **Avaliação Composta**: *Composite Risk Index* (CRI) quando há interdependência

   Quando existe interdependência material, aplica-se a métrica unificada que integra:

   - **CIA *Score* (ISMS):** (C + I + A) / 3
   - ***Safety Score* (SMS):** Probabilidade × Severidade

- **Ponderação Dinâmica:** ajustada conforme criticidade do ativo e grau de interdependência

O resultado é um índice único que permite decisões de mitigação mais consistentes e alinhadas entre ambos os domínios.

Papel da IA

Na fase de avaliação, a Inteligência Artificial atua como mecanismo central de análise, correlação e priorização de risco. O seu contributo centra-se em quatro dimensões fundamentais:

1. **Quantificação automática do risco:**

   A IA processa grandes volumes de dados operacionais e de cibersegurança (telemetria, *logs*, relatórios de *safety*, vulnerabilidades, histórico de incidentes), gerando estimativas de probabilidade e severidade mais consistentes e menos sujeitas a viés humano.

2. **Correlação entre domínios ISMS–SMS:**

   A IA identifica interdependências entre impactos CIA e efeitos operacionais, detetando relações invisíveis à avaliação manual (ex.: uma vulnerabilidade que afeta disponibilidade pode ter impacto direto na capacidade operacional).

3. **Cálculo assistido do *Composite Risk Index* (CRI):**

   O sistema pondera dinamicamente os *scores* de segurança da informação e de *safety*, ajustando o peso da interdependência entre domínios com base em padrões históricos, contexto operacional e criticidade do ativo.

4. **Priorização inteligente:**

   A IA aplica modelos de aprendizagem supervisionada e não supervisionada para sugerir prioridades de tratamento, destacando os riscos com maior potencial de gerar consequências operacionais ou regulatórias.

A IA Explicável (XAI), funciona como um apoio analítico avançado, contribuindo para a quantificação automática dos riscos, análises preditivas e cálculo do *Composite Risk Index*, a interpretação e validação final permanecem sempre sob responsabilidade dos decisores

competentes, o CISO no domínio ISMS e o *Safety Manager* no domínio SMS. Assim, a IA complementa a capacidade humana de deteção e correlação, oferecendo maior profundidade analítica, enquanto a decisão sobre aceitabilidade, impacto e necessidade de mitigação continua a ser exclusivamente humana, assegurando responsabilidade, transparência e confiança em todo o processo.

Fase 3 - Comunicar

A comunicação dos riscos, decisões e medidas de mitigação é um elemento central do CESAR *Framework*, garantindo alinhamento organizacional, transparência regulatória e coerência entre os domínios ISMS e SMS. Esta fase estrutura-se em quatro níveis complementares:

1. **Comunicação Técnica (ISMS/SMS):**

   Divulgação de resultados detalhados das avaliações de risco, incluindo justificações produzidas por IA Explicável (XAI), de forma a apoiar a rastreabilidade e a tomada de decisão em ambos os domínios.

2. **Comunicação Gerencial/Executiva:**

   Apresentação de *dashboards* visuais, relatórios consolidados e indicadores críticos de risco para a gestão de topo, permitindo visão estratégica e priorização informada de recursos.

3. **Comunicação Regulamentar/Externa:**

   Produção automática de relatórios em conformidade com os requisitos do EASA Part-IS, Diretiva NIS2, Reguladores da indústria (EASA, ANAC, CNCS) e demais obrigações aplicáveis, assegurando resposta adequada a auditorias e eventos externos.

4. **Comunicação Interdepartamental:**

   Troca contínua e bidirecional de informação entre ISMS e SMS, assegurando que decisões, medidas mitigadoras e incidentes relevantes são partilhados de forma estruturada e tempestiva.

Papel da IA

Na fase de comunicação, a Inteligência Artificial atua como suporte analítico e documental, mas nunca como agente decisor. A IA organiza e sintetiza resultados de risco, gera visualizações automáticas e produz explicações claras através de mecanismos de IA Explicável (XAI), assegurando que cada conclusão é transparente e auditável. Além disso, automatiza relatórios técnicos e regulatórios em conformidade com o EASA Part-IS e a Diretiva NIS2, reduzindo esforço manual e aumentando consistência.

Fase 4 - Mitigar

A fase de mitigação transforma os resultados da avaliação em ações concretas, assegurando que cada risco identificado recebe um tratamento adequado e alinhado com os requisitos regulatórios do ISMS e do SMS.

A mitigação estrutura-se em cinco componentes principais:

1. **Planeamento:**
   A IA apoia a definição de medidas de mitigação sugerindo controlos baseados em boas práticas, conhecimento acumulado e correlação histórica de incidentes, sem substituir o julgamento técnico dos responsáveis.

2. **Análise de Impacto Cruzado:**
   Cada medida proposta é avaliada quanto ao impacto simultâneo nos domínios de *safety* e cibersegurança, garantindo coerência entre requisitos operacionais e de proteção digital.

3. **Implementação Coordenada:**
   As ações de mitigação são executadas de forma articulada entre ISMS e SMS, assegurando alinhamento entre equipas, processos e responsabilidades.

4. **Monitorização de Eficácia:**
   Após a implementação, são realizadas validações técnicas e operacionais para confirmar se as medidas reduziram efetivamente o risco nos níveis esperados.

5. **Documentação:**
   Todos os passos são registados com rastreabilidade completa, permitindo auditorias, inspeções regulatórias e melhoria contínua.

Papel da IA

Na fase de mitigação, a Inteligência Artificial apoia o processo através da sugestão de controlos, análise de impacto cruzado e priorização de ações, utilizando padrões históricos, bases de conhecimento e correlação entre incidentes. A IA ajuda a identificar a eficácia provável de cada medida, estimando efeitos secundários nos domínios ISMS e SMS e destacando possíveis conflitos operacionais. Além disso, contribui para a monitorização pós-implementação, analisando desvios, indicadores de desempenho e sinais de risco residual.

Fase 5 - Aceitar

Processo de Aceitação

1. Validação de Mitigação: IA compila evidências de eficácia
2. Análise Conjunta: CISO + *Safety Manager* avaliam reciprocamente
3. Documentação XAI: Justificação explicável da decisão
4. Gestão de Mudança: MoC como gatilho de reavaliação

Critério Fundamental: Aceitação requer aprovação simultânea de CISO E *Safety Manager*. Se um rejeitar, ciclo reabre automaticamente para nova mitigação.

Fase 6 - Evidenciar

A fase de Evidenciação assegura que todo o processo de gestão de riscos, desde a identificação até à aceitação, está documentado de forma transparente, verificável e auditável. Esta etapa é essencial para demonstrar conformidade com o EASA Part-IS, apoiar auditorias internas/externas e assegurar rastreabilidade contínua. A evidenciação organiza-se em quatro eixos principais:

1. **Consolidação Multidomínio:**

Reúne evidências provenientes simultaneamente do ISMS e do SMS, assegurando que os riscos com impacto cruzado foram tratados de forma coordenada e coerente.

2. **Validação Regulamentar**:

   A IA confirma automaticamente o alinhamento com requisitos aplicáveis, incluindo EASA Part-IS, NIS2 e políticas internas, verificando se todos os controlos obrigatórios foram implementados e documentados.

3. **Geração Automática de Relatórios**:

   São produzidos relatórios executivos, técnicos e regulamentares de forma automatizada, otimizando o processo de prestação de contas e garantindo consistência na comunicação com gestores, autoridades e auditores.

4. ***Audit Trail* e Rastreabilidade**:

   Toda a informação é armazenada com registos de auditoria completos, incluindo *hashing* criptográfico (como SHA-256), garantindo integridade, autenticidade e preservação das evidências ao longo do tempo.

Fase 7 - Melhorar

A última fase do ciclo CESAR consolida o princípio de melhoria contínua, assegurando que a organização evolui a partir da experiência acumulada, das lições aprendidas e da monitorização sistemática do desempenho. Esta fase estrutura-se em quatro vetores principais:

1. **Análise de Desempenho**:

   Avaliam-se a eficácia das medidas implementadas, os indicadores-chave de desempenho (KPIs) e a evolução do risco residual, permitindo identificar áreas que necessitam de reforço ou otimização.

2. ***Feedback Loop***:

   Os resultados desta fase alimentam novamente as etapas de Identificar e Avaliar, garantindo que novos padrões, falhas emergentes ou mudanças operacionais são imediatamente incorporados no ciclo de gestão de risco.

3. **Aprimoramento da IA**:

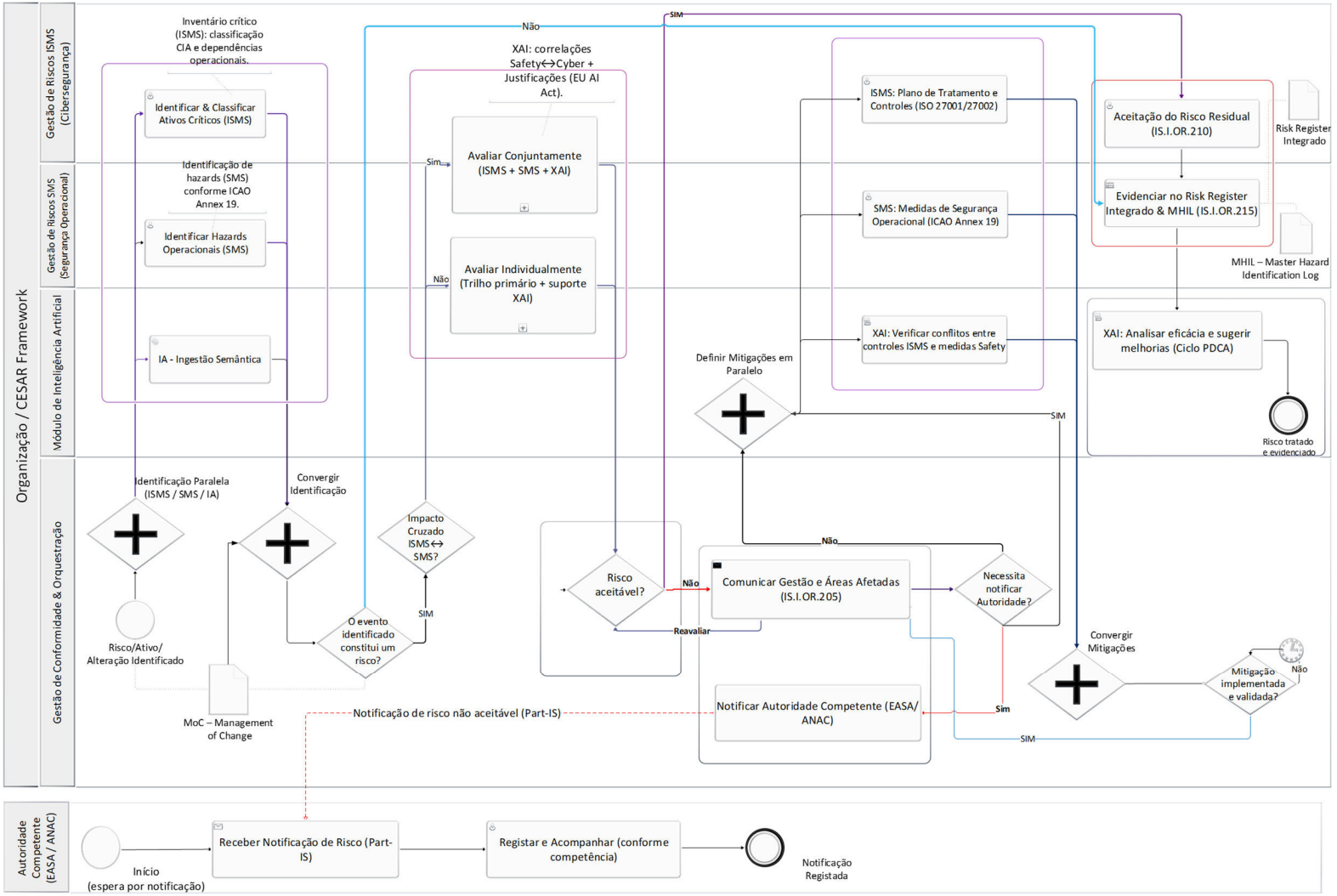
   Os modelos de IA são recalibrados com supervisão humana, incorporando novos dados, correções, ajustamentos de parâmetros e validações que aumentam a precisão, a explicabilidade e a confiança no sistema.

4. **Revisão de Políticas e Procedimentos**:

   Políticas internas, controlos, matrizes de risco e processos operacionais são atualizados com base em evidências, auditorias, recomendações regulatórias e boas práticas, fortalecendo a maturidade organizacional e a resiliência.

A Figura 15 apresenta uma visão integrada dos fluxos BPMN processuais do CESAR, demonstrando a natureza cíclica, iterativa e evolutiva do modelo.

Fig. 15 - Fluxo BPMN representando cada fase do Modelo CESAR



Fonte: Definição BPMN CESAR

Em todas as fases do CESAR *Framework*, a Inteligência Artificial atua como um elemento de suporte avançado, analisando dados, identificando padrões, sugerindo medidas e produzindo explicações transparentes através de XAI, mas nunca como substituto da supervisão humana. Em conformidade com o princípio de *meaningful human control* definido pelo (EU) AI Act e com os requisitos do EASA Part-IS, a IA não toma decisões autónomas nem implementa medidas sem validação. Assim, todas as recomendações geradas pelos modelos são obrigatoriamente revistas, interpretadas e aprovadas pelos responsáveis competentes, o CISO no âmbito da cibersegurança e o *Safety Manager* no domínio operacional, assegurando que o processo permanece transparente, auditável e alinhado com as obrigações regulatórias. Este equilíbrio entre automação avançada e autoridade humana garante que a IA reforça a gestão integrada de riscos, sem comprometer a responsabilidade institucional nem a segurança da aviação.

7.5. Demonstração de Conformidade Regulatória

O CESAR *Framework* foi concebido desde o início para satisfazer simultaneamente múltiplos requisitos regulatórios. A Tabela da Figura 16 demonstra mapeamento exaustivo entre fases do modelo e cláusulas regulatórias.

Fig. 16 - Tabela Matriz de Conformidade Regulatória do CESAR

Fase CESAR	EASA Part-IS	ISO 27001/27005	NIS2	EU AI Act
Identificar	IS.I.OR.205 (a)(1-2) Identify risks.	ISO 27005 Clause 7.2 *Asset identif.*	Art. 21(2)(a) *Risk assessment*	Art. 9(2) *Risk mgmt system*
Avaliar	IS.I.OR.205 (c) *Risk assessment, safety* impact	ISO 27005 Clause 8 *Risk assessment*	Art. 21(2)(b) *Risk analysis*	Art. 15 *Accuracy, robustness*
Comunicar	IS.I.OR.210 (b) *Communication*	ISO 27001 Clause 7.4 *Communication*	Art. 23 *Notification*	Art. 13 *Transparency to users*
Mitigar	IS.I.OR.210 (a) *Risk treatment*	ISO 27005 Clause 9 *Risk treatment*	Art. 21(2)(c) *Risk treatment*	Art. 14 *Human oversight*
Aceitar	IS.I.OR.205 (d) Review + Accept	ISO 27005 Clause 9.4 *Risk acceptance*	Art. 20(1) *Governance approval*	Art. 9(4) *Risk acceptance*
Evidenciar	IS.I.OR.215/240 Report/Record-Keep	ISO 27001 Clause 9.2/9.3 *Audit*	Art. 23 *Reporting obligations*	Art. 12 *Record-keeping*
Melhorar	IS.I.OR.260 Continuous improvement	ISO 27001 Clause 10 *Improvement*	Art. 21(2)(g) *Policies review*	Art. 17 *Quality management*

Fonte: Análise comparativa de requisitos regulatórios.

O CESAR *Framework* evidencia um nível elevado de conformidade regulatória, assegurando aderência transversal aos principais referenciais europeus:

- **100% (7/7)** dos requisitos nucleares do **EASA Part-IS**
- **86% (6/7)** das cláusulas estruturantes da **ISO/IEC 27001**
- **83% (5/6)** dos artigos relevantes da **Diretiva NIS2**
- **86% (6/7)** dos artigos aplicáveis do **EU AI Act**

Esta conformidade multirreferencial permite às organizações reduzir significativamente o esforço de *compliance*, uma vez que um único modelo de implementação assegura alinhamento simultâneo com diversos padrões regulatórios e normativos.

8. VALIDAÇÃO CONCEPTUAL E ACEITAÇÃO ORGANIZACIONAL

8.1. Introdução

Este capítulo apresenta o processo de validação conceptual do CESAR através de *workshop* realizado com profissionais da EuroAtlantic Airways (EAA), constituindo a Fase 4 (Demonstração) e Fase 5 (Avaliação) da metodologia *Design Science Research* descrita no Capítulo 2.

Importa esclarecer desde o início que a validação realizada é de natureza conceptual e exploratória, não técnica ou empírica. O *workshop* teve como objetivo:

- Avaliar a aceitação organizacional do modelo proposto,
- Verificar a compreensibilidade do *framework* por profissionais,
- Identificar requisitos práticos para futura implementação,
- Recolher *feedback* qualitativo sobre viabilidade e aplicabilidade

O que NÃO foi validado:

- Performance técnica de algoritmos de IA,
- Integração com sistemas existentes (ERP, IQSMS, FDM),
- Métricas de *accuracy*, false positives, ou eficácia,
- Conformidade regulatória operacional verificada,
- Redução mensurável de incidentes ou riscos.

Esta distinção é fundamental para interpretação correta dos resultados apresentados nas secções seguintes.

8.2. Objetivos da Validação Conceptual

A validação conceptual do CESAR *Framework* foi estruturada em cinco objetivos específicos, definidos de acordo com os princípios de avaliação de artefactos no *Design Science Research* (Hevner et al., 2004):

Objetivo 1: Avaliar a Compreensibilidade do Modelo

Examinar se profissionais de diferentes domínios (IT, *Safety*, *Security* e Operações) conseguem compreender claramente a lógica do CESAR, as suas fases e os mecanismos de integração entre ISMS e SMS.

Objetivo 2: Aferir o Grau de Aceitação Organizacional

Determinar se o modelo é percebido como viável, útil e desejável no contexto organizacional, identificando potenciais fontes de resistência cultural, processual ou estrutural.

Objetivo 3: Identificar Requisitos Técnicos para Implementação

Recolher informação sobre necessidades técnicas essenciais à futura operacionalização do modelo, incluindo infraestrutura tecnológica, disponibilidade de dados, integração com sistemas existentes e requisitos de automação.

Objetivo 4: Validar o Alinhamento Regulatório

Confirmar que o mapeamento entre o ciclo CESAR e os requisitos do EASA Part-IS é interpretado como correto, consistente e completo pelos profissionais com conhecimento da regulamentação europeia aplicável.

Objetivo 5: Recolher Contributos para Melhoria Contínua do Artefacto

Obter sugestões de melhoria, ajustes metodológicos ou funcionalidades adicionais que possam aumentar a aplicabilidade prática, a precisão analítica e o valor organizacional do modelo.

8.3. Preparação do *Workshop*

8.3.1. Planeamento e Desenho

O *workshop* foi planeado seguindo abordagem participativa e interativa, privilegiando demonstração prática e discussão aberta sobre apresentação formal unilateral.

Formato: Sessão presencial única

Duração: 4 horas (com pausa de 15 minutos)

Local: Sala de reuniões EuroAtlantic Airways, Carnaxide, Lisboa

Data: 2025

Estrutura da Sessão:

Parte 1 (90 min): Apresentação Conceptual

- Contexto regulatório (EASA Part-IS, NIS2, AI Act)
- Lacunas identificadas na RSL
- Princípios e arquitetura do CESAR
- Ciclo das 7 fases detalhado

Parte 2 (60 min): Demonstração de Cenários

- Cenário A (SMS): Análise de relatório FDM
- Cenário B (ISMS): Vulnerabilidade em servidor aplicacional
- Cenário C (Integrado): Falha ERP com impacto operacional

Parte 3 (90 min): Discussão e *Feedback*

- Sessão aberta de perguntas e respostas
- Discussão sobre viabilidade técnica
- Identificação de requisitos e barreiras
- Sugestões de melhoria

Materiais Preparados:

- Apresentação PowerPoint (55 slides)
- Diagramas BPMN das fases CESAR (formato A3)
- *Mockups* de *dashboards* (visualizações estáticas)
- Documento síntese (2 páginas) distribuído aos participantes

8.3.2. Caracterização dos Participantes

O *workshop* reuniu 10 profissionais da EuroAtlantic Airways, cuidadosamente selecionados para representar as áreas-chave afetadas pela integração ISMS-SMS, ver tabela 17.

Tabela 17 - Perfil dos Participantes do *Workshop*

ID	Função	Departamento	Exp.(anos)	Formação
P1	CISO / IT *Manager*	IT	30	Eng. Informática
P2	*Safety Manager*	*Safety* & QA	20	Eng. Aeronáutica
P3	*Security Manager*	*Security*	12	Gestão
P4	*Chief Pilot*	*Flight Ops*	30	Piloto Comercial
P5	*Accountable Manager*	Direção	30	Eng. Aeronáutica
P6	CFO	Financeiro	20	Economia
P7	Diretor Técnico	Manutenção	22	Eng. Mecânica
P8	*Project Manager*	PMO	35	Gestão
P9	*Developer*	IT	6	Informática
P10	*Infrastructure Lead*	IT	20	Redes/Sistemas

Fonte: Dados recolhidos via formulário pré-*workshop*.

Análise do Perfil:

- Experiência média: 22,5 anos (desvio padrão: 9 anos),
- Diversidade departamental: 6 áreas distintas representadas,
- Nível hierárquico: *Mix* de gestão executiva (P5, P6), gestão intermédia (P1-P4, P7) e técnicos (P8-P10),
- Familiaridade com EASA Part-IS: 7/10 participantes (70%) tinham conhecimento prévio do regulamento.

A composição hierárquica refletiu um equilíbrio entre perspetivas múltiplas, técnica (IT), operacional (*Safety*/Ops), estratégica (Direção), e regulatória (*Safety*/*Security*), permitindo captar perspetivas estratégicas, operacionais e tecnológicas. Adicionalmente, 70% dos participantes reportaram possuir conhecimento prévio do EASA Part-IS, reforçando a robustez da análise de alinhamento regulatório do modelo.

8.3.3. Instrumentos de Recolha de Dados

Dado o carácter exploratório da validação, optou-se por instrumentos qualitativos que privilegiassem profundidade sobre quantificação:

Instrumento 1: Observação Participante. A investigadora (que conduziu o *workshop*) registou:

- Nível de *engagement* dos participantes
- Reações não-verbais durante apresentação
- Dinâmica de interação entre áreas
- Momentos de confusão ou clareza

Instrumento 2: Registo de Perguntas. Todas as questões formuladas pelos participantes foram documentadas textualmente, capturando:

- Formulação exata da pergunta
- Identidade do participante (anonimizada como P1-P10)
- Momento da sessão em que surgiu

Instrumento 3: Notas de Discussão. Durante a Parte 3, foram registadas:

- Sugestões de melhoria propostas
- Correções identificadas
- Preocupações levantadas
- Casos de uso adicionais sugeridos

Limitação Metodológica Reconhecida: Não foram utilizados instrumentos quantitativos estruturados (questionários com escalas Likert, por exemplo) que permitiriam medição estatística de aceitação. Esta foi escolha deliberada dado:

- Amostra pequena (n=10) inadequada para análise estatística

- Prioridade em *feedback* qualitativo profundo
- Natureza exploratória da validação conceptual

8.3.4. Procedimentos de Condução

Preparação Pré-*Workshop*:

- Convites enviados 3 semanas antes
- Documento preparatório (5 páginas) distribuído 1 semana antes
- Confirmação de participação e recolha de perfis
- Preparação de sala com TV, quadro interativo, materiais impressos

Durante o *Workshop*:

- Introdução e explicação dos objetivos (10 min)
- Parte 1: Apresentação sem interrupções, perguntas no final (90 min)
- Pausa (15 min)
- Parte 2: Demonstração interativa de cenários (60 min)
- Parte 3: Discussão aberta facilitada pela investigadora (90 min)

Gestão da Discussão para garantir participação equilibrada:

- Perguntas dirigidas especificamente a participantes silenciosos
- Moderação de discussões para evitar domínio de vozes individuais
- Incentivo a perspetivas divergentes

Registo de Dados:

- Notas manuscritas pela investigadora
- Fotografias dos diagramas anotados pelos participantes

8.4. Execução do *Workshop*

8.4.1. Preparação e Materiais

A apresentação foi estruturada para construir compreensão progressiva do CESAR, partindo do contexto regulatório até aos detalhes técnicos.

Slide Deck (55 slides):

- Slides 1-10: Contexto (ameaças *cyber*, incidentes, regulação)
- Slides 11-20: Lacunas identificadas na RSL (com dados quantitativos)
- Slides 21-35: CESAR *Framework* detalhado (arquitetura, fases)
- Slides 36-45: Mapeamento regulatório (Part-IS, NIS2, AI Act)
- Slides 46-55: Cenários de aplicação e próximos passos

Diagramas BPMN (3 fluxos). Impressos em formato A3 para discussão colaborativa:

- Fluxo "Identificar + Avaliar" (*swimlanes*: ISMS, SMS, IA, MoC)
- Fluxo "Comunicar + Mitigar" (com decisão gates e aprovações)
- Fluxo "Aceitar + Evidenciar + Melhorar" (ciclo fechado)

8.4.2. Dinâmica da Sessão

A apresentação iniciou-se com contextualização do problema através de dados concretos da RSL (Cap. 3): apenas 5% dos estudos abordam Part-IS, degradação de performance 87,3% → 74,8%. Este enquadramento quantitativo gerou *engagement* imediato, com vários participantes fazendo anotações. O *Safety Manager* (P2) interveio espontaneamente após os slides sobre convergência *Safety-Security-Cybersecurity*, comentando "Isto é exatamente o que precisamos. Hoje o CISO reporta-me incidentes, mas não consigo avaliar o impacto real em *safety*.".

A apresentação das 7 fases do CESAR gerou particular interesse. O *Accountable Manager* (P5) solicitou pausa para esclarecer a diferença entre "Aceitar" e "Evidenciar", revelando necessidade de clarificação terminológica.

Parte 2: Demonstração de Cenários (60 min):

Cenário A: Análise de Relatório FDM. Simulou-se deteção pelo *Flight Data Monitoring* de *exceedance* (excesso de velocidade em aproximação). O CESAR:

- Identificou o evento via *parsing* do relatório FDM
- Classificou como risco *safety* (severidade: média)
- Correlacionou com dados meteorológicos e *NOTAMs*
- Recomendou: investigação SMS padrão
- Verificou se havia componente *cyber* (ex: falha FMS) → Não detetado

Feedback: *Chief Pilot* (P4) validou que o fluxo corresponde ao processo SMS atual, mas valorizou a verificação automática de potencial causa *cyber*.

Cenário B: Vulnerabilidade em Servidor Aplicacional. Simulou-se alerta de CVE crítico em *WebLogic* que suporta aplicação de tripulações. O CESAR:

- Identificou vulnerabilidade via *feeds* MITRE ATT&CK
- Classificou como risco ISMS (CIA: alta disponibilidade)
- Correlacionou com inventário de ativos → Servidor crítico
- Avaliou potencial impacto SMS → Indisponibilidade de *roster* afeta operações
- Recomendou: *patching* urgente + avaliação pelo *Safety Manager*

Feedback: CISO (P1) questionou "Como a IA distingue entre servidor crítico e não-crítico?" Resposta: Através de inventário de ativos previamente classificado (IS.I.OR.205(a)).

Cenário C: Falha ERP Financeiro (Caso Integrado). Simulou-se indisponibilidade do ERP que gere pagamentos. O CESAR:

- Identificou falha técnica via *logs*
- Classificou inicialmente como risco ISMS (disponibilidade)
- Correlação IA identificou potencial impacto SMS:
    - Atraso pagamento salários → moral tripulações
    - Atraso pagamento fornecedores críticos → manutenção
- Recomendou: avaliação cruzada CISO + *Safety Manager*
- Sugestão: contingência financeira + comunicação proativa

Feedback: Este cenário gerou discussão intensa. CFO (P6) comentou "Nunca pensei em falha financeira como risco *safety*. Faz sentido." *Security Manager* (P3) sugeriu incluir também riscos de fraude/*insider"*.

Durante este cenário, identificou-se necessidade de módulo de rejeição rápida de sugestões irrelevantes da IA (correção #1 - ver secção 8.5.2).

Parte 3: Discussão e *Feedback*. Esta fase foi a mais rica em dados qualitativos. A discussão organizou-se naturalmente em torno de quatro temas:

Tema 1: Viabilidade Técnica

- Discussão sobre infraestrutura IT necessária, capacidade de
- processamento, integração com sistemas legados. *Developer* (P9) e
- *Infrastructure Lead* (P10) fizeram perguntas técnicas detalhadas sobre
- APIs, formatos de dados, latência.

Tema 2: Governança e Responsabilidades. Debate sobre quem seria "dono" do CESAR na organização. *Accountable Manager* (P5) enfatizou necessidade de clareza nas responsabilidades entre CISO e *Safety Manager*.

Tema 3: Gestão de Mudança.

Security Manager (P3) levantou questão cultural "Como garantir que pessoas usarão o sistema e não o verão como mais uma ferramenta de controlo?"

Tema 4: Próximos Passos Práticos (15 min)

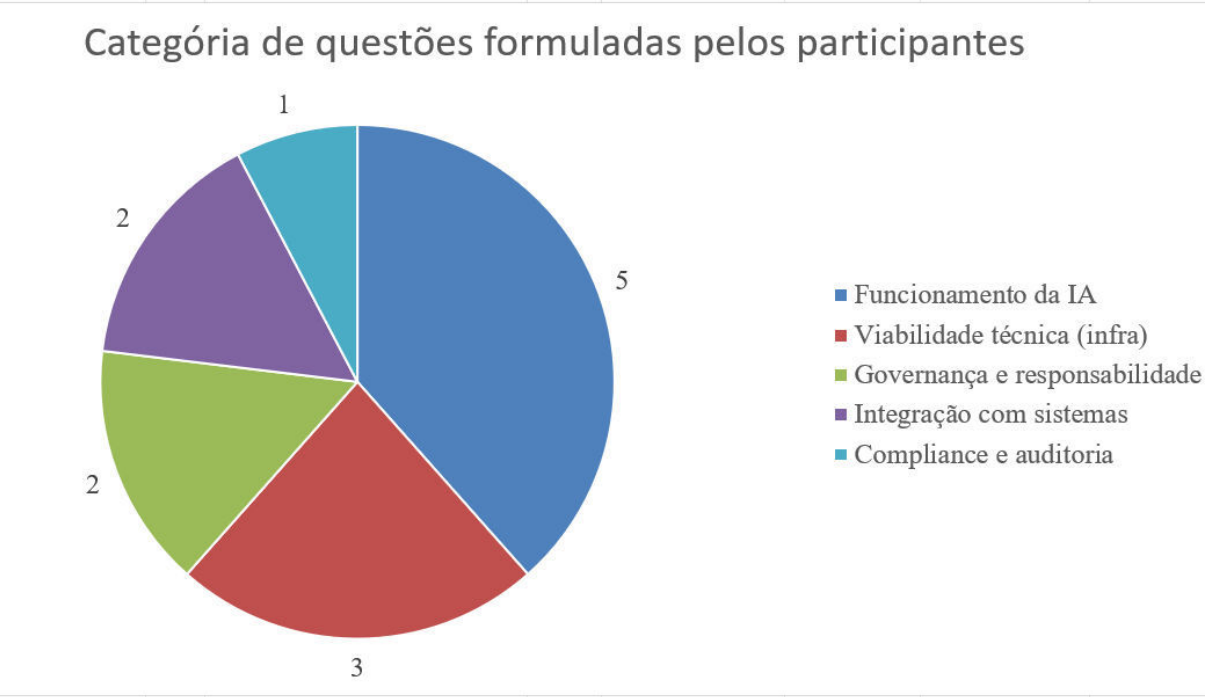
Project Manager (P8) propôs abordagem faseada: começar com piloto em âmbito reduzido antes de *roll-out* completo.

8.5. Resultados da Validação

8.5.1. Questões Levantadas pelos Participantes

Durante o *workshop*, foram formuladas 13 questões pelos participantes, refletindo preocupações legítimas sobre implementação prática do CESAR, ver Gráfico 2.

Gráfico 2 - Categoria de questões formuladas pelos participantes



Fonte: Análise das questões registadas durante *workshop*.

A predominância de questões sobre IA (38,5%) evidencia que este é o elemento menos familiar dos participantes, requerendo maior esforço de explicação e desmistificação. A preocupação com viabilidade técnica (23,1%) reflete consciência realista sobre desafios de implementação.

Questões Selecionadas e Respostas:

Q1: "Como funciona a parte da IA?" (P3, P7, P9)

A recorrência desta pergunta revelou necessidade de explicação mais detalhada sobre o motor de IA. Esclareceu-se que o CESAR utiliza abordagem híbrida: ML para classificação + regras lógicas para correlação, com XAI garantindo que cada recomendação é justificada.

Q2: "O que é esta IA XAI?" (P4, P5)

Explicou-se que XAI (*Explainable* AI) significa que cada decisão da IA vem acompanhada de explicação: "Classifiquei este risco como alto porque: (1) CVE score > 9.0, (2) ativo é crítico, (3) sem *patch* disponível." Esta transparência é exigida pelo (EU) AI Act.

Q3: "A EuroAtlantic tem condições de desenvolver o projeto?" (P6, P8)

Discussão honesta sobre maturidade tecnológica da organização. Concluiu-se que EAA possui base (servidores, dados, *logs*) mas necessitaria de apoio externo especializado para desenvolvimento inicial do motor de IA. Alternativa: adquirir solução comercial e customizá-la ao CESAR.

Q4: "O módulo de IA é um módulo comprado?" (P1, P9)

Esclareceu-se que o CESAR é *framework* conceptual, não produto comercial. A implementação técnica poderia seguir três caminhos: (a) desenvolvimento interno, (b) aquisição de plataforma GRC e customização, ou (c) parceria com fornecedor especializado.

Q5: "Quanto tempo levaria para termos o modelo implementado?" (P5, P8)

Estimativa conservadora apresentada:

- Fase 1 (*Design* detalhado + integração dados): 6 meses
- Fase 2 (Desenvolvimento IA + testes): 9 meses
- Fase 3 (Piloto controlado): 6 meses
- Total: ~21 meses até produção completa

Q6: "Como funciona o treino da IA?" (P2, P9)

Explicou-se conceito de *supervised learning* com dados históricos da EAA (*logs*, incidentes, relatórios SMS) combinados com bases externas (ENISA, MITRE). Treino seria iterativo, com validação humana contínua.

Q7: "No âmbito do EASA Part-IS, o próprio modelo deve ter os riscos avaliados?" (P2)

Resposta afirmativa enfática. Esta questão demonstrou maturidade regulatória do participante. Confirmou-se que o CESAR, como sistema de informação crítico, deve estar no inventário de ativos (IS.I.OR.205(a)) e ter seus próprios riscos avaliados (meta-risco).

Q8: "Se é visível na EAA hoje?" (P3)

Esclareceu-se que não: CESAR está em fase de validação conceptual, sem implementação técnica. O *workshop* serve precisamente para avaliar viabilidade antes de eventual desenvolvimento.

Q9: "Níveis de acesso?" (P1, P3)

Discussão sobre modelo RBAC (*Role-Based Access Control*): *Safety Manager* vê tudo de *safety* + correlações *cyber*; CISO vê tudo de *cyber* + correlações *safety*; Direção vê *dashboard* agregado; Auditores veem *logs* completos.

Q10: "Se a IA vai 'beber' na Internet?" (P1)

Preocupação legítima sobre segurança. Esclareceu-se que IA não opera em tempo real com fontes externas abertas. Utiliza bases de dados internas + *feeds* certificados pré-validados (ENISA, CERT-EU, CNCS) sincronizados periodicamente.

Q11: "Como a IA lê os *logs*? Por exemplo, da rede ou do IQSMS." (P9, P10)

Explicação técnica sobre ETL (*Extract-Transform-Load*) e NLP. *Logs* são interpretados, entidades extraídas (IPs, *timestamps*, eventos), e correlacionados semanticamente com relatórios SMS.

Q12: "Como avaliamos os dados?" (P2, P8)

Discussão sobre *data governance*: qualidade de dados é crítica para IA. CESAR deve incluir módulo de validação que verifica completude, consistência e atualidade dos dados antes de processar.

Q13: "Foi falado do viés que pode ser criado na IA." (P5)

Discussão sobre *bias* algorítmico. Explicou-se que XAI ajuda a identificar viés (ex: IA sempre classificando certos tipos de eventos como mais graves). Mitigação: *datasets* balanceados + revisão humana periódica + retreino.

8.5.2. Correções Identificadas Durante Demonstração

Durante os cenários práticos, emergiram duas correções importantes ao modelo inicial:

Correção #1: Tratamento de Sugestões Irrelevantes da IA.

No Cenário C (ERP financeiro), a IA sugeriu avaliar se havia componente de *ransomware* (dado que indisponibilidade é sintoma comum). Após investigação (simulada), confirmou-se que era falha técnica banal, sem componente malicioso.

Problema Identificado: O modelo original não previa mecanismo ágil para "descartar" sugestões da IA rapidamente quando claramente irrelevantes, forçando processo completo de avaliação.

Solução Proposta: Adicionar ao ciclo CESAR um "*fast-track rejection gate*" na fase Avaliar:

- Se analista humano determina (com justificativa) que sugestão IA é irrelevante → marca como "Rejeitado - Falso Positivo".
- Evento é arquivado (não eliminado) para *audit trail*.
- IA aprende com estes *rejections* (*feedback loop*).

Impacto: Reduz carga de trabalho sem comprometer rigor. Mantém rastreabilidade (Part-IS IS.I.OR.240 *compliance*).

Correção #2: Avaliação Cruzada de Riscos Financeiros

O mesmo cenário C revelou que riscos financeiros/admin, tradicionalmente fora do âmbito SMS, podem ter impactos *safety* indiretos.

Problema Identificado: Modelo original assume que se ativo não é "operacionalmente crítico" (ex: ERP financeiro), não requer avaliação SMS. Isto ignora impactos indiretos (moral, fornecedores).

Solução Proposta:

- Mesmo quando risco é claramente ISMS-*only*, realizar *quick safety check*: "Existe algum impacto indireto concebível em *safety*?".
- Se sim → escalar para *Safety Manager* (avaliação leve, não completa).
- Se não → prosseguir apenas com ISMS.

Impacto: Aumenta abrangência sem sobrecarregar SMS com avaliações desnecessárias. Alinha-se com princípio de precaução da aviação.

8.5.3. Sugestões dos Participantes

Duas sugestões principais emergiram da discussão:

Sugestão #1: Avaliação Preventiva Sistemática (P2, P7). "Mesmo quando um ativo claramente não tem impacto *safety* direto, deveria haver pelo menos um *check* preventivo mínimo pelo SMS, para evitar *blind spots."*

Alinha-se com cultura *safety* proativa da aviação. Integrada na Correção #2 acima.

Sugestão #2: Módulo Simplificado de Rejeição (P1, P9). "Precisa existir um botão tipo *'Not Relevant'* que permita descartar rapidamente alertas da IA que são obviamente falsos positivos, mas que fique registado para auditoria."

Analistas não podem gastar tempo em análise completa de cada sugestão da IA se algumas são claramente irrelevantes. Integrada na Correção #1 acima, com adição de interface simplificada no *dashboard* que requer apenas:

- Seleção da razão de rejeição (*dropdown*)
- Comentário opcional (texto livre)
- Confirmação

Resultado: Rejeição leva <30 segundos, mantém *compliance* com IS.I.OR.240 (*record-keeping*), e alimenta *machine learning* para reduzir futuros falsos positivos.

8.5.4. Perceções sobre Aceitação Organizacional

Além das questões e sugestões formais, a observação participante permitiu captar perceções qualitativas sobre aceitação do modelo.

Indicadores Positivos de Aceitação:

1. *Engagement* Elevado

Todos os 10 participantes permaneceram atentos e participativos durante as 4 horas. Não houve dispersão ou desinteresse observado. *Safety Manager* (P2) e *Chief Pilot* (P4) fizeram anotações extensas.

2. Entusiasmo de Champions

Dois participantes destacaram-se como "*early adopters*" entusiastas: *Security Manager* (P3) fez múltiplas perguntas técnicas, propôs casos de uso adicionais, verbalizou: "Isto é exatamente o que precisamos para demonstrar valor do *Security* à operação". *Chief Pilot* (P4): Conhecido

pelo gosto por tecnologia, defendeu “Este modelo colocará a EuroAtlantic na vanguarda. Devemos avançar". CISO (P1) validou que arquitetura proposta é tecnicamente viável, comentando "Temos os dados, temos os *logs*, temos a infraestrutura base. O desafio é integrar, não construir do zero". Múltiplos participantes verbalizaram reconhecer o problema que CESAR resolve. CFO (P6) "Hoje tratamos *cyber*, *safety*, *security* como silos. Isto pode mudar". *Accountable Manager* (P5) manifestou interesse estratégico, afirmando "Vou discutir com o *Board*. Pode ser diferencial competitivo e de *compliance*".

Cautela do *Accountable Manager* (P5). Embora interessado, manifestou reservas sobre:

- Governança: "Quem decide quando há conflito entre CISO e *Safety Mgr*?"
- Controlo humano: "Até que ponto deixamos a IA decidir?"
- Responsabilidade legal: "Se IA falhar e houver incidente, quem responde perante ANAC/EASA?"

Estas reservas são legítimas e refletem maturidade de gestão. *Accountable Manager* tem responsabilidade legal final, pelo que ceticismo saudável é esperado e apropriado.

Diretor Técnico (P7) e *Project Manager* (P8) expressaram preocupação com:

- Curva de aprendizagem para utilizadores
- Esforço de gestão de mudança necessário
- Risco de resistência das equipas

Preocupações práticas válidas sobre implementação, não sobre conceito.

CFO perguntou "Qual o retorno do investimento? Como quantificamos benefício?". Resposta dada: ROI é difícil de quantificar exatamente porque valor principal é prevenção (incidentes evitados). Benefícios mensuráveis:

- Redução de carga administrativa (auditorias unificadas)
- *Compliance* assegurado (evita multas NIS2: até 2% *revenue*)
- Vantagem competitiva (diferenciação no mercado)

Safety Manager e *Accountable Manager* questionaram nível apropriado de autonomia da IA, expressando preferência por "IA assistida" sobre "IA autónoma". Resposta dada: CESAR é

deliberadamente desenhado como *decision support system*, não *autonomous decision maker*. IA recomenda, humano decide. Alinhado com (EU) AI Act Artigo 14 (*human oversight*).

Globalmente, a reação foi predominantemente positiva, com aceitação conceptual elevada, mas reservas práticas legítimas sobre implementação. O modelo foi percebido como:

- Relevante (resolve problema real)
- Alinhado regulatoriamente (satisfaz EASAPart-IS)
- Tecnicamente viável (com ressalvas)

Não houve rejeição do modelo, mas reconhecimento de que implementação exigirá maturidade organizacional, investimento, e compromisso da liderança.

8.6. Discussão Crítica dos Resultados

8.6.1. Interpretação das Descobertas

Os resultados do *workshop* confirmam a viabilidade conceptual do CESAR *Framework,* mas evidenciam claramente que validação técnica e operacional permanece como trabalho futuro necessário. O que foi efetivamente validado:

- Compreensibilidade: Participantes com *backgrounds* diversos (técnico, operacional, executivo) compreenderam o modelo e suas fases.
- Relevância: Problema que CESAR resolve foi reconhecido como real e urgente (*deadline* EASA Part-IS: outubro 2025).
- Alinhamento regulatório: Mapeamento EAS Part-IS foi validado por profissionais familiarizados com a regulação (*Safety Mgr*, CISO).
- Aceitação cultural: Não houve resistência cultural ou organizacional ao conceito de integração ISMS-SMS.
- *Feedback* construtivo: Sugestões e correções melhoraram o modelo, demonstrando *engagement* genuíno

8.6.2. Limitações da Validação Realizada

É fundamental reconhecer explicitamente as limitações desta validação:

Limitação 1: Amostra Não Representativa.

- n=10 participantes de uma única organização.
- Não permite generalização para setor aeronáutico europeu.
- EuroAtlantic é operador médio; resultados podem diferir em grandes operadores (TAP, Ibéria) ou pequenos (aviação geral).

Limitação 2: Ausência de Implementação Técnica

- *Workshop* baseou-se em apresentação conceptual.
- Cenários foram simulados, não executados por sistema real.
- Impossível avaliar performance, robustez ou escalabilidade.

Limitação 3: Viés do Investigador

- Investigadora conduziu *workshop* e recolheu dados
- Risco de influenciar participantes ou interpretar *feedback* favoravelmente
- Mitigação parcial: perguntas abertas, encorajamento de críticas

Limitação 4: Contexto Organizacional Específico

- EAA tem cultura de inovação e abertura a tecnologia (*Chief Pilot tech-savvy*)
- Resultados podem não replicar-se em organizações mais conservadoras
- Presença da gestão de topo (*Accountable Mgr*, CFO) pode ter inibido críticas.

Limitação 5: Validação de Curto Prazo

- *Workshop* único de 4 horas
- Não captura evolução de perceções ao longo do tempo
- Não permite avaliar sustentabilidade do interesse

Limitação 6: Ausência de Comparação

- Não foi apresentado modelo alternativo para comparação
- Participantes não avaliaram CESAR vs. outras abordagens
- Impossível afirmar se CESAR é superior a alternativas

8.7. Contributos da Validação para o Modelo CESAR

Apesar das limitações, a validação gerou contributos concretos:

Contributo #1: Refinamento Conceptual. As 2 correções identificadas (*fast-track rejection*, avaliação cruzada preventiva) melhoraram substancialmente a aplicabilidade prática do modelo, endereçando eficiência operacional sem comprometer rigor.

Contributo #2: Priorização de Funcionalidades. *Workshop* permitiu identificar funcionalidades mais valorizadas: *Dashboards* executivos (P5, P6): alta prioridade, Explicabilidade de decisões IA (P1, P2, P5): crítica, Integração com IQSMS/FDM (P2): essencial, Módulo de rejeição rápida (P1, P9): muito desejável.

Contributo #3: Identificação de Barreiras Práticas. Desafio técnico: Integração com sistemas legados não-API, Desafio organizacional: Definição clara de *ownership* do CESAR, Desafio cultural: Resistência à "caixa negra" da IA, Desafio financeiro: ROI incerto para investimento significativo.

Contributo #4: Validação de Mapeamento Regulatório. *Safety Manager* (P2) e CISO (P1), ambos familiarizados com Part-IS, validaram que o mapeamento entre fases CESAR e requisitos IS.I.OR é correcto e completo. Este é contributo importante dado expertise dos validadores.

Contributo #5: Estabelecimento de Requisitos para Implementação. *Workshop* clarificou pré-requisitos técnicos para futura implementação: Inventário de ativos completo e atualizado (IS.I.OR.205), *Logs* estruturados e acessíveis (SIEM, FDM, IQSMS), Infraestrutura computacional adequada (servidores, *storage*), Competências internas ou parceria externa para desenvolvimento IA, *Governance framework* definindo RACI (*Responsible, Accountable, Consulted, Informed*).

8.8. Comparação com Validações na Literatura

A Revisão Sistemática (Cap. 3) identificou que dos 40 estudos analisados: 30% são estudos de caso (maioritariamente simulados), 17,5% são propostas de *frameworks*, Apenas 15% reportam estudos experimentais. Apenas 6 estudos (15%) realizaram validação em ambiente operacional real. A validação do CESAR posiciona-se como:

- Superior a 17,5% dos estudos (*frameworks* puramente teóricos sem validação),
- Comparável a 30% dos estudos (validação via *stakeholders*/caso simulado),
- Inferior a 15% dos estudos (validação experimental/operacional).

Portanto, embora limitada, a validação realizada está alinhada com práticas correntes da área, que se caracteriza por predominância de trabalho conceptual sobre empírico.

Frameworks comparáveis identificados na RSL:

- Study #12 (*Federated Learning* para-ATM): *Workshop* com 8 *controllers*,
- Study #23 (*Risk correlation framework*): *Focus group* com 12 profissionais,
- Study #31 (*AI-based threat detection*): Validação conceptual via *survey*.

O CESAR diferencia-se por:

- Maior diversidade de participantes (6 áreas vs 1-2 áreas típicas),
- Demonstração de cenários práticos (maioria usa apenas apresentação),
- Presença de decisores de topo (AM, CFO) que confere peso estratégico.

8.9. Recomendações para Validação Futura

Para avançar de validação conceptual para validação empírica robusta, recomendam-se:

Fase 1 - Validação Técnica (6-12 meses). Desenvolvimento de protótipo funcional (MVP - *Minimum Viable Product*) com: Testes de algoritmos ML com dados históricos reais da EAA, Medição de *accuracy*, *precision*, *recall*, F1-*score*, *Benchmark* contra *baseline* (processo manual atual).

Fase 2 - Piloto Controlado (6-12 meses) com: Implementação em ambiente não-produtivo (*sandbox*). Teste com *subset* de dados reais, mas sem impacto operacional, Validação de integrações técnicas (IQSMS, FDM, SIEM), Refinamento baseado em *feedback* de utilizadores.

Fase 3 - Implementação Operacional Faseada (12-18 meses) com: *Roll-out* progressivo por áreas (começar por ISMS, depois SMS), Monitorização contínua de KPIs, Comparação pré/pós implementação (incidentes, conformidade, eficiência), Ajustes iterativos.

Fase 4 - Validação Regulatória (6 meses) com: Auditoria por autoridade competente (ANAC), Verificação de conformidade com EASA Part-IS, Certificação ou *approval* formal.

Fase 5 - Generalização (opcional) com: Replicação em outras organizações aeronáuticas, Validação de transferibilidade do modelo, Publicação de resultados empíricos.

8.10. Síntese do Capítulo

Este capítulo apresentou a validação conceptual do CESAR *Framework* através de *workshop* com 10 profissionais da EuroAtlantic Airways, constituindo etapa crítica na metodologia *Design Science Research*. A validação cumpre seu propósito dentro do âmbito de uma dissertação de mestrado, estabelecendo bases para publicação de *framework* conceptual, fundamentação para projeto de implementação técnica, identificação de requisitos para investigação futura.

O CESAR *Framework*, refinado através desta validação, está agora suficientemente maduro para publicação académica como modelo conceptual, apresentação a decisores para avaliação de investimento, base para desenvolvimento técnico em projeto futuro.

O próximo capítulo (Capítulo 9) apresenta as conclusões gerais da dissertação, sintetiza contributos científicos e práticos, e estabelece agenda de investigação futura centrada na implementação técnica e validação empírica robusta do modelo.

9. CONCLUSÕES E TRABALHO FUTURO

9.1. Síntese da Investigação

Esta dissertação abordou um desafio emergente na aviação civil europeia de como integrar efetivamente a gestão de cibersegurança (ISMS) com a gestão de segurança operacional (SMS), conforme exigido pelo EASA Part-IS até outubro de 2025. O problema não é meramente técnico, mas representa uma questão conceptual sobre como dois domínios historicamente distintos, com culturas, linguagens e práticas próprias, podem convergir num sistema unificado sem perder suas especificidades.

A Revisão Sistemática da Literatura confirmou esta lacuna de forma quantitativa: apenas 5% dos 40 estudos analisados abordam o EASA Part-IS, e apenas 10% propõem integração explícita entre ISMS e SMS. Mais revelador foi descobrir que sistemas de IA que funcionam com 87,3% de *accuracy* em aplicações isoladas degradam para 74,8% quando tentam endereçar requisitos integrados. Esta degradação de 12,5 pontos percentuais não é acidental, evidencia que as abordagens atuais não foram concebidas para satisfazer simultaneamente múltiplas dimensões regulatórias.

Em resposta, desenvolveu-se o CESAR *Framework*, um modelo conceptual que operacionaliza os requisitos do EASA Part-IS através de um ciclo de sete fases que integra nativamente ISMS e SMS, incorpora Inteligência Artificial Explicável para correlação automática de riscos, e mapeia explicitamente cada requisito regulatório (IS.I.OR.200-260). O modelo distingue-se por não tratar integração como exercício de coordenação entre sistemas paralelos, mas como processo unificado com governança partilhada e correlação sistemática de riscos *cross-domain*.

A validação conceptual, realizada através de *workshop* com dez profissionais da EuroAtlantic Airways, revelou aceitação organizacional positiva. Os participantes compreenderam o *framework* e perceberam-no como resposta relevante aos seus desafios práticos. O *workshop* gerou ainda refinamentos concretos, dois mecanismos que aumentam a eficiência operacional sem comprometer rigor regulatório, demonstrando que o processo de validação foi verdadeiramente colaborativo e não meramente confirmativo.

Foi demonstrada a viabilidade conceptual do CESAR. Profissionais experientes da aviação, quando apresentados ao modelo, compreenderam sua lógica, reconheceram sua relevância, e não identificaram barreiras conceptuais insuperáveis. Este não é resultado trivial – muitos

frameworks académicos falham precisamente neste teste de realidade. O CESAR passou. Foi validado que o mapeamento regulatório está correto. O *Safety Manager* e o CISO da EuroAtlantic Airways, ambos responsáveis diretos pela implementação do Part-IS, confirmaram que o ciclo proposto endereça todos os requisitos mandatórios. Esta validação por especialistas do domínio confere robustez ao modelo. Foram identificados refinamentos práticos que melhoraram o *framework*. O mecanismo de rejeição rápida de falsos positivos e a avaliação cruzada preventiva emergiram da discussão com *stakeholders*, demonstrando que a validação gerou contributos reais, não apenas confirmação de pressupostos. Contudo, permanece por validar a eficácia técnica e operacional.

9.2. Resposta às Questões de Pesquisa

As cinco questões que orientaram a pesquisa da literatura construíram progressivamente a fundamentação necessária para o CESAR *Framework*.

A primeira questão explorou o panorama de ameaças cibernéticas na aviação. *Ransomware* emerge como ameaça predominante (57,5% dos estudos), refletindo incidentes reais de alto impacto como os ataques à TAP Air Portugal e ao Aeroporto de Kuala Lumpur. Ataques a infraestrutura crítica (45% dos estudos) e engenharia social (30%) completam o quadro, evidenciando que tanto vulnerabilidades técnicas quanto humanas colocam o setor em risco. Esta diversidade fundamenta a necessidade de sistemas inteligentes capazes de processar volumes massivos de dados e identificar padrões que humanos dificilmente reconheceriam sozinhos.

A segunda questão mapeou o enquadramento regulatório europeu, identificando quatro instrumentos principais: EASA Part-IS (específico para aviação), NIS2 (infraestruturas críticas), (EU) AI Act (sistemas de IA de alto risco) e ISO 27001 (*framework* técnico). Embora complementares, estes regulamentos criam complexidade significativa de *compliance*. Organizações devem satisfazê-los simultaneamente, e nenhum fornece orientação operacional detalhada sobre como fazê-lo.

A terceira questão investigou os desafios práticos de implementação. Integração técnica é o obstáculo mais prevalente (72,5% dos estudos), mas não se trata apenas de conectar sistemas. *Safety Management Systems* são estruturas maduras, consolidadas ao longo de décadas, com culturas organizacionais bem estabelecidas. Integrá-los com *Information Security Management Systems* exige reconciliar culturas distintas, criar linguagem comum, e redesenhar *workflows*

consolidados. A escassez de competências híbridas (35% dos estudos) sublinha que perfis que dominem simultaneamente aviação, cibersegurança e IA são raros.

A quarta questão examinou aplicações de IA na aviação. *Supervised Machine Learning* é a técnica mais utilizada (72,5%), mas o achado crítico é que 58% dos estudos que usam ML não abordam conformidade regulatória. Este *disconnect* fundamental, sistemas otimizados para performance técnica, mas não concebidos para satisfazer requisitos regulatórios, explica a degradação de *performance* observada em sistemas integrados.

A quinta questão, retirou lições da literatura que levou a que se definissem requisitos para que constitui, como estruturar um processo verdadeiramente integrado. A resposta materializa-se no CESAR *Framework*, fundamentado em três princípios: integração nativa (não paralela), IA explicável como capacitador essencial (não opcional), e *compliance by design* (não validação posterior).

A contribuição desta dissertação situa-se no domínio do *design* conceptual rigoroso e validação inicial, estabelecendo fundações sólidas sobre as quais investigação futura possa construir. Este é papel legítimo de investigação de mestrado: não resolver completamente problema complexo, mas avançar conhecimento de forma significativa.

9.3. Limitações e Trabalhos Futuros

O trabalho desenvolvido abre três eixos principais de investigação futura, organizados por prioridade e complexidade. O primeiro e mais prioritário é a validação técnica e empírica. Isto envolveria desenvolver protótipo funcional do CESAR com implementação real dos algoritmos de IA, integração efetiva com sistemas operacionais (IQSMS, FDM, SIEM), e testes rigorosos com dados reais. Estudos de caso longitudinais em múltiplas organizações ao longo de 18-24 meses mediriam impacto real em redução de incidentes, melhoria de *compliance*, e carga de trabalho. Esta investigação seria naturalmente objeto de doutoramento, gerando publicações em *journals* de topo como *Safety Science* ou *Computers & Security*. Validação específica da *performance* dos algoritmos seria complementar essencial. Testar rigorosamente técnicas como *Random Forest, XGBoost e Bayesian Networks* em *datasets* realistas de aviação estabeleceria *benchmarks* confiáveis e validaria pressupostos sobre *trade-off* entre explicabilidade e *accuracy*. Questões fundamentais incluem se este *trade-off* é tão severo quanto literatura sugere, ou se técnicas modernas de XAI mitigam o problema significativamente.

O segundo eixo centra-se em extensões do modelo. Uma direção natural seria expandir a integração para incluir *Physical Security Management*, desenvolvendo convergência tripla (*Information Security + Safety + Physical Security)* que endereçasse simultaneamente EASA Part-IS, *Annex* 19 e *Annex* 17. Outra extensão valiosa seria adaptar o CESAR a diferentes tipologias organizacionais – aeroportos enfrentam desafios distintos de companhias aéreas, organizações ATM/ANS têm requisitos críticos de latência, e aviação geral opera com recursos muito mais limitados. Olhando para o futuro mais distante, adaptar o CESAR para aeronaves autónomas seria investigação visionária, mas cada vez mais relevante. *Drones* comerciais, *urban air mobility* e eventualmente aeronaves pilotadas por IA representam contexto onde integração entre cibersegurança, *safety* e IA será ainda mais crítica, e onde novos riscos emergirão quando a própria operação depender de sistemas que podem ser alvos de ataques.

O terceiro eixo explora transferibilidade para outros setores críticos regulados pela NIS2. Energia, saúde, transportes ferroviários e marítimos, e telecomunicações enfrentam desafios conceptualmente similares. Investigação comparativa exploraria se princípios do CESAR são verdadeiramente generalizáveis ou idiossincráticos à aviação, contribuindo para compreensão mais ampla sobre integração de domínios de segurança em infraestruturas críticas.

9.4. Implicações Práticas e Políticas

Para organizações aeronáuticas enfrentando o *deadline* de outubro de 2025, o CESAR oferece *roadmap* conceptual que reduz incerteza. Mesmo sem implementação técnica imediata, seus princípios podem orientar decisões: estruturar *governance* facilitando colaboração entre CISO e *Safety Manager* desde início, investir em qualidade de dados como pré-requisito, desenhar processos com integração em mente desde conceção, e considerar explicabilidade como requisito não-negociável ao planear utilizar IA. Para autoridades regulatórias, particularmente EASA, a investigação evidencia necessidade de *guidance* mais prescritivo. O EASA Part-IS estabelece "o quê", mas deixa ambiguidade significativa sobre "como". Desenvolvimento de *Acceptable Means of Compliance* mais detalhados, incluindo exemplos concretos de processos integrados e clarificação sobre utilização aceitável de IA, reduziria fragmentação de implementações. Para fornecedores de tecnologia, CESAR representa oportunidade de mercado. Existe *gap* entre exigência regulatória e capacidade atual de organizações, criando demanda por soluções que operacionalizam integração ISMS-SMS. Desenvolvimento de plataformas comerciais baseadas nestes princípios poderia capturar valor substancial. Para instituições académicas, a investigação evidencia necessidade urgente de formar competências

híbridas. Currículos devem evoluir para formar profissionais que transcendam silos tradicionais, combinando engenharia aeronáutica com *computer science* e *cybersecurity*.

9.5. Reflexão Final

Esta dissertação iniciou-se com a observação de um paradoxo: a aviação civil é simultaneamente um dos setores mais seguros e mais vulneráveis do mundo. Mais seguro porque décadas de aprendizagem estabeleceram cultura de *safety* sem paralelo. Mais vulnerável porque esta segurança depende crescentemente de sistemas digitais que abrem superfícies de ataque inexploradas.

O CESAR *Framework* emerge como resposta conceptual, propondo que segurança cibernética e segurança operacional não devem ser geridas como domínios paralelos, mas como dimensões integradas de sistema unificado. A validação conceptual demonstrou que esta visão é compreensível, desejável e viável na perspetiva de quem enfrenta diariamente estes desafios. Contudo, entre conceito e realidade operacional existe *gap* significativo que apenas implementação técnica rigorosa e validação empírica poderão preencher. Esta dissertação estabelece as fundações. A jornada de transformar CESAR *framework* conceptual em sistema operacional testado é trabalho para investigação futura, trabalho necessário, complexo, mas fundamentado em bases sólidas.

Se esta investigação contribuir para que pelo menos algumas organizações aeronáuticas naveguem com maior clareza a transição mandatória para gestão integrada de risco, terá cumprido seu propósito. Se inspirar investigação subsequente que complete o caminho de conceito a implementação validada, terá excedido expectativas. E se demonstrar que integração rigorosa entre domínios tradicionalmente separados não é apenas exigência regulatória, mas oportunidade de fortalecer simultaneamente múltiplas dimensões de segurança, terá alcançado sua ambição mais profunda. A aviação sempre progrediu através de ciclos de aprendizagem, tragédias que catalisaram mudanças regulatórias, incidentes que revelaram vulnerabilidades inesperadas, inovações que transformaram possibilidades. Este trabalho insere-se nesta tradição, procurando antecipar desafios emergentes antes que se manifestem em consequências graves. É exercício de precaução informada, fundamentada em evidência empírica e validada junto de quem conhece profundamente o setor.

O futuro da aviação será inevitavelmente mais digital, mais interconectado, mais dependente de Inteligência Artificial. Garantir que esta transformação ocorra sem comprometer a segurança

que caracteriza o setor exige *frameworks* conceptuais robustos, validação rigorosa, e colaboração estreita entre investigação académica, prática industrial e política regulatória. Esta dissertação procura contribuir, de forma modesta, mas rigorosa, para este esforço coletivo.

REFERÊNCIAS BIBLIOGRÁFICAS

Abozaid, F., & Baydoun, A. (2024). Resilience of Aviation Cyber-Physical Systems to Malicious Attacks. *2024 International Conference on Computer and Applications, ICCA 2024*. https://doi.org/10.1109/ICCA62237.2024.10927823

Aghazadeh Ardebili, A., Lezzi, M., & Pourmadadkar, M. (2024). Risk Assessment for Cyber Resilience of Critical Infrastructures: Methods, Governance, and Standards. In *Applied Sciences (Switzerland)* (Vol. 14, Issue 24). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/app142411807

Ahmed, W. (2025). Artificial Intelligence in Aviation: A Review of Machine Learning and Deep Learning Applications for Enhanced Safety and Security. *Premier Journal of Artificial Intelligence*. https://doi.org/10.70389/PJAI.100013

Ali, M., Hu, Y. F., & Li, J. P. (2025). Federated Learning Augmented Cybersecurity for SDN-Based Aeronautical Communication Network. *Electronics (Switzerland)*, *14*(8). https://doi.org/10.3390/electronics14081535

Annex 17. (2022). *Annex 17 — Security: Safeguarding International Civil Aviation against Acts of Unlawful Interference. International Standards and Recommended Practices* (12th Edition). International Civil Aviation Organization.

Annex 17. (2025). *ICAO Annex 17 – Security: Safeguarding International Civil Aviation Against Acts of Unlawful Interference*.

Annex 19. (2013). *ICAO Annex 19 — Safety Management. International Standards and Recommended Practices* (1st Edition). International Civil Aviation Organization.

ARINC 618. (2011). *ARINC Characteristic 618: Air/Ground Character-Oriented Protocol Specification. ARINC.*

Bozena Konecka-Szydelko, M. (2021). Aviation safety in the European transport policy. *NTAD 2021 - 16th International Scientific Conference on New Trends in Aviation Development 2021, Proceedings*, 102–106. https://doi.org/10.1109/NTAD54074.2021.9746516

Çevik, N., & Akleylek, S. (2024). SoK of Machine Learning and Deep Learning Based Anomaly Detection Methods for Automatic Dependent Surveillance- Broadcast. *IEEE Access*, *12*, 35643–35662. https://doi.org/10.1109/ACCESS.2024.3369181

Delgado-Aguilera, R. J., Vicent, O. P., Xiaojie, Y., Maria, Z. S., Francisco, P. M., & Cesar, G. A. (2024). Establishing Rigorous Certification Standards: A Systematic Methodology for AI Safety-Critical Systems in Military Aviation. *IEEE Access*, *12*, 161982–161994. https://doi.org/10.1109/ACCESS.2024.3487591

Demir, G., Moslem, S., & Duleba, S. (2024). Artificial Intelligence in Aviation Safety: Systematic Review and Biometric Analysis. In *International Journal of Computational Intelligence Systems* (Vol. 17, Issue 1). Springer Science and Business Media B.V. https://doi.org/10.1007/s44196-024-00671-w

Dong, T., Yang, Q., Ebadi, N., Luo, X. R., & Rad, P. (2021). Identifying Incident Causal Factors to Improve Aviation Transportation Safety: Proposing a Deep Learning Approach. *Journal of Advanced Transportation*, *2021*. https://doi.org/10.1155/2021/5540046

EASA. (2024). *EASA Part IS - Explanatory Note to ED Decisions 2023/008/R, 2023/009/R and 2023/010/R*. https://www.easa.europa.eu/en/downloads/138236/en

EASA AI. (2025). *ARTIFICIAL INTELLIGENCE ROADMAP 2.0 Human-centric approach to AI in aviation Human-centric approach to AI in aviation*. https://www.easa.europa.eu/en/downloads/137919/en

EASA Cyber. (2025). *Cybersecurity - Main EASA activities*. https://www.easa.europa.eu/en/domains/cyber-security/main-easa-activities

Easy Rules. (2025). *Easy Access Rules for Information Security (Regulations (EU) 2023/203 and 2022/1645)*. Https://Www.Easa.Europa.Eu/En/Document-Library/Easy-Access-Rules/Easy-Access-Rules-Information-Security-Regulations-Eu-2023203.

Ekstedt, M., Afzal, Z., Mukherjee, P., Hacks, S., & Lagerström, R. (2023). Yet another cybersecurity risk assessment framework. *International Journal of Information Security*, *22*(6), 1713–1729. https://doi.org/10.1007/s10207-023-00713-y

Eleimat, M., & Őszi, A. (2025). Cybersecurity in Aviation: Exploring the Significance, Applications, and Challenges of Cybersecurity in the Aviation Sector. *Periodica Polytechnica Transportation Engineering*, *53*(2), 169–183. https://doi.org/10.3311/PPtr.37153

EU IA. (2023). *Artificial Intelligence Roadmap 2.0: Learning assurance and trustworthiness in aviation AI systems*. https://www.easa.europa.eu/en/document-library/general-publications/artificial-intelligence-roadmap-20

Faruk, I., Fatin, ✉, Plabon, W., Saha, U. S., & Hossain, M. D. (2025). *AI-Driven Project Risk Management: Leveraging Artificial Intelligence to Predict, Mitigate, and Manage Project Risks in Critical Infrastructure and National Security Projects*. https://doi.org/10.32996/jcsts.2025.7.6.16

FAYE, S., ABDULRAHMAN, J., TALB, R. A., & MARTIN, R. J. (2024). Cybersecurity in Aviation: A Case-Based Approach to Preparedness. *International Journal of Information Security and Cybercrime*, *13*(2), 33–45. https://doi.org/10.19107/ijisc.2024.02.03

Filinovych, V., & Hu, Z. (2021). Aviation and the Cybersecurity Threats. *Proceedings of the International Conference on Business, Accounting, Management, Banking, Economic Security and Legal Regulation Research (BAMBEL 2021)*, *188*. https://doi.org/10.2991/aebmr.k.210826.021

Florido-Benítez, L. (2024). The types of hackers and cyberattacks in the aviation industry. In *Journal of Transportation Security* (Vol. 17, Issue 1). Springer. https://doi.org/10.1007/s12198-024-00281-9

Garcia, A. B. (2022). *Machine Learning and Artificial Intelligence Methods for Machine Learning and Artificial Intelligence Methods for Cybersecurity Data within the Aviation Ecosystem Cybersecurity Data within the Aviation Ecosystem Scholarly Commons Citation Scholarly Commons Citation*. https://commons.erau.edu/edt/700/

Garcia, A. B., Babiceanu, R. F., & Seker, R. (2021). Artificial intelligence and machine learning approaches for aviation cybersecurity: An overview. *Integrated Communications, Navigation and Surveillance Conference, ICNS*, *2021-April*. https://doi.org/10.1109/ICNS52807.2021.9441594

Guskova, N., Chopart, M., & Kraus, J. (2025). EASA Part IS in U-Space Operations: Is System-Theoretic Process Analysis for Security Sufficient to Meet Information Security Risk Assessment Requirements? *Procedia Computer Science*, *253*, 2448–2457. https://doi.org/10.1016/j.procs.2025.01.305

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, *28*(1), 75–105. https://doi.org/10.2307/25148625

ICAO b. (2016). *International Civil Aviation Organization. (2016). Annex 19 to the Convention on International Civil Aviation – Safety Management (2nd ed.)*. https://www.icao.int/safety/SafetyManagement/Pages/Annex19.aspx

ISO/IEC 27000. (2018). *ISO/IEC 27000:2018 - Information technology – Security techniques – Information security management systems – Overview and vocabulary*. ISO.

ISO/IEC 27001. (2022). *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements*.

ISO/IEC 27005. (2022). *ISO/IEC 27005:2022 — Information security, cybersecurity and privacy protection — Guidance on information security risk management*.

Jiang, Y., Tran, T. H., & Williams, L. (2023). Machine learning and mixed reality for smart aviation: Applications and challenges. *Journal of Air Transport Management*, *111*. https://doi.org/10.1016/j.jairtraman.2023.102437

Kabashkin, I., Misnevs, B., & Zervina, O. (2023). Artificial Intelligence in Aviation: New Professionals for New Technologies. *Applied Sciences (Switzerland)*, *13*(21). https://doi.org/10.3390/app132111660

Kirwan, B. (2024). The Impact of Artificial Intelligence on Future Aviation Safety Culture. *Future Transportation*, *4*(2), 349–379. https://doi.org/10.3390/futuretransp4020018

Kitchenham, B., & Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering* (Issue EBSE-2007-01).

Kondala, M., & Patibandla, R. (2024). Predictive Maintenance in Aviation using Artificial Intelligence. In *Journal of Artificial Intelligence General Science* (Vol. 1). JAIGS. https://ojs.boulibrary.com/index.php/JAIGS

Kotadiya, A. (2024). *Enhancing Aviation Cybersecurity Through AI Integration*. https://doi.org/10.21276/IERJ24004829981448

Lakhani, Prof. D. (2025). "AI-Driven Cybersecurity Risks and Defense in Avionics Systems." *International Journal Of Scientific Research In Engineering And Management*, *09*(05), 1–9. https://doi.org/10.55041/IJSREM47827

Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2018, November 13). Implementing cyber-security measures in airports to improve cyber-resilience. *2018 Global Internet of Things Summit, GIoTS 2018*. https://doi.org/10.1109/GIOTS.2018.8534523

Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2019). Smart airport cybersecurity: Threat mitigation and cyber resilience controls. *Sensors (Switzerland)*, *19*(1). https://doi.org/10.3390/s19010019

Mizrak, F., & Reyhan Akkartal, G. (2024). Prioritizing cybersecurity initiatives in aviation: A dematel-QSFS methodology. *Heliyon*, *10*(16). https://doi.org/10.1016/j.heliyon.2024.e35487

Monev, V. (2024). Aviation Safety within an Information Security Risk Management Process (EASA Part-IS). *2024 38th International Conference on Information Technologies, InfoTech 2024 - Proceedings*. https://doi.org/10.1109/InfoTech63258.2024.10701382

New, M. D., & Wallace, R. J. (2025). Classifying Aviation Safety Reports: Using Supervised Natural Language Processing (NLP) in an Applied Context. *Safety*, *11*(1). https://doi.org/10.3390/safety11010007

Niraula, M. (2022). Cybersecurity and Interoperability of Aviation Safety Service Ecosystem. *Integrated Communications, Navigation and Surveillance Conference, ICNS*, *2022-April*. https://doi.org/10.1109/ICNS54818.2022.9771482

Nobles, C., Burrell, D., & Waller, T. (2022). The Need for a Global Aviation Cybersecurity Defense Policy. *Land Forces Academy Review*, *27*(1), 19–26. https://doi.org/10.2478/raft-2022-0003

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, *372*, n71. https://doi.org/10.1136/bmj.n71

PART IS. (2023). *Regulamento de Execução (UE) 2023/203 - Consolidada*. https://eur-lex.europa.eu/eli/reg_impl/2023/203/2025-05-01

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Reason, J. (1997). *Managing the Risks of Organizational Accidents*. Ashgate. https://doi.org/10.4324/9781315543543

Sai, S., Sai, R., & Chamola, V. (2025). Generative AI for Industry 5.0: Analyzing the Impact of ChatGPT, DALLE, and Other Models. *IEEE Open Journal of the Communications Society*, *6*, 3056–3066. https://doi.org/10.1109/OJCOMS.2024.3400161

Sheikhi, S., Eceiza, M., Arellano, C., López, O., Kelnberger, S., Lindner, R., Partanen, J., & Lovén, L. (2025). Bridging Theory and Practice: Addressing Current Cybersecurity Gaps in Industry 5.0. *IEEE Access*, *13*, 92891–92905. https://doi.org/10.1109/ACCESS.2025.3569130

Stastny, P., & Stoica, A.-M. (2022). Protecting aviation safety against cybersecurity threats. *IOP Conference Series: Materials Science and Engineering*, *1226*(1), 012025. https://doi.org/10.1088/1757-899x/1226/1/012025

Taleqani, A. R., Nygard, K. E., Bridgelall, R., & Hough, J. (2018). Machine Learning Approach to Cyber Security in Aviation. *IEEE International Conference on Electro Information Technology*, *2018-May*, 147–152. https://doi.org/10.1109/EIT.2018.8500165

UE 2017/373. (2017). *Regulamento de Execução (UE) 2017/373 da Comissão, de 1 de março de 2017*. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32017R0373

UE 2018/1139. (2018). *Regras da aviação civil e a Agência da União Europeia para a Segurança da Aviação*. https://eur-lex.europa.eu/PT/legal-content/summary/civil-aviation-rules-and-the-european-union-aviation-safety-agency.html

UE 2019/1583. (2019). *Regulamento de Execução (UE) 2019/1583 da Comissão, de 25 de setembro de 2019,*. https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX:32019R1583

UE 2022/1645. (2022). *Commission Delegated Regulation (EU) 2022/1645 of 14 July 2022 laying down rules for the application of Regulation (EU) 2018/1139 as regards requirements for the management of information security risks with a potential impact on aviation safety for organizations covered by certain Commission Regulations*.

UE 2022/2555. (2022). *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148*.

UE 2023/203. (2023). *Commission Implementing Regulation (EU) 2023/203 of 27 October 2022 laying down rules for the application of Regulation (EU) 2018/1139 as regards requirements for the management of information security risks with a potential impact on aviation safety*.

UE 2024/1689. (2024). *Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho relativo a um quadro harmonizado para a Inteligência Artificial (AI Act)*. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32024R1689

Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., Andonovic, I., & Bellekens, X. (2022). Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends. In *Information (Switzerland)* (Vol. 13, Issue 3). MDPI. https://doi.org/10.3390/info13030146

Werthwein, M., & Annighoefer, B. (2024). Model-Based Avionics Cybersecurity Framework for Identification of Risk and Evaluation. *AIAA/IEEE Digital Avionics Systems Conference - Proceedings*. https://doi.org/10.1109/DASC62030.2024.10749689

Xie, Y., Gardi, A., & Sabatini, R. (2023). Cybersecurity Risks and Threats in Avionics and Autonomous Systems. *2023 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, 814–819. https://doi.org/10.1109/DASC/PiCom/CBDCom/Cy59711.2023.10361328

Zhou, D., Zhuang, X., Zuo, H., Wang, H., & Yan, H. (2020). Deep Learning-Based Approach for Civil Aircraft Hazard Identification and Prediction. *IEEE Access*, *8*, 103665–103683. https://doi.org/10.1109/ACCESS.2020.2997371