UFSM

InterAção

ISSN 2357-7975
ACESSO ABERTO

IA., Santa Maria, v. 17, n. 2, e95382, p. 1-26, jun. 2026 • https://dx.doi.org/10.5902/2357797595382
Submissão: 11/02/2026 • Aprovação: 15/05/2026 • Publicação: 1º/06/2026

Artigos Dossiê

Do Ato de Securitização à capacidade organizacional: proposta de Framework Estratégico e Modelo de Maturidade para a Gestão de Riscos Cibernéticos em Cadeias de Suprimentos Aeroespaciais (C-SCRM)

From the Act of Securitization to organizational capability: Strategic Framework and Maturity Model Proposal for Cyber Risk Management in Aerospace Supply Chains (C-SCRM)

Andre Luiz Anjos de Figueiredo[I]
Pedro Arthur Linhares Lima[II]

[I]Universidade Federal Rural do Rio de Janeiro, Seropédica, RJ, Brasil
[II]Universidade da Força Aérea, Rio de Janeiro, RJ, Brasil

Resumo

Este artigo examina a gestão de riscos cibernéticos em cadeias de suprimentos aeroespaciais sob a perspectiva da securitização, sustentando que a digitalização converteu a base industrial em infraestrutura crítica de soberania nacional. A partir da integração entre a Teoria da Securitização e a Teoria do Poder Aeroespacial, propõe-se o *Securitization and Aerospace Power Framework for Cyber Supply Chain Risk Management* (SAPF-CSCRM), fundamentado nos referenciais do National Institute of Standards and Technology (NIST, 2022) e no modelo *Cybersecurity Capability Maturity Model* do Department of Energy (DOE, 2022). No interior dessa arquitetura, o *Aerospace Cyber Supply Chain Risk Management Maturity Model* (AMM-CSCRM) opera como mecanismo de governança por maturidade, articulando tipologia de riscos, controles normativos e níveis de capacidade organizacional. A validação empírica, por meio do estudo de caso do Jet Propulsion Laboratory (NASA/JPL), demonstra que a ausência de controles básicos de gestão de ativos compromete a maturidade organizacional e invalida investimentos em segurança avançada. Conclui-se que a soberania digital depende de governança estruturada e maturidade verificável em C-SCRM.

Palavras-chave: Securitização; Poder aeroespacial; *Cyber Supply Chain Risk Management*; Modelo de maturidade; NIST

Abstract

This article examines cybersecurity risk management in aerospace *supply chains* from a securitization perspective, arguing that digitalization has transformed the industrial base into critical infrastructure for national sovereignty. Drawing on the integration of Securitization Theory and Aerospace Power Theory, the *Securitization and Aerospace Power Framework for Cyber Supply Chain Risk Management* (SAPF-CSCRM) is proposed, grounded in the National Institute of Standards and Technology (NIST, 2022) *framework* and the *Cybersecurity Capability Maturity Model* (C2M2) by the Department of Energy (DOE, 2022). Within this architecture, the *Aerospace Cyber Supply Chain Risk Management Maturity Model* (AMM-CSCRM) functions as a maturity governance mechanism, articulating risk typologies, normative controls, and organizational capability levels. Empirical validation through the Jet Propulsion Laboratory (NASA/JPL) case study demonstrates that the absence of basic asset management controls undermines organizational maturity and nullifies investments in advanced security. The study concludes that digital sovereignty depends on structured governance and verifiable maturity in C-SCRM.

Keywords: Securitization; Aerospace power; *Cyber Supply Chain Risk Management*; Maturity model; NIST

INTRODUÇÃO

O avanço da automação e o progressivo distanciamento das forças armadas do campo de batalha redefiniram os vetores do conflito contemporâneo. Nesse cenário, a cibersegurança tornou-se componente estrutural da defesa nacional, com ameaças direcionadas sistematicamente às infraestruturas críticas dos setores público e privado (BRASIL, 2023; PINTO; GRASSI, 2020).

Para fins deste artigo, adota-se o conceito estabelecido pela Estratégia Nacional de Cibersegurança (E-Ciber): cibersegurança é o conjunto de ferramentas, diretrizes, melhores práticas e tecnologias empregadas para proteger o ciberespaço e os ciberativos organizacionais (BRASIL, 2025). O ciberespaço compreende o ambiente virtual onde informações digitais transitam, são processadas ou armazenadas (BRASIL, 2023).

A interdependência global e a digitalização converteram a cadeia de suprimentos em vetor de ameaça existencial, elevando a gestão de riscos de questão técnica a dimensão da defesa nacional. A cadeia de suprimentos aeroespacial, com mais de 25.000 fornecedores por aeronave, amplifica essa exposição: o crescimento de ataques

de *ransomware* evidencia o risco concreto de paralisação produtiva (AEROSPACE INDUSTRIES ASSOCIATION, 2023). Com a economia espacial estimada em 630 bilhões de dólares, o impacto de incidentes cibernéticos nesse setor extrapola a dimensão econômica e atinge a soberania operacional (UNITED STATES, 2025).

A securitização desse contexto redefine a integridade de *software* e a proteção da propriedade intelectual como pilares da vantagem militar. Governos adversários podem coagir fornecedores a inserir vulnerabilidades ou *backdoors* em sistemas militares, comprometendo-os desde a origem (PAULUS, 2025). O incidente da Viasat durante a invasão da Ucrânia demonstrou que ataques à cadeia de suprimentos podem comprometer diretamente o comando e controle militar, razão pela qual a cadeia de *software* é identificada como o "Calcanhar de Aquiles" das forças armadas modernas (PAULUS, 2025). A dissolução da fronteira entre alvos civis e militares torna a infraestrutura aeroespacial essencialmente dual, exigindo coordenação que transcende os mecanismos de mercado (AEROSPACE SUPPLY CHAIN RESILIENCY TASK FORCE, 2024; UNITED STATES, 2025).

Tecnologias como a Internet das Coisas (IoT) e os sistemas da Indústria 4.0 elevaram a eficiência logística, mas ampliaram a superfície de ataque (CHEUNG; BELL; BHATTACHARJYA, 2021). Nesse quadro, o *Cyber Supply Chain Risk Management* (C-SCRM) define-se como a estratégia organizacional de controle sobre os processos *end-to-end* que constituem as redes de TI, *hardware* e *software* (BOYSON, 2014; GHADGE *et al*., 2020). Em resposta, o Brasil instituiu o Decreto nº 12.573/2025, criando a E-Ciber para promover a soberania nacional e proteger infraestruturas críticas.

A lacuna que este artigo preenche, entretanto, não é normativa: é teórica. Os *frameworks* tradicionais de C-SCRM tratam o problema como questão de conformidade técnica, sem articular a dimensão política da securitização com a governança por maturidade organizacional. A questão central é: como o Estado pode converter a soberania decretada politicamente em capacidade de defesa real nas cadeias de suprimentos aeroespaciais? Para respondê-la, propõe-se o *Securitization and Aerospace*

Power Framework for C-SCRM (SAPF-CSCRM), arquitetura estratégica multinível que integra a dimensão política da E-Ciber aos requisitos técnicos de governança. No interior dessa arquitetura, o *Aerospace Cyber Supply Chain Risk Management Maturity Model* (AMM-CSCRM) opera como mecanismo de operacionalização da soberania digital, convertendo diretrizes políticas em capacidade organizacional verificável.

FUNDAMENTAÇÃO TEÓRICA

Cadeias de suprimentos digitais aeroespaciais

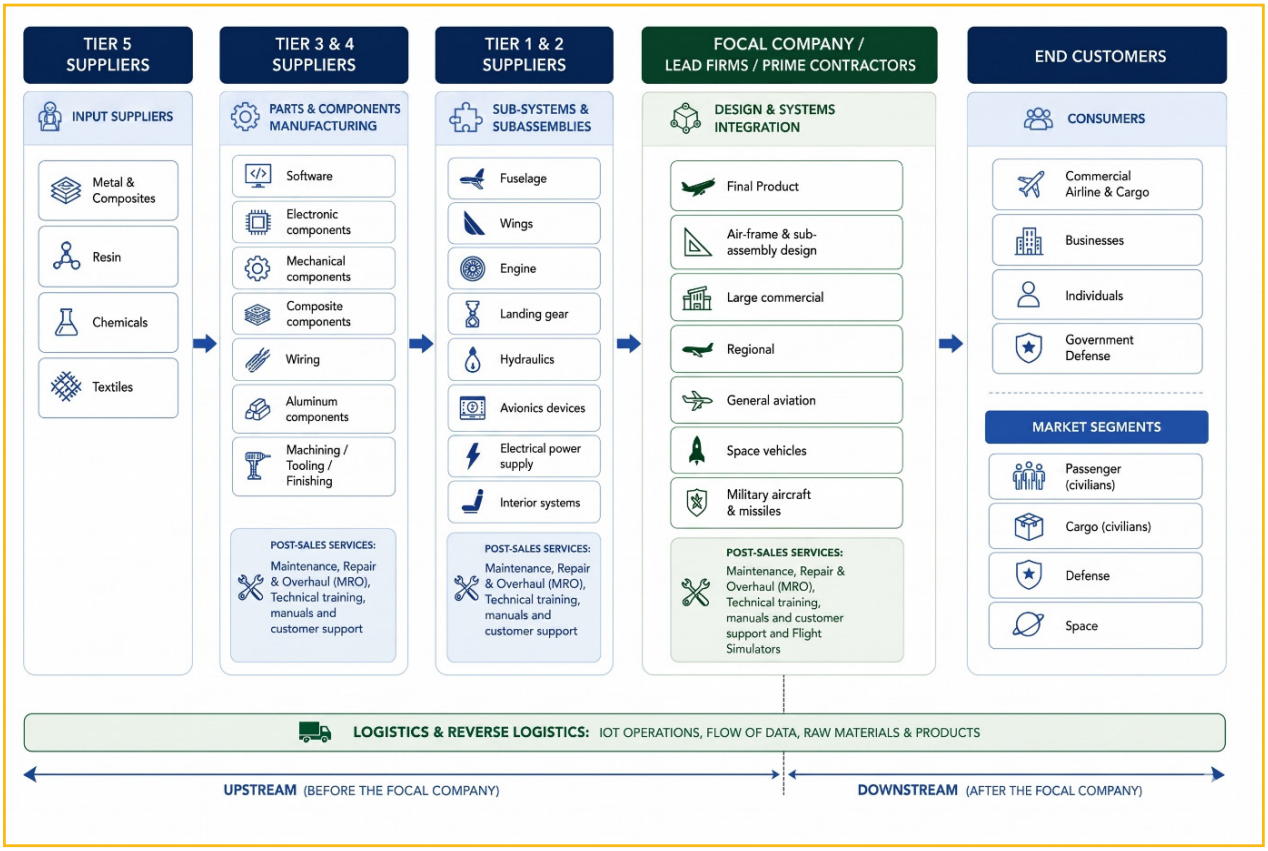
As cadeias de suprimentos aeroespaciais constituem ecossistemas globais e multiníveis integrados por fabricantes, organizações de manutenção e operadores civis e militares, sustentados por redes internacionais de fornecedores cuja complexidade limita a visibilidade ponta a ponta e exige sistemas de informação integrados, conforme sintetizado na figura 1. Essas cadeias são adicionalmente moldadas por políticas industriais, imperativos de segurança nacional, inovação tecnológica e restrições geopolíticas que condicionam sua competitividade e segurança estratégica (MILLER, 2020; BAMBER; GEREFFI, 2013).

As cadeias de suprimentos cibernéticas configuram-se como sistemas ciberfísicos sustentados por infraestruturas digitais integradas e pelo uso estratégico de dados. Essa configuração permite reconfigurações algorítmicas instantâneas, respostas em tempo real às oscilações da demanda e maior visibilidade operacional por meio de tecnologias como a Internet das Coisas (MACCARTHY; IVANOV, 2022; GHADGE *et al*., 2020; CORRÊA, 2019). Quando essa conectividade se funde aos sistemas ciberfísicos, a linha entre o virtual e o material se dissolve, gerando ativos que o NIST (2022) posiciona como elementos estratégicos para a segurança de infraestruturas críticas.

O uso de *blockchain* e *digital twins* amplia a confiabilidade e a sofisticação operacional dessas cadeias, ao permitir registros imutáveis para auditorias e contratos inteligentes, bem como a simulação virtual de ativos físicos para antecipação de

falhas e otimização da manutenção (CORRÊA, 2019; MACCARTHY; IVANOV, 2022). A computação em nuvem e de borda garantem a descentralização necessária para a agilidade sistêmica; a tecnologia 5G entrega a baixa latência requerida para a sincronia dessas ferramentas em ambientes de alta densidade tecnológica (MACCARTHY; IVANOV, 2022).

Figura 1 – Cadeia de suprimentos aeroespacial

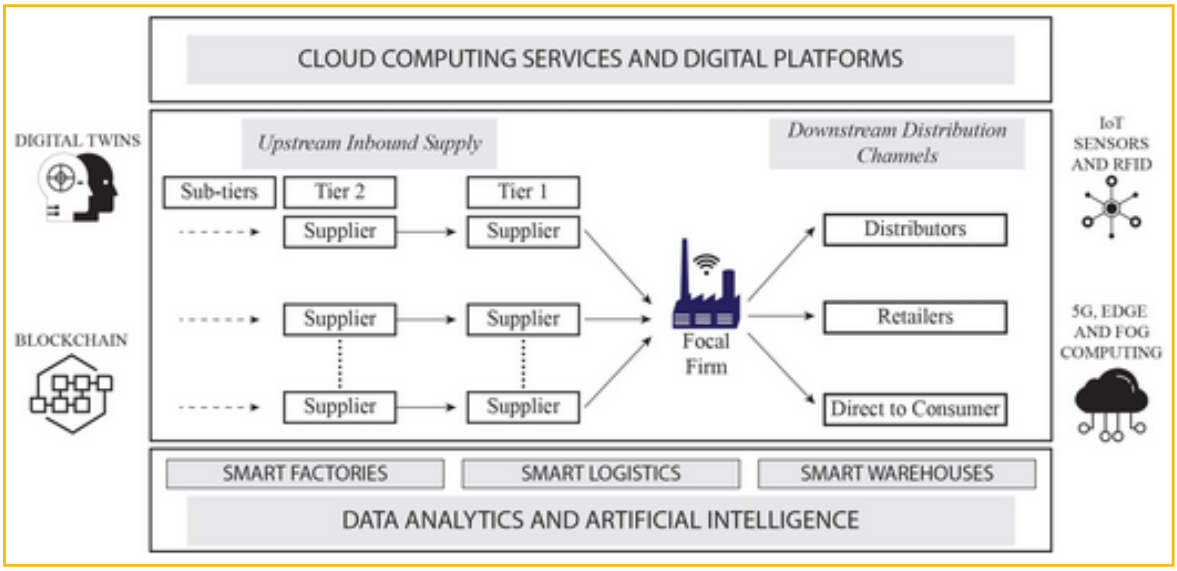


Fonte: Adaptado de BAMBER e GEREFFI (2013, p. 8)

Essa integração entre camadas física e informacional altera não apenas o funcionamento das cadeias aeroespaciais, mas a própria natureza dos riscos a que estão expostas, conforme figura 2. O incremento de eficiência trazido por sistemas ciberfísicos e computação em nuvem é inseparável da ampliação das superfícies de ataque e da criação de dependências que desafiam as organizações. Essa dualidade exige modelos de governança que integrem aspectos técnicos e estratégicos, superando abordagens reativas. É nesse ponto que a convergência entre a Teoria

da Securitização e a Teoria do Poder Aeroespacial revela sua relevância analítica: ela elucida a natureza política das ameaças a essas cadeias e fundamenta a exigência de respostas institucionalmente estruturadas.

Figura 2 – Tecnologias digitais ao longo da cadeia de suprimentos



Fonte: MACCARTHY e IVANOV (2022)

A Teoria da Securitização e cadeias de suprimentos no ciberespaço

A teoria da securitização constitui arcabouço fundamental para compreender a segurança internacional contemporânea. Ao conceber a segurança como uma construção social produzida por discursos e práticas políticas, ela revela como determinados temas são transformados em ameaças existenciais, legitimando medidas urgentes e extraordinárias, especialmente no contexto pós-Guerra Fria (BALZACQ, 2011; BUZAN; WÆVER, 2003; HANSEN; NISSENBAUM, 2009).

A teoria propõe três estágios na trajetória de um tema público: o estado não politizado, em que o assunto está fora do radar do Estado; o politizado, quando entra na agenda de debates e recursos; e o securitizado, quando rompe com a lógica da política ordinária e passa a ser tratado sob a ótica da sobrevivência, autorizando a transgressão das regras convencionais em nome da proteção do que está em jogo

(HANSEN; NISSENBAUM, 2009). Em suas leituras mais recentes, esse processo é compreendido como uma rede de práticas que envolve desde a produção da ameaça até sua aceitação por uma audiência específica, pois é essa validação que permite ao discurso gerar efeitos políticos reais (BALZACQ, 2011; BUZAN; WÆVER, 2003).

A teoria desafia a ideia de que as ameaças são dados objetivos da realidade, argumentando que elas são construídas coletivamente por meio de narrativas políticas. Como sintetizam BUZAN e WÆVER (2003), a segurança é um campo de disputa onde se decide o que deve ou não ser tratado como questão de vida ou morte, e não se pode deduzi-la apenas de dados frios. Essa perspectiva opera em múltiplas escalas: distingue dinâmicas entre grandes potências e interações regionais, além de fornecer instrumentos para classificar complexos regionais de segurança diante da ampliação de ameaças militares, econômicas, ambientais e sociais (BUZAN; WÆVER, 2003).

No plano digital, a cibersegurança foi reconhecida pela Escola de Copenhague como setor de segurança autônomo, com ameaças e prioridades próprias (HANSEN; NISSENBAUM, 2009). Se em sua origem foi tratada como domínio técnico de efeitos limitados (BUZAN; WÆVER; WILDE, 1998), sua fusão com os setores militar e econômico tornou essa autonomia incontornável. Os objetos a proteger estendem-se da infraestrutura física ao indivíduo, conectando-se a estruturas mais amplas como o Estado e a economia nacional (HANSEN; NISSENBAUM, 2009). A transição da segurança de computadores para a cibersegurança estratégica ocorre precisamente quando falhas técnicas deixam de ser problemas isolados e passam a ser narradas como ameaças à segurança nacional (NISSENBAUM, 2005; HANSEN; NISSENBAUM, 2009).

Nesse processo, HANSEN e NISSENBAUM (2009) identificam três gramáticas securitizantes: a hipersecuritização, voltada a desastres de grande escala; as práticas cotidianas, que ligam a proteção do indivíduo à segurança da rede; e a tecnificação, que frequentemente disfarça escolhas políticas sob o manto do conhecimento técnico especializado.

No Brasil, a E-Ciber é expressão nítida desse movimento. Ao elevar a proteção de serviços essenciais ao nível de prioridade estratégica, o Estado adota a lógica da urgência existencial. Diretrizes como a atualização rigorosa de infraestruturas e os novos requisitos para contratações públicas materializam as ações extraordinárias que a teoria prevê como resposta aos riscos (BRASIL, 2020; HANSEN; NISSENBAUM, 2009). Ao vincular ataques cibernéticos a danos na confiança pública e na economia, a estratégia une a segurança do *bit* à segurança do regime político.

Fundamentos da teoria aeroespacial e do poder aéreo na estruturação de cadeias de suprimentos aeroespaciais

A estruturação de cadeias de suprimentos no setor aeroespacial não pode ser compreendida isoladamente das teorias que fundamentam o Poder Aéreo e Aeroespacial. A natureza tecnológica, a dependência industrial e a necessidade de projeção global, intrínsecas a esse poder, moldam os requisitos logísticos e de suprimentos de qualquer nação que almeja operar no estado da arte.

O Poder Aéreo, em sua concepção clássica e moderna, transcende a operação de aeronaves. Como observa ROSA (2014), há consenso de que esse poder engloba elementos que extrapolam o simples emprego de aeronaves, incluindo a infraestrutura, o complexo científico-tecnológico e a indústria aeroespacial. CHUN (2001) define o poder aeroespacial como a exploração do ambiente acima da superfície terrestre para conduzir operações em apoio aos objetivos nacionais, dependendo fundamentalmente da tecnologia e de uma força de trabalho capacitada para sustentá-lo.

Essa dependência da base industrial foi identificada desde os primórdios da teoria. DOUHET (2019) argumentava, em 1921, que a aviação civil e a indústria aeronáutica deveriam ser fomentadas pelo Estado por constituírem reserva vital para a defesa nacional. Tal postulado implica reconhecer a cadeia de suprimentos e manutenção civil como base de mobilização para o poder militar, conforme a diretriz: para ter uma aviação militar eficaz, uma nação deve possuir uma aviação civil forte e numerosa (DOUHET, 2019, p. 336).

GRAY (2012) aprofunda esse raciocínio ao afirmar que o poder aéreo é um projeto de longo prazo, gerado pela riqueza nacional e por uma base avançada de ciência, tecnologia e capacidade industrial. Para o autor, a avaliação competente do poder aéreo de um país deve necessariamente levar em conta a taxa de produção de aeronaves e a escala e eficiência da organização de reparo e manutenção (GRAY, 2012, p. 311). A cadeia de suprimentos, portanto, não é atividade de suporte: é componente constitutivo do próprio poder aéreo.

CHUN (2001) reforça essa perspectiva ao destacar que a manutenção de uma força aeroespacial exige uma base tecnológica onde pessoas devem fabricar, manter e operar os sistemas de suporte de forma ininterrupta. Além disso, alerta para a interdependência global: nações podem depender de indústrias estrangeiras para componentes críticos (chips de computador e matérias-primas estratégicas), o que introduz riscos sistêmicos à gestão da cadeia de suprimentos.

ROSA (2014) identifica a "Sustentabilidade" como princípio de guerra aplicável à guerra aérea, definindo-a como a capacidade de durar na ação, estreitamente ligada ao esforço logístico de preparação e condução da operação, à capacidade de apoio das bases aéreas e ao estoque de combustíveis, armamentos e disponibilidade de aeronaves. Nesse quadro, a falha na estruturação adequada do fluxo logístico pode resultar em colapso da capacidade de combate, como historicamente demonstrado pela incapacidade da Luftwaffe em manter suas linhas de suprimento na frente russa durante a Segunda Guerra Mundial (ROSA, 2014).

A "Mobilidade Aérea" constitui outra função central na teoria aeroespacial, por ser a ferramenta que viabiliza a fluidez da cadeia de suprimentos moderna. CHUN (2001) a descreve como a capacidade de mover homens, munições e máquinas para qualquer local do mundo em curto espaço de tempo. Na teoria sistêmica de John Warden, os "Sistemas Essenciais" (fontes de energia, indústria e suprimentos) e a "Infraestrutura" (vias de transporte) são centros de gravidade críticos (ROSA, 2014).

Essa leitura impõe uma dupla perspectiva estratégica para a cadeia de suprimentos aeroespacial. Sob a dimensão defensiva/preventiva, a cadeia de suprimentos própria constitui um centro de gravidade nos anéis de "Sistemas Essenciais" e "Infraestrutura" da teoria de Warden III, devendo ser robusta, redundante e protegida para garantir a operação do poder aéreo e evitar a paralisia estratégica decorrente de vulnerabilidade logística (WARDEN III apud ROSA, 2014). Sob a dimensão ofensiva/projetiva, a capacidade de atingir a cadeia de suprimentos adversária opera como forma de paralisia estratégica: SLESSOR já argumentava que o objetivo da força aérea inclui atacar o sistema de suprimentos e as linhas de comunicação do inimigo, visando degradar sua capacidade de combate antes que as forças alcancem a frente de batalha (SLESSOR apud ROSA, 2014).

A teoria aeroespacial evoluiu, assim, de uma visão centrada na batalha aérea para uma compreensão sistêmica na qual a logística, a base industrial e a cadeia de suprimentos são determinantes. Como sintetiza GRAY (2012, p. 110), "as tecnologias avançadas e as capacidades [...] dependem de como os líderes aeroespaciais lidam com sua aplicação", o que inclui, inequivocamente, a gestão eficiente dos recursos que sustentam essas tecnologias.

A E-Ciber como ato de securitização

No Brasil, a materialização desse processo ocorre por meio da Estratégia Nacional de Cibersegurança (E-Ciber), instituída pelo Decreto nº 12.573/2025. Sob a perspectiva das Relações Internacionais, a E-Ciber não é apenas um documento técnico: é o ato de securitização formal. Ao estabelecer eixos temáticos como "Soberania Nacional e Governança" e "Segurança e Resiliência das Infraestruturas Críticas" (BRASIL, 2025), o Estado brasileiro reconhece oficialmente que a vulnerabilidade digital configura ameaça existencial. O decreto vincula ataques cibernéticos a danos na economia, na confiança pública e na capacidade de defesa, adotando a lógica da urgência. Esse ato político legitima ações extraordinárias, como a imposição de padrões rigorosos de governança à Base Industrial de Defesa (BID).

Contudo, a teoria alerta para um equívoco estrutural: o ato de fala, isto é, o decreto, não garante, por si só, a segurança. A soberania digital declarada politicamente só se materializa quando convertida em capacidade organizacional verificável. Essa lacuna de conversão, entre o discurso político e a capacidade prática, é precisamente o problema que o SAPF-CSCRM e o AMM-CSCRM se propõem a resolver.

METODOLOGIA

Esta pesquisa adota a *Design Science Research* (DSR) como paradigma orientador, modalidade que admite o uso de ferramentas computacionais para apoiar a construção, a representação e a documentação de artefatos científicos (HEVNER *et al*., 2004; PEFFERS *et al*., 2007). A escolha se justifica pela natureza propositiva do trabalho, cujo produto central são dois artefatos de governança: o SAPF-CSCRM e o AMM-CSCRM. A construção desses artefatos fundamenta-se na integração teórica entre a Teoria da Securitização (BUZAN; WÆVER, 2003; BALZACQ, 2011; HANSEN; NISSENBAUM, 2009) e a Teoria do Poder Aeroespacial (DOUHET, 2019; GRAY, 2012; CHUN, 2001), tendo como referenciais normativos o *framework* do NIST (2022) e o modelo C2M2 do DOE (2022).

A validação empírica dos artefatos foi conduzida por meio de estudo de caso único, método apropriado quando a investigação busca responder questões de "como" e "por que" sobre fenômenos contemporâneos com pouco controle do pesquisador sobre os eventos (YIN, 2001). O caso selecionado é o incidente de segurança de abril de 2018 no *Jet Propulsion Laboratory* (JPL) da NASA, classificado como caso desviante nos termos de GERRING (2007) por revelar falha em controle básico de gestão de ativos em organização de reconhecida maturidade tecnológica. A unidade de análise é o sistema de gestão de ativos de TI do JPL, compreendendo a base de dados ITSDB e os processos operacionais a ela associados.

O estudo configura-se como investigação de resultado único (*single-outcome study*), com o objetivo de explicar causalmente o desfecho de exfiltração de dados da missão *Mars Science Laboratory*. Para estabelecer a causalidade interna, empregou-

se a técnica de rastreamento de processo (*process tracing*), que permite identificar mecanismos causais entre a causa e o efeito por meio de cadeia de evidências dentro de um único caso (GERRING, 2007). A validade do construto foi assegurada pela triangulação de quatro fontes preconizadas por YIN (2001): o Relatório de Auditoria nº IG-19-022 do Gabinete do Inspetor-Geral da NASA como fonte documental primária; registros em arquivo representados pelas planilhas de inventário paralelas mantidas pelos administradores de sistemas; entrevistas com os responsáveis pela gestão dos ativos auditados; e o artefato físico constituído pelo dispositivo Raspberry Pi não autorizado conectado à rede.

O uso de ferramentas de inteligência artificial (ChatGPT, Claude, NotebookLM e Gemini) foi restrito a funções instrumentais como organização documental, extração de dados, verificação de consistência terminológica, formatação e revisão gramatical, em consonância com os princípios de transparência propostos por KHALIFA e ALBADAWY (2024). Nenhuma decisão analítica, interpretativa ou de modelagem foi delegada a essas ferramentas; a lógica de integração, a estruturação conceitual, o encadeamento metodológico e as decisões de design dos artefatos, incluindo a análise dos documentos normativos como o NIST (2022) e o DOE (2022), são integralmente autorais.

Todas as etapas que exigiram julgamento intelectual, interpretação crítica e decisões metodológicas foram conduzidas exclusivamente pelos pesquisadores, assegurando integridade autoral e rigor científico ao trabalho.

FRAMEWORK ESTRATÉGICO (SAPF-CSCRM): CONVERTENDO DISCURSO EM CAPACIDADE

Este artigo introduz o *Securitization and Aerospace Power Framework for Cyber Supply Chain Risk Management* (SAPF-CSCRM), arquitetura estratégica multinível que converte a legitimação política do risco em capacidade organizacional verificável. O *framework* articula, em cadeia causal, a teoria da securitização, a teoria do poder aeroespacial e a governança de riscos cibernéticos, tendo o *Aerospace Cyber Supply Chain*

Risk Management Maturity Model (AMM-CSCRM) como núcleo de operacionalização, conforme Figura 3.

A originalidade do SAPF-CSCRM reside em uma articulação que os *frameworks* tradicionais de C-SCRM não realizam: a integração entre a dimensão política da securitização, os imperativos estratégicos do poder aeroespacial e os mecanismos de maturidade organizacional. Enquanto abordagens convencionais tratam a gestão de riscos como questão de conformidade normativa, o SAPF-CSCRM opera como arquitetura de conversão do discurso político à capacidade prática, estruturada em seis níveis hierárquicos e causais.

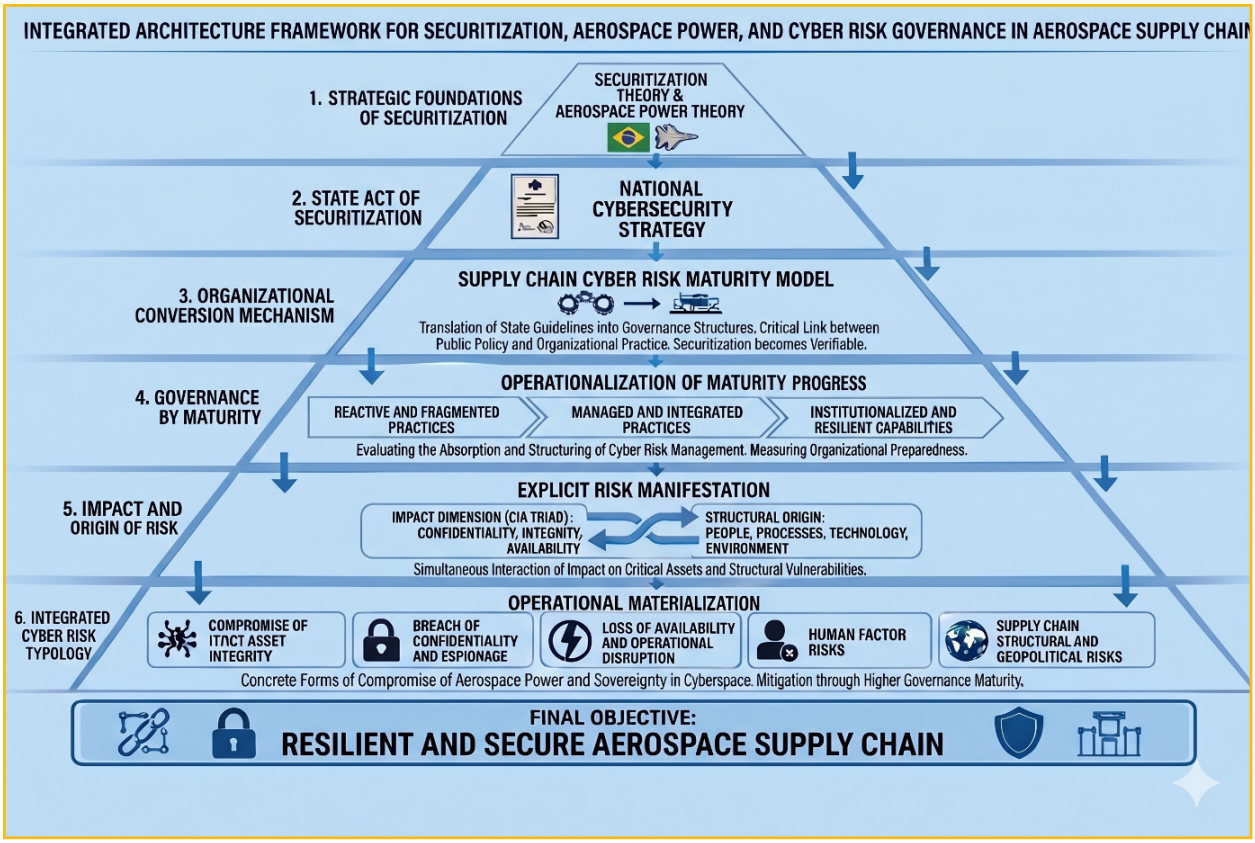
No primeiro nível, a legitimação política do risco posiciona as cadeias de suprimentos aeroespaciais como elementos críticos de segurança nacional: o risco é formalmente reconhecido como ameaça à soberania e à capacidade militar. No segundo nível, essa percepção política se formaliza em diretrizes institucionais por meio da política E-Ciber, que traduz o ato de securitização em obrigações normativas para o setor. O terceiro nível converte essas diretrizes em estruturas de governança para as organizações das cadeias de suprimentos, onde o AMM-CSCRM é introduzido como mecanismo de avaliação e progressão.

No quarto nível, o *framework* opera a governança por maturidade: avalia o grau em que as organizações adotam e institucionalizam práticas de C-SCRM, distinguindo respostas reativas de capacidades proativas como medida do preparo organizacional frente às ameaças. No quinto nível, analisa-se a origem e o impacto do risco, considerando a inter-relação entre ativos críticos e fragilidades organizacionais. Por fim, o sexto nível mapeia como os riscos cibernéticos se materializam operacionalmente, em classes como perda da integridade de ativos e espionagem industrial, comprometendo o poder aeroespacial e a soberania no ciberespaço. A mitigação desses riscos é necessariamente gradual, associada à progressão dos mecanismos de maturidade.

O SAPF-CSCRM estabelece, assim, uma lógica de conversão multinível: a teoria legitima o risco, o ato estatal o formaliza, as estruturas de governança o operacionalizam

e a maturidade torna mensurável o grau em que a soberania declarada se traduz em capacidade real. Essa arquitetura não apenas descreve o problema: ela o estrutura causalmente.

Figura 3 – Arquitetura multinível do SAPF-CSCRM para conversão estratégica da securitização em capacidade organizacional



Fonte: Autores (2026)

Legenda: Consulta a partir da articulação teórica com a teoria da securitização, a teoria do poder aeroespacial, E-Ciber (Decreto nº 12.573/2025), os referenciais do NIST (2022) e o modelo C2M2 do DOE (2022).

Embora o SAPF-CSCRM estabeleça a arquitetura necessária para articular securitização, poder aeroespacial e governança de riscos, sua efetividade depende da capacidade organizacional de implementar, sustentar e avaliar essas diretrizes ao longo do tempo. Isso exige um mecanismo capaz de mensurar estruturadamente o grau de maturidade das práticas de gestão, identificar lacunas e progressões e estabelecer níveis mínimos de capacidade verificável.

AMM-CSCRM: MECANISMO DE GOVERNANÇA POR MATURIDADE EM CADEIAS DE SUPRIMENTOS AEROESPACIAIS

O *Aerospace Cyber Supply Chain Risk Management Maturity Model* (AMM-CSCRM) é o mecanismo pelo qual o SAPF-CSCRM se torna operacional. Diferentemente de abordagens normativas baseadas em listas de controles, o AMM-CSCRM integra riscos, controles e capacidades organizacionais em uma arquitetura de avaliação de maturidade. Composto por três componentes principais (uma tipologia de riscos cibernéticos, os controles do NIST (2022) como referência técnica e o modelo C2M2 do DOE (2022) para mensuração da maturidade), o modelo assegura que a evolução das capacidades organizacionais seja monitorada de forma sistemática e normativamente fundamentada. Essa abordagem reconhece a maturidade como resultado da interação entre execução técnica e governança organizacional, indo além da mera presença de tecnologias de segurança.

O AMM-CSCRM adota a lógica de dupla progressão derivada do DOE (2022) e integrada aos controles do NIST (2022), estabelecendo dois eixos complementares de maturidade em C-SCRM, conforme sintetizado no Quadro 1. A progressão por gestão, de natureza organizacional, avalia o grau de institucionalização das práticas, considerando planejamento, documentação, financiamento, monitoramento e continuidade operacional. A progressão por abordagem, de natureza técnica, avalia a profundidade, completude e eficácia dos controles de proteção, detecção, resposta e resiliência aplicados à cadeia de suprimentos cibernética. No AMM-CSCRM, a maturidade resulta da interseção entre esses dois eixos: exige simultaneamente governança institucionalizada e implementação técnica efetiva dos controles normativos.

Quadro 1 – Dimensões de progressão avaliativa no AMM-CSCRM: gestão e abordagem técnica

Tipo de Progressão	Origem	Foco	O que avalia
Gestão	DOE (2022)	Processual	O quão institucionalizado, planejado e revisado é o domínio.
Abordagem	NIST (2022)	Técnico	A completude e eficácia da implementação dos controles.

Fonte: Autores (2026)

Legenda: Com base no modelo C2M2 do DOE (2022) e nos referenciais do NIST (2022).

De acordo com o DOE (2022), o cálculo do Nível de Indicador de Maturidade (MIL), adotado integralmente pelo AMM-CSCRM conforme apresentado no Quadro 2, utiliza escala de 0 a 3 aplicada independentemente aos dez domínios do modelo. Os níveis são cumulativos: a organização deve realizar todas as práticas dos níveis anteriores para atingir um nível superior. Durante a autoavaliação, cada prática é classificada como *Fully Implemented*, *Largely Implemented*, *Partially Implemented* ou *Not Implemented*, sendo consideradas "realizadas" apenas as práticas total ou amplamente implementadas. Práticas parcialmente ou não implementadas impedem o alcance do nível correspondente. Como os domínios são independentes, a organização pode apresentar diferentes níveis de maturidade em cada área, como MIL 1 em Gestão de Ativos e MIL 3 em Gestão de Riscos.

Quadro 2 – Regras normativas para avaliação da maturidade organizacional no AMM-CSCRM

Critério	Descrição
Escala MIL	0 a 3
Domínios	Dez domínios do modelo C2M2
Natureza Cumulativa	MILs são cumulativos; deve realizar todas as práticas do nível e dos anteriores
Prática "Realizada"	Somente *Fully Implemented* ou *Largely Implemented* são consideradas realizadas
Fully Implemented	Prática está completa
Largely Implemented	Prática está completa, mas há oportunidades de melhoria
Partially Implemented	Prática está incompleta, múltiplas oportunidades de melhoria
Not Implemented	Prática ausente ou não realizada
Resultados por Domínio	Pontuações diferentes por domínio (ex: MIL 1 em Gestão de Ativos, MIL 3 em Gestão de Riscos)

Fonte: Autores (2026)

Legenda: Com base no modelo C2M2 e nos critérios de definição dos *Maturity Indicator Level*s (MIL) (DOE, 2022).

RESULTADOS E DISCUSSÃO: VALIDAÇÃO DO AMM-CSCRM: O "PONTO CEGO" DA NASA

Estudo de caso: falha de inventário de ativos no Laboratório de Propulsão a Jato (JPL)

Esta seção valida empiricamente o SAPF-CSCRM e o AMM-CSCRM por meio do incidente de segurança ocorrido em abril de 2018 no *Jet Propulsion Laboratory* (JPL) da NASA. O caso ilustra falhas de governança de ativos cibernéticos em uma cadeia de suprimentos aeroespacial, permitindo testar a capacidade explicativa dos modelos propostos. A análise visa à generalização analítica, e não estatística.

O incidente do JPL é classificado metodologicamente como caso desviante (GERRING, 2007): a NASA, organização de alta maturidade tecnológica e alvo constante de ameaças persistentes avançadas, falha em um controle básico como a manutenção de inventário preciso de ativos. Essa anomalia torna o caso teoricamente fértil para compreender por que práticas essenciais são negligenciadas em organizações tecnologicamente avançadas. A unidade de análise não é a organização JPL em sua totalidade, mas o sistema de gestão de ativos de TI: a base de dados ITSDB e os processos humanos a ela associados.

A análise ancora-se na definição legal de ciberativos estabelecida no Art. 2º, inciso I, da E-Ciber: "*hardwares*, *softwares*, redes, dispositivos, aplicações, serviços, sistemas e dados utilizados para processar, armazenar ou transmitir informações", classificados como eixo temático essencial para a soberania nacional. A incapacidade de governar esses ativos, como evidenciado no JPL, representa vulnerabilidade direta à capacidade do Estado de exercer controle sobre suas infraestruturas críticas. Para fins de validação empírica do AMM-CSCRM, a análise normativa é deliberadamente restrita a um único controle representativo do C2M2 do DOE (2022), especificamente a prática ASSET-1a, e a um único controle do NIST (2022), o CM-8, ambos associados à gestão de ativos.

Aplicação do AMM-CSCRM: Domínio ASSET

Com base nas evidências documentais do Relatório de Auditoria IG-19-022, aplica-se o AMM-CSCRM ao Domínio ASSET (Gestão de Ativos, Mudanças e Configurações). O relatório indica que a base de dados ITSDB apresentava registros incompletos e imprecisos, sem refletir a configuração real dos ativos conectados à rede do JPL. Dispositivos críticos, incluindo o Raspberry Pi utilizado como vetor do ataque, não estavam registrados no inventário oficial nem haviam passado pelos procedimentos formais de aprovação de segurança. Essa condição caracteriza a não realização da prática ASSET-1a do C2M2 (DOE, 2022), que exige o inventário de ativos de TI e TO relevantes para a entrega das funções organizacionais. Sob a perspectiva do NIST (2022), a mesma evidência revela a violação do controle CM-8, que requer a manutenção de inventário de componentes compatível com a configuração efetivamente em operação.

A falha não se limita a um desvio pontual de conformidade: evidencia ausência de visibilidade organizacional mínima sobre os ciberativos, condição que inviabiliza a maturidade básica exigida no nível MIL 1 do domínio ASSET. A incompletude do inventário e a dissociação entre o sistema oficial e a prática operacional impedem a caracterização da prática ASSET-1a como realizada, resultando na classificação da organização abaixo do limiar básico de maturidade nesse domínio.

A implicação estratégica é direta: para a soberania nacional, nos termos da E-Ciber, o MIL 1 no Domínio ASSET é condição existencial. Não há segurança avançada que compense a ausência de visibilidade básica sobre os ativos. A falha no nível fundamental invalida investimentos em níveis superiores (MIL 2 ou MIL 3), pois não se protege o que não se conhece.

Triangulação de evidências

A validade do construto foi assegurada pela convergência de quatro fontes preconizadas por YIN (2001). O Relatório de Auditoria nº IG-19-022 constitui a fonte documental primária: após análise de varreduras de vulnerabilidade e relatórios de sistemas críticos, 4 de 13 sistemas amostrados não estavam devidamente

registrados na ITSDB. Os registros em arquivo revelaram uma estrutura paralela de gestão (*shadow IT*): 8 de 11 administradores de sistemas mantinham planilhas de inventário separadas em vez de atualizar o sistema oficial, corroborando a ineficácia da ferramenta institucional. As entrevistas forneceram o contexto humano da falha: um administrador admitiu não introduzir regularmente novos dispositivos no ITSDB porque a função de atualização "às vezes não funciona" e ele "esquece de introduzir as informações dos ativos" posteriormente. O artefato físico, um dispositivo Raspberry Pi conectado à rede sem autorização nem registro, materializou o risco: ativos desconhecidos comprometem a integridade de toda a rede.

A convergência dessas quatro fontes estabelece uma cadeia de evidências que demonstra não se tratar de erro isolado, mas de padrão estrutural de falha de governança.

Process tracing: Cadeia causal

A técnica de rastreamento de processo (*process tracing*) (GERRING, 2007) permitiu reconstruir a cadeia causal que liga a falha de governança à exfiltração de dados. O antecedente foi a falha de governança: a ITSDB apresentava problemas de usabilidade e confiabilidade, levando administradores a manterem planilhas paralelas desconectadas do sistema central. Como mecanismo de falha, a ausência de controle de mudanças permitiu que um usuário conectasse um Raspberry Pi à rede sem aprovação ou registro. No evento crítico, cibercriminosos comprometeram a conta de um usuário externo e utilizaram o dispositivo não autorizado como porta de entrada, progredindo lateralmente para sistemas de missão pela falta de segmentação adequada no *gateway* de rede. A falha de detecção decorreu diretamente da invisibilidade do dispositivo: por não constar no inventário oficial, o Raspberry Pi permaneceu fora das varreduras de segurança e da aplicação de *patches*. O resultado foi a permanência do invasor na rede por aproximadamente dez meses sem detecção, com a exfiltração de 500 megabytes de dados da missão Mars Science Laboratory.

Esse encadeamento valida a premissa central do AMM-CSCRM: a falha na gestão de ativos foi o mecanismo causal determinante para o sucesso do ataque, e não uma falha secundária ou colateral.

Generalização analítica

O achado principal do caso NASA/JPL corrobora a proposição teórica do SAPF-CSCRM: a função “Identificar” do *framework* do NIST (2022), expressa na precisão do inventário, é pré-requisito não negociável para a cibersegurança. Ferramentas de “Proteção” e “Detecção” tornam-se ineficazes sem visibilidade completa sobre o que está conectado à rede. A validação pelo AMM-CSCRM confirma a lógica cumulativa do modelo: embora a organização possuísse capacidades técnicas sofisticadas, a falha nas práticas básicas ASSET-1a e CM-8 no MIL 1 impediu o atingimento de níveis superiores de maturidade e anulou a eficácia dos investimentos em segurança avançada.

Sob a perspectiva da E-Ciber, o caso reforça a necessidade de mecanismos robustos de fiscalização: a falha por erro técnico ou esquecimento ilustra a insuficiência de diretrizes políticas sem governança por maturidade. O estudo valida as diretrizes do Art. 6º, inciso II, e do Art. 10º, inciso II, do Decreto nº 12.573/2025, que preveem a governança por maturidade como instrumento necessário para evitar que falhas administrativas básicas comprometam a soberania sobre ativos estratégicos aeroespaciais.

O incidente no JPL transcende uma falha técnica operacional para se configurar como validação empírica do AMM-CSCRM: a segurança das cadeias de suprimentos aeroespaciais é um fenômeno simultaneamente estratégico, político e militar. A vulnerabilidade de um único ativo não gerido comprometeu a integridade da missão *Mars Science Laboratory* e evidenciou que o poder espacial no século XXI depende decisivamente de *software*, dados e redes, tornando a infraestrutura digital uma extensão funcional do sistema de comando e controle. Sob a ótica da Teoria da Securitização, o caso confirma que o reconhecimento político da ameaça, representado pela E-Ciber, só produz efeitos reais quando convertido em capacidade organizacional verificável.

O Quadro 3 sintetiza as seis etapas da validação empírica do AMM-CSCRM aplicada ao caso NASA/JPL, estruturadas a partir do método de estudo de caso

(YIN, 2001) e do desenho de caso desviante com process tracing (GERRING, 2007). A sequência percorre desde a definição da questão central como a fragilidade no sistema de inventário ITSDB permitiu a persistência da ameaça, até a conclusão analítica de que controles avançados de cibersegurança dependem da integridade de práticas fundamentais, como o inventário de ativos. A teoria mobilizada ancora-se no Domínio ASSET do modelo, especificamente na prática ASSET-1a e no controle CM-8 (nível de maturidade MIL 1), cujas falhas são evidenciadas por triangulação de fontes: o relatório de auditoria IG-19-022 *do Office of Inspector General* da NASA, registros de planilhas paralelas, o dispositivo Raspberry Pi não autorizado e depoimentos colhidos nas entrevistas. A articulação entre essas etapas demonstra a coerência interna do processo analítico e fundamenta a generalização analítica proposta, referenciada nos frameworks do NIST (2022) e do C2M2 do DOE (2022).

Quadro 3 – Síntese metodológica da validação empírica do AMM-CSCRM no caso NASA/JPL

Etapa	Ação Metodológica	Aplicação no Caso NASA/JPL
1. Design	Definir Questão (YIN, 2001)	Como a falha no ITSDB permitiu a persistência da ameaça?
2. Seleção	Caso Desviante (GERRING, 2007)	NASA (alta tecnologia) falhando em controle básico (inventário).
3. Teoria	Maturidade (AMM-CSCRM)	Falha no Domínio ASSET: prática ASSET-1a e controle CM-8 (MIL 1)
4. Evidência	Triangulação (YIN, 2001)	Relatório IG-19-022, planilhas paralelas, Raspberry Pi, entrevistas.
5. Análise	Process tracing (GERRING, 2007)	Dispositivo não registrado, sem monitoramento, invasão persistente.
6. Conclusão	Generalização Analítica (YIN, 2001)	A segurança avançada depende da integridade do inventário básico.

Fonte: Autores (2026)

Legenda: A partir da aplicação do método de estudo de caso (YIN, 2001), do desenho de caso desviante e *process tracing* (GERRING, 2007), do Modelo de Maturidade AMM-CSCRM, e das evidências empíricas do relatório de auditoria do Office of Inspector General da NASA (IG-19-022), em articulação com os referenciais do NIST (2022) e do modelo C2M2 do DOE (2022).

CONCLUSÃO

A securitização do ciberespaço constitui, hoje, um processo político. Decretos como a E-Ciber formalizam o reconhecimento de que a cadeia de suprimentos aeroespacial é infraestrutura crítica de soberania nacional. O que este artigo demonstra é que esse reconhecimento é necessário, mas insuficiente: a soberania digital não se realiza pelo ato de fala: ela exige maturidade organizacional verificável.

O SAPF-CSCRM articula essa lacuna de conversão por meio de uma arquitetura estratégica multinível que os *frameworks* tradicionais de C-SCRM não oferecem: a integração causal entre securitização, poder aeroespacial e governança por maturidade. Ao estruturar a trajetória da legitimação política à capacidade prática, passando pela formalização institucional e pela avaliação organizacional, o *framework* não apenas descreve o problema: ele o equaciona teoricamente.

O AMM-CSCRM operacionaliza esse caminho. Ao integrar tipologia de riscos, controles normativos e Níveis de Indicador de Maturidade em uma lógica de dupla progressão, simultaneamente processual e técnica, o modelo converte as diretrizes da E-Ciber em capacidade industrial e digital mensurável. Sua contribuição não é apenas avaliativa: é instrumental para a construção do modelo nacional de maturidade em cibersegurança previsto no Decreto nº 12.573/2025.

A validação empírica pelo caso NASA/JPL revela o custo estratégico da imaturidade básica: a ausência de inventário preciso de ativos no MIL 1 do domínio ASSET criou um ponto cego estrutural que tornou ineficazes as ferramentas avançadas de monitoramento da organização. Dez meses de intrusão e 500 megabytes de dados de missão crítica exfiltrados são a tradução operacional de uma falha que não era técnica em sua origem: era de governança. Não se protege o que não se conhece. A gestão de ativos não é requisito administrativo: é condição existencial da segurança cibernética.

Embora sem pretensão de generalização estatística, a validação do AMM-CSCRM no domínio de gestão de ativos confirma a governança por maturidade como o instrumento necessário para converter os eixos da E-Ciber em capacidade real, e não apenas em compromisso normativo.

REFERÊNCIAS

AEROSPACE INDUSTRIES ASSOCIATION. **Supply chain cybersecurity recommendations report**. [S.l.]: Aerospace Industries Association, 2023. Disponível em: https://www.aia-aerospace.org/wp-content/uploads/Supply-Chain-Cybersecurity-Recommendations-Report.pdf. Acesso em: 24 jan. 2026.

AEROSPACE SUPPLY CHAIN RESILIENCY TASK FORCE. **Aerospace supply chain resiliency task force report to Congress**. [S.l.]: Federal Aviation Administration, 2024. Disponível em: https://gama.aero/wp-content/uploads/Aerospace-Supply-Chain-Resiliency-Task-Force-Report-FINAL.pdf. Acesso em: 24 jan. 2026.

BALZACQ, Thierry. **Securitization Theory: How Security Problems Emerge and Dissolve**. London & New York: Routledge, 2011.

BAMBER, Penny; GEREFFI, Gary. **Costa Rica in the Aerospace Global Value Chain: opportunities for entry & upgrading**. Durham: Duke University, Center on Globalization, Governance and Competitiveness, 2013. Disponível em: https://www.researchgate.net/publication/265333072_Costa_Rica_in_the_Aerospace_Global_Value_Chain_Opportunities_for_Upgrading. Acesso em: 1 jan. 2024.

BOYSON, Sandor. Cyber supply chain risk management: revolutionizing the strategic control of critical IT systems. **Technovation**, [S.l.], v. 34, n. 7, p. 342-353, jul. 2014. DOI: http://dx.doi.org/10.1016/j.technovation.2014.02.001. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0166497214000194. Acesso em: 13 jan. 2026.

BRASIL. Comando da Aeronáutica. **Concepção Estratégica: Força Aérea 100**. Brasília, DF: Centro de Comunicação Social da Aeronáutica, 2018. Disponível em: https://www.fab.mil.br/Download/arquivos/FA100.pdf. Acesso em: 13 jan. 2026.

BRASIL. Decreto nº 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. **Diário Oficial da União**: seção 1, Brasília, DF, 6 fev. 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419. Acesso em: 13 jan. 2026.

BRASIL. Decreto nº 12.573, de 4 de agosto de 2025. Institui a Estratégia Nacional de Cibersegurança. **Diário Oficial da União**: seção 1, Brasília, DF, ed. 146, p. 2, 5 ago. 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/d12573.htm. Acesso em: 15 maio 2026.

BRASIL. Ministério da Defesa. Portaria GM-MD n° 5.081, de 16 de outubro de 2023. Aprova a Doutrina Militar de Defesa Cibernética. **Diário Oficial da União**: seção 1, Brasília, DF, 25 out. 2023. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/estado-maior-conjunto-das-forcas-armadas/doutrina-militar/publicacoes-1/publicacoes/MD31M07DoutrinaMilitardeDefesaCiberntica2Edio2023.pdf. Acesso em: 15 maio 2026.

BUZAN, Barry; HANSEN, Lene. **The Evolution of International Security Studies**. Cambridge: Cambridge University Press, 2009.

BUZAN, Barry; WÆVER, Ole. **Regions and Powers: The Structure of International Security**. Cambridge: Cambridge University Press, 2003.

BUZAN, Barry; WÆVER, Ole; WILDE, Jaap de. **Security: A New Framework for Analysis**. Boulder, CO: Lynne Rienner, 1998.

CHEUNG, Kam-Fung; BELL, Michael G. H.; BHATTACHARJYA, Jyotirmoyee. Cybersecurity in logistics and supply chain management: an overview and future research directions. **Transportation Research Part E: Logistics and Transportation Review**, [S.l.], v. 146, p. 102217, fev. 2021. Acesso em: 15 maio 2026.

CHUN, Clayton K. S. **Aerospace Power in the Twenty-First Century: a basic primer**. Colorado Springs: United States Air Force Academy; Maxwell Air Force Base: Air University Press, 2001.

CORRÊA, Henrique Luiz. **Administração de cadeias de suprimentos e logística: integração na era da indústria 4.0**. 2. ed. São Paulo: Atlas, 2019.

DOUHET, Giulio. **The command of the air**. Tradução de Dino Ferrari. Maxwell AFB: Air University Press, Curtis E. LeMay Center for Doctrine Development and Education, 2019.

GERRING, John. **Case study research: principles and practices**. Cambridge: Cambridge University Press, 2007.

GHADGE, Abhijeet et al. **Managing cyber risk in supply chains: a review and research agenda**. [S.l.: s.n.], 2020. Disponível em: https://www.researchgate.net/publication/334736415_Managing_cyber_risk_in_supply_chains_A_review_and_research_agenda. Acesso em: 13 jan. 2026.

GRAY, Colin S. **Airpower for strategic effect**. Maxwell Air Force Base: Air University Press, Air Force Research Institute, 2012.

HANSEN, Lene; NISSENBAUM, Helen. Digital Disaster, Cyber Security, and the Copenhagen School. **International Studies Quarterly**, [S.l.], v. 53, n. 4, p. 1155-1175, 2009. Disponível em: https://nissenbaum.tech.cornell.edu/papers/Digital%20Disaster.pdf. Acesso em: 15 maio 2026.

HEVNER, Alan R. et al. Design Science in Information Systems Research. **MIS Quarterly**, [S.l.], v. 28, n. 1, p. 75-106, 1 mar. 2004. Disponível em: https://www.researchgate.net/publication/201168946_Design_Science_in_Information_Systems_Research. Acesso em: 15 maio 2026.

KHALIFA, M.; ALBADAWY, M. Using artificial intelligence in academic writing and research: an essential productivity tool. **Computer Methods and Programs in Biomedicine Update**, [S.l.], v. 5, p. 100145, 5 mar. 2024. Disponível em: https://www.researchgate.net/publication/378752005_Using_Artificial_Intelligence_in_Academic_Writing_and_Research_An_Essential_Productivity_Tool. Acesso em: 15 maio 2026.

MACCARTHY, Bart L.; IVANOV, Dmitry. The Digital Supply Chain: emergence, concepts, definitions, and technologies. In: MACCARTHY, Bart L.; IVANOV, Dmitry (ed.). **The Digital Supply Chain**. Amsterdam: Elsevier, 2022. Cap. 1. p. 22-44.

MILLER, Randall. **Why supply chain management is important in aerospace and defense**. [S.l.]: EY, 2020. Disponível em: https://www.ey.com/en_au/aerospace-defense/why-supply-chain-management-is-important-in-aerospace-and-defense. Acesso em: 13 jan. 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations: NIST SP 800-161r1**. Gaithersburg, MD: U.S. Department of Commerce, 2022. Disponível em: https://doi.org/10.6028/NIST.SP.800-161r1-upd1. Acesso em: 8 abr. 2025.

NISSENBAUM, Helen. Where Computer Security Meets National Security. **Ethics and Information Technology**, [S.l.], v. 7, n. 2, p. 61-73, 2005.

PAULUS, Alexandra. **An Achilles heel of today's armed forces: managing software supply chain risk in the military sector**. Berlin: Stiftung Wissenschaft und Politik, 2025. Disponível em: https://www.swp-berlin.org/publications/products/research_papers/2025RP06_SoftwareSupplyChainRisk_Military.pdf. Acesso em: 24 jan. 2026.

PEFFERS, Ken et al. A Design Science Research Methodology for Information Systems Research. **Journal of Management Information Systems**, [S.l.], v. 24, n. 3, p. 45-77, dez. 2007. Disponível em: https://www.researchgate.net/publication/284503626_A_design_science_research_methodology_for_information_systems_research. Acesso em: 15 maio 2026.

PINTO, Danielle Jacon Ayres; GRASSI, Jessica Maria. Guerra cibernética, ameaças às infraestruturas críticas e a defesa cibernética do Brasil. **Revista Brasileira de Estudos de Defesa**, Niterói, v. 7, n. 2, p. 103-131, jul./dez. 2020. Disponível em: https://rbed.abedef.org/rbed/article/view/75178. Acesso em: 15 maio 2026.

ROSA, Carlos Eduardo Valle. **Poder Aéreo: guia de estudos**. Rio de Janeiro: Luzes, 2014.

UNITED STATES. Department of Energy. **Cybersecurity Capability Maturity Model (C2M2)**. Version 2.1. Washington, DC: Department of Energy, 2022. Disponível em: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2. Acesso em: 8 abr. 2025.

UNITED STATES. Executive Office of the President. Office of the National Cyber Director; National Space Council. **Space system cybersecurity: space industry perspectives**. Washington, DC: The White House, 2025. Disponível em: https://bidenwhitehouse.archives.gov/wp-content/uploads/2025/01/Space-System-Cybersecurity-Industry-Perspectives-Report.pdf. Acesso em: 24 jan. 2026.

UNITED STATES. National Aeronautics and Space Administration. Office of Inspector General. **NASA's Jet Propulsion Laboratory (JPL): IG-19-022**. [S.l.], 2019. Disponível em: https://oig.nasa.gov/wp-content/uploads/2024/02/IG-19-022.pdf. Acesso em: 8 abr. 2025.

YIN, Robert K. **Estudo de caso: planejamento e métodos**. Tradução de Daniel Grassi. 2. ed. Porto Alegre: Bookman, 2001.

Autoria

1 Andre Luiz Anjos de Figueiredo

Graduado em Administração pela Universidade Santa Úrsula, Mestre em Logística pela Pontifícia Universidade Católica do Rio de Janeiro, Doutorando em Ciências Aeroespaciais pela Universidade da Força Aérea, Professor
https://orcid.org/0000-0003-4002-7219 • figueiredo.anjos23@gmail.com

2 Pedro Arthur Linhares Lima

Graduado em Formação de Oficiais Intendentes pela Academia da Força Aérea, Mestre em Computer Science pela Air Force Institute of Technology, Doutorado em Engenharia de Produção pela Universidade Federal do Rio de Janeiro, MBA em Planejamento Estratégico pela Universidade Federal do Rio de Janeiro, Professor
https://orcid.org/0000-0002-2581-8381 • https://ror.org/03t7a2639

Como citar este artigo

FIGUEIREDO, A. L. A.; LIMA, P. A. L. Do Ato de Securitização à capacidade organizacional: Proposta de Framework Estratégico e Modelo de Maturidade para a Gestão de Riscos Cibernéticos em Cadeias de Suprimentos Aeroespaciais (C-SCRM). **InterAção**, Santa Maria, v. 17, n. 2, e95382, p. 1-26, jun. 2026. DOI 10.5902/1980509895382. Disponível em: https://dx.doi.org/10.5902/2357797595382. Acesso em: dia mês abreviado. ano.