DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Proposta de Modelo Hierárquico para Avaliação de Criticidade em Infraestruturas Críticas Brasileiras: Comparação com o Modelo PPSI

Edvan Gomes da Silva

Programa de Pós-Graduação Profissional em Engenharia Elétrica

DEPARTAMENTO DE ENGENHARIA ELÉTRICA
FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Proposta de Modelo Hierárquico para Avaliação de Criticidade em Infraestruturas Críticas Brasileiras: Comparação com o Modelo PPSI

Edvan Gomes da Silva

Dissertação de Mestrado Profissional submetida ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Mestre em Engenharia Elétrica

Banca Examinadora

Rafael Rabelo Nunes, Dr., ADM/FACE/UnB _____
Orientador

Prof. Banca 1, Ph.D, FT/UnB _____
Examinador Interno

Prof. Banca 2, Ph.D, FT/UnB _____
Examinador interno

FICHA CATALOGRÁFICA

SILVA GOMES, EDVAN
Proposta de Modelo Hierárquico para Avaliação de Criticidade em Infraestruturas Críticas Brasileiras: Comparação com o Modelo PPSI [Distrito Federal] 2025.
xvi, 63 p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2025).
Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

1. Infraestruturas Críticas
2. Avaliação de Criticidade
3. Gestão de Ativos
4. Critérios

I. ENE/FT/UnB
II. Título (série)

PUBLICAÇÃO: PPEE.MP.092

REFERÊNCIA BIBLIOGRÁFICA

SILVA GOMES, EDVAN. (2025). *Proposta de Modelo Hierárquico para Avaliação de Criticidade em Infraestruturas Críticas Brasileiras: Comparação com o Modelo PPSI*. Dissertação de Mestrado Profissional, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 63 p.

CESSÃO DE DIREITOS

AUTOR: Edvan Gomes da Silva
TÍTULO: Proposta de Modelo Hierárquico para Avaliação de Criticidade em Infraestruturas Críticas Brasileiras: Comparação com o Modelo PPSI.
GRAU: Mestre em Engenharia Elétrica ANO: 2025
PUBLICAÇÃO: PPEE.MP.092

Edvan Gomes da Silva
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

DEDICATÓRIA

Dedico este trabalho, à minha esposa e ao meu filho, que demonstraram notável resiliência ao suportar minha ausência em diversos momentos para que eu pudesse me dedicar aos estudos, além de me darem o apoio necessário nos momentos mais exaustivos.

AGRADECIMENTOS

Expresso meus sinceros agradecimentos a Fernando Rocha Moreira, que reconheceu em mim um potencial acadêmico e me incentivou a ingressar no curso de mestrado. Agradeço também ao meu orientador, Rafael Rabelo Nunes, cuja excelência profissional me permitiu não apenas aprofundar os conhecimentos específicos da minha pesquisa, mas também adquirir lições valiosas para meu desenvolvimento pessoal e profissional, além de momentos de descontração ao longo desta jornada. Minha gratidão se estende a Marcus Georg, por seu auxílio fundamental na construção dos modelos e na condução da pesquisa. Agradeço ao meu coorientador, Luiz Antonio Ribeiro Junior, cujo apoio técnico e orientação na metodologia foram essenciais para o desenvolvimento deste trabalho. Sua confiança em minha capacidade de enfrentar desafios e submeter artigos a revistas de maior impacto foi importante para meu crescimento acadêmico e profissional. Por fim, agradeço a Laerte Peotta, pelo constante incentivo e apoio no ambiente de trabalho, essenciais para a conclusão deste estudo.

RESUMO

A sociedade contemporânea depende de sistemas que desempenham funções críticas para o processamento, armazenamento e transmissão de informações sensíveis, estando cada vez mais exposta a ameaças cibernéticas. Este trabalho tem como objetivo propor um modelo hierárquico para a avaliação da criticidade de sistemas aplicável às infraestruturas críticas brasileiras, fundamentado na análise de metodologias internacionais e na estrutura do Programa de Privacidade e Segurança da Informação (PPSI). O estudo concentrou-se na identificação, categorização e estruturação dos critérios e subcritérios utilizados por diferentes países e organizações para definição e análise de infraestruturas críticas, sem a aplicação de métodos de ponderação. Inspirando-se na abordagem hierárquica de métodos multicritério, como o Analytic Hierarchy Process (AHP), mas sem sua implementação direta, a pesquisa resultou em um modelo sistematizado de critérios, alinhado às melhores práticas internacionais e adaptado ao contexto brasileiro. A principal contribuição consiste em fornecer uma base conceitual e metodológica que pode apoiar gestores e profissionais de segurança na identificação e priorização de ativos críticos, promovendo o aprimoramento das estratégias de proteção e gestão de riscos em infraestruturas essenciais para o funcionamento da sociedade. Os resultados demonstram que estruturas existentes no contexto brasileiro, especialmente em órgãos governamentais, podem ser aprimoradas por meio do modelo proposto, apontando para a necessidade de revisão e adaptação contínua das práticas de avaliação da criticidade, de forma a aumentar a resiliência das infraestruturas críticas diante das ameaças emergentes.

ABSTRACT

Contemporary society depends on systems that perform critical functions for the processing, storage, and transmission of sensitive information, becoming increasingly exposed to cyber threats. This work aims to propose a hierarchical model for assessing the criticality of systems applicable to Brazilian critical infrastructures, based on the analysis of international methodologies and the structure of the Privacy and Information Security Program (PPSI). The study focused on the identification, categorization, and structuring of criteria and subcriteria used by different countries and organizations for the definition and analysis of critical infrastructures, without applying weighting methods. Inspired by the hierarchical approach of multicriteria methods, such as the Analytic Hierarchy Process (AHP), but without its direct implementation, the research resulted in a systematized model of criteria aligned with international best practices and adapted to the Brazilian context. The main contribution is to provide a conceptual and methodological foundation that can support managers and security professionals in identifying and prioritizing critical assets, promoting the improvement of protection strategies and risk management in infrastructures essential to the functioning of society. The results demonstrate that existing structures within the Brazilian context, especially in governmental bodies, can be improved through the proposed model, highlighting the need for

continuous review and adaptation of criticality assessment practices to enhance the resilience of critical infrastructures in the face of emerging threats.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AHP	Analytic Hierarchy Process
IC	Infraestruturas Críticas
PPSI	Programa de Privacidade e Segurança da Informação
TCU	Tribunal de Contas da União
SISP	Sistema de Administração dos Recursos de Tecnologia da Informação
NCIAP	Programa Nacional de Garantia da Infraestrutura Crítica
CIA	Central Intelligence Agency
RU	Reino Unido
APF	Administração Pública Federal
TI	Tecnologia da Informação
ITAM	IT Asset Management (Gestão de Ativos de TI)
ONS	Operador Nacional do Sistema Elétrico
CPIC	Comissão de Proteção de Infraestruturas Críticas
UE	União Europeia
ICE	Infraestruturas Críticas Europeias
CNPIC	Centro Nacional para a Proteção de Infraestruturas Críticas (Espanha)
PPD-21	Presidential Policy Directive 21 (Diretiva Presidencial de Política 21, EUA)
NIST	National Institute of Standards and Technology
ISO	International Organization for Standardization

1 INTRODUÇÃO

A sociedade contemporânea depende profundamente de sistemas que executam funções críticas de processamento, armazenamento e transmissão de informações sensíveis; contudo, observa-se a crescente disseminação de diversos tipos de ameaças que se infiltram nos setores empresariais e industriais [1]. É importante ressaltar que fabricantes e organizações nem sempre estão devidamente preparados para lidar com os impactos decorrentes de ataques cibernéticos bem-sucedidos ou acidentes nesses contextos [2].

Estima-se que o ônus associado ao cibercrime atinja a marca de US$ 10,5 trilhões até 2025 [3]. Para combater isso, os defensores empregam uma variedade de produtos de segurança com o propósito de evitar, detectar e interromper ataques em andamento. No entanto, o aumento contínuo em termos de capacidade, persistência e complexidade dos ataques adversários tem contribuído para a ineficácia das abordagens tradicionais de defesa [4].

Nesse contexto, a gestão de riscos assume importância central. Conforme indicado por Cynthia Brumfield [5], o planejamento e a gestão de riscos de segurança cibernética constituem a etapa inicial para orientar a empresa em direção à segurança digital. Para profissionais sem experiência na área, isso pode representar um desafio. Brumfield enfatiza que a preparação antecipada é essencial como primeiro passo para lidar com incidentes cibernéticos [5].

Além disso, a gestão de riscos desempenha papel relevante na segurança das Infraestruturas Críticas, envolvendo a implementação de um método lógico e sistemático para estabelecer contextos, identificar, avaliar e tratar os riscos, a fim de cumprir critérios e requisitos essenciais para garantir a continuidade das operações. Importa destacar que os esforços dedicados à proteção dessas infraestruturas não garantem segurança absoluta. Em situações de crise, instalações, bens, serviços ou sistemas podem ser afetados, demandando a implementação de medidas de mitigação e contingência para aumentar a resiliência da infraestrutura e garantir seu retorno à normalidade dentro de padrões de tempo adequados à sua criticidade [6].

Para uma gestão de segurança eficaz, é imperativo que a organização identifique o risco e o valor crítico de cada dispositivo catalogado em seu inventário de ativos, destacando a importância de determinar os responsáveis pela autorização de acesso a esses dispositivos. Aspectos fundamentais, como apetite e tolerância ao risco, práticas de mitigação, tratamento de risco residual, implementação de contramedidas específicas para cada dispositivo ou serviço, juntamente com a realização de análises de impacto nos negócios, são essenciais para uma compreensão clara dos fatores estratégicos envolvidos [7].

Nesse sentido, modelos de avaliação de criticidade de sistemas tornam-se ferramentas essenciais para identificar o nível de criticidade de cada sistema relevante da organização, devido à sua exposição a riscos de privacidade e segurança da informação [8]. Um exemplo é o modelo adotado pelo Tribunal de Contas da União (TCU), por meio do Acórdão 1.889/2020-TCU-Plenário, que visa realizar o levantamento de riscos em sistemas informacionais da Administração Pública Federal. Este modelo considera fatores como impactos e vulnerabilidades associados aos sistemas, aplicando pesos e cálculos específicos para determinar a criticidade [9].

O padrão CIP-002-1 (Identificação de Ativos Críticos), criado pela North American Electric Reliability Corporation, exige uma metodologia de avaliação baseada em riscos para identificar ativos críticos [10]. No entanto, não especifica um método particular nem estabelece requisitos detalhados para uma abordagem adequada. Há uma necessidade premente de esclarecer como as metodologias de análise de risco existentes podem ser empregadas para avaliar, categorizar, priorizar e proteger as infraestruturas críticas [11].

A capacidade de determinar uma hierarquia de prioridades para os sistemas a serem monitorados garante uma proteção mais eficiente, ao mesmo tempo em que otimiza a alocação dos recursos de segurança da organização. Com clareza sobre quais sistemas necessitam de proteção prioritária, a organização pode desenvolver um conjunto unificado de controles de segurança relevantes [12].

Estabelecer a definição do termo "crítico"para a organização é um pré-requisito essencial para o gerenciamento de riscos, pois é fundamental para compreender exatamente o que precisa ser gerenciado. Em muitas organizações, essa não é uma tarefa simples. Unidades de negócios individuais, colaboradores isolados e grupos de executivos frequentemente possuem suas próprias concepções sobre o que constitui um ativo crítico [13].

A dificuldade em discernir entre o que é crítico para a organização e o que é crítico para o desempenho individual abre espaço para uma abordagem equivocada, na qual se tenta proteger todos os ativos igualmente, em vez de concentrar-se naqueles que os atacantes possam almejar e que possam gerar uma crise se comprometidos. Quando as organizações caem nessa armadilha, a priorização clara de programas e atividades torna-se desafiadora [13].

Muitas soluções metodológicas já foram desenvolvidas para abordar questões de cibersegurança. No entanto, a análise de ativos críticos para proteção contra ataques cibernéticos e os impactos comerciais resultantes não recebe a devida ênfase. Essa análise pode desempenhar um papel estratégico para as empresas, ajudando-as a entender em quais ativos devem concentrar seus esforços de segurança, em que ordem de prioridade e em que extensão [14].

Considerando esses aspectos, este trabalho tem como objetivo principal propor um modelo hierárquico de critérios para a avaliação das infraestruturas críticas brasileiras, fundamentado na análise dos critérios atualmente utilizados para classificação de ativos críticos, assim como no Anexo I do Programa de Privacidade e Segurança da Informação (PPSI), com o intuito de aprimorar a aplicação desse modelo em órgãos governamentais.

1.1 MOTIVAÇÃO E JUSTIFICATIVA

A sociedade contemporânea opera sobre uma base de ativos interdependentes – da distribuição de energia à entrega de serviços governamentais – cuja falha pode comprometer vidas humanas, a economia e a própria nas instituições. Ao longo dos últimos vinte anos, nações como Estados Unidos, Japão, Holanda e Portugal consolidaram metodologias de avaliação de criticidade que orientam investimentos e políticas de proteção. No Brasil, entretanto, ainda inexistem critérios unificados, validados e alinhados às especificidades regulatórias e operacionais dos órgãos públicos. Essa lacuna metodológica faz com que muitos gestores classifiquem todos os sistemas como igualmente “críticos”, dispersando recursos escassos e reduzindo a

efetividade das ações de segurança.

Motiva-se, portanto, esta pesquisa pelo seguinte conjunto de fatores:

1. **Problema prático solucionado**
   A dissertação desenvolve e apresenta um modelo hierárquico de decisão que consolida, organiza e adapta critérios extraídos de doze diretrizes internacionais e do Programa de Privacidade e Segurança da Informação (PPSI). Isso resolve o desafio concreto enfrentado pelos órgãos do SISP ao tentar priorizar sistemas sem uma estrutura comparável de referência.

2. **Contribuição científica original**
   Oferece a primeira síntese sistemática das práticas de avaliação de criticidade de doze jurisdições, evidenciando lacunas conceituais e propondo um arcabouço alinhado ao contexto brasileiro.
   Avança a literatura nacional ao demonstrar como métodos multicritério (AHP) podem ser empregados mesmo quando não se dispõe, preliminarmente, de ponderações consensuais entre especialistas.

3. **Amplitude da revisão de literatura**
   Foram analisados diversos documentos (leis, diretrizes e relatórios técnicos). Esse mapeamento permitiu identificar padrões de impacto (pessoas, economia, geografia, interdependências) que serviram de alicerce para o modelo proposto.

4. **Relevância estratégica para o País**
   A proposta alinha-se ao Plano Nacional de Segurança de Infraestruturas Críticas (PLANSIC) e fornece subsídios imediatos para o aprimoramento do Anexo I do PPSI, documento hoje utilizado por tribunais de contas e pelos ministérios na avaliação de sistemas sensíveis.
   Ao permitir a correta hierarquização de ativos, o modelo pode potencializar a alocação de verbas públicas em controles que realmente reduzem riscos sistêmicos – tema particularmente urgente diante do crescimento estimado do cibercrime para US$ 10,5 tri até 2025.

5. **Benefícios sociais e econômicos esperados**
   Redução do tempo médio de resposta a incidentes em órgãos federais, uma vez que prioriza-se a continuidade dos serviços que suportam funções vitais.
   Uso mais eficiente de contratos de tecnologia, pois evita duplicidade de investimentos em sistemas de baixa relevância estratégica.

Em síntese, esta dissertação convida o leitor a internalizar não apenas a urgência do problema, mas também os ganhos concretos advindos de uma abordagem criteriosa, baseada em evidências e adaptada à realidade nacional. Ao propor um modelo hierárquico, espera-se contribuir para que o Brasil migre de ações reativas para uma estratégia proativa de proteção das infraestruturas que sustentam a vida moderna.

1.2 PROBLEMA DE PESQUISA

Como desenvolver e estruturar um modelo hierárquico de critérios e subcritérios, alinhado às necessidades e especificidades do contexto brasileiro, que possibilite a aplicação efetiva de métodos multicritério

para identificar e classificar sistemas de infraestruturas críticas, proporcionando maior transparência, coerência e eficiência na alocação de recursos e na adoção de medidas de segurança?

1.3 OBJETIVOS

1.3.1 Objetivo Geral

Propor um modelo hierárquico de critérios aplicável a avaliação das infraestruturas críticas brasileiras, com base na análise de metodologias internacionais e no modelo proposto pelo Programa de Privacidade e Segurança da Informação (PPSI), visando uma aplicação mais eficiente em órgãos governamentais.

1.3.2 Objetivos Específicos

1. Investigar os critérios adotados por países e organizações internacionais para a definição de infraestruturas críticas.

2. Analisar os critérios do modelo de criticidade de sistemas proposto pelo PPSI, comparando-o com outras metodologias globais.

3. Desenvolver um modelo hierárquico utilizando os critérios identificados na literatura e no modelo do PPSI.

4. Comparar as principais características e diferenças entre o modelo PPSI e o modelo hierárquico de critérios e subcritérios proposto para avaliação de infraestruturas críticas.

1.4 RESULTADOS ESPERADOS

Espera-se que o modelo hierárquico de critérios e subcritérios desenvolvido nesta dissertação contribua de maneira significativa para o aprimoramento das práticas de avaliação de criticidade adotadas por órgãos públicos e setores estratégicos no Brasil. Como referência conceitual, o modelo sintetiza metodologias internacionais e adapta recomendações do Programa de Privacidade e Segurança da Informação (PPSI), oferecendo uma estrutura metodológica, sistematizada e alinhada ao contexto regulatório e operacional brasileiro.

Entre os principais resultados esperados, destacam-se:

- **Base metodológica para avaliações futuras:** O modelo proposto poderá ser capaz de orientar a realização de avaliações mais consistentes e reproduzíveis de sistemas críticos, tanto em processos internos de ministérios, tribunais, autarquias e demais órgãos federais, quanto como apoio a futuras iniciativas normativas e regulatórias. Espera-se que ele seja utilizado, por exemplo, em revisões periódicas do Anexo I do PPSI e em processos de auditoria ou fiscalização conduzidos por órgãos de controle.

- **Padronização conceitual:** Ao organizar e classificar critérios e subcritérios de modo estruturado, o modelo pode favorecer a padronização dos processos de identificação e classificação de ativos críticos no âmbito do setor público, reduzindo divergências interpretativas e promovendo maior transparência e coerência na análise de riscos.
- **Subsídio para decisões estratégicas:** Espera-se que a implementação do modelo contribua para decisões mais fundamentadas e eficientes na alocação de recursos, priorização de ações de segurança e definição de controles em ambientes de recursos limitados e ameaças crescentes.
- **Estímulo à integração entre áreas:** O modelo pode fomentar o diálogo interdisciplinar entre as áreas de tecnologia, gestão de riscos, auditoria e governança, promovendo uma visão holística sobre criticidade e incentivando a atuação coordenada nos diferentes níveis da administração pública.
- **Potencial de replicação e adaptação:** Espera-se que a estrutura desenvolvida nesta dissertação seja suscetível de replicação e adaptação em contextos estaduais, municipais e em setores privados que enfrentam desafios análogos na avaliação de infraestruturas críticas.
- **Contribuição científica e inovação:** O detalhamento metodológico e a síntese comparativa internacional apresentada na dissertação podem ampliar o acervo científico sobre avaliação de criticidade em infraestrutura crítica, servindo de referência para pesquisadores, profissionais de segurança e gestores de projetos estratégicos.
- **Facilitação de treinamento e disseminação:** O modelo poderá ser incorporado em programas de capacitação para servidores públicos e gestores de ativos críticos, podendo apoiar políticas de formação contínua e disseminação de boas práticas em cibersegurança e gestão de riscos.

Por fim, reconhece-se que a adoção do modelo demandará esforço de internalização e ajuste por parte dos órgãos interessados, inclusive no que se refere à sensibilização e à ampliação do entendimento sobre sua aplicabilidade. Todavia, espera-se que a estrutura proposta promova ganhos de eficiência, assertividade e maturidade institucional no tratamento do tema, com impactos positivos a médio e longo prazo para a resiliência das infraestruturas críticas e para a governança de segurança da informação no país.

1.5 PUBLICAÇÕES RESULTANTES DESTA PESQUISA

As publicações decorrentes do desenvolvimento desta dissertação estão organizadas, a seguir, em duas categorias: (i) publicações diretamente relacionadas à pesquisa e (ii) publicações indiretas — estas correspondem a trabalhos publicados no período em colaboração com o grupo de pesquisa, mas cuja relação é de apoio metodológico, temático ou de contexto ampliado.

1.5.1 Publicações diretamente relacionadas à dissertação

- DA Silva, E. G., Georg, M. A. C., Júnior, L. A. R., Ferreira, L. R., de Melo, L. P., & Nunes, R. R. (2025). International Perspectives on Critical Infrastructure: Evaluation Criteria and Definitions. *International Journal of Critical Infrastructure Protection*, 100761.

- DA Silva, E. G., Moreira, F. R., Georg, M. A. C., dos Santos, R. R., Ribeiro Júnior, L. A., & Nunes, R. R. (2025). Binary Decision Support Using AHP: A Model for Alternative Analysis. *Algorithms*, 18(6), 320.

- DA SILVA, E. G.; GEORG, M. A. C.; RIBEIRO JUNIOR, L. A.; FERREIRA, L. R.; NUNES, R. R. Tomada de Decisão em Segurança Cibernética: Modelo para Identificação de Joias da Coroa. *Revista Ibérica de Sistemas e Tecnologias de Informação* (RISTI), 2025. (Aceito para publicação)

1.5.2 Publicações indiretamente relacionadas à pesquisa

- Silva, E. G.; Vieira, A. A. S.; Pires, L. A. S.; Albuquerque, R. O.; Nunes, R. R. Análise de Feeds de Inteligência de Ataques DDoS sob a Ótica da Qualidade da Informação. *Revista Ibérica de Sistemas e Tecnologias de Informação* (RISTI), 2024. (Qualis A4)

- Silva Camelo Paiva, Giovanna; Gomes da Silva, Edvan; André de Melo Alves, Carlos; Rabelo Nunes, Rafael. Aplicação da Lei Geral de Proteção de Dados Pessoais para agentes de tratamento de pequeno porte: análise em clínicas odontológicas. *NAVUS Revista de Gestão e Tecnologia*, 2024.

- Zottmann, Carlos Eduardo Miranda; Gondim, João J. C.; do Amaral, Thiago M. S.; Silva, E. G.; Nunes, Rafael Rabelo. Comparação de abordagens de proteção à cadeia de suprimento de software. *Revista Ibérica de Sistemas e Tecnologias de Informação* (RISTI), 2024. (Qualis A4)

- Silva, Jady Pamella Barbacena; Silva, Edvan Gomes; Ferreira, Lucas Vinícius Andrade; Nunes, Rafael Rabelo. Proteção Cibernética no Judiciário Brasileiro: Um Estudo Comparativo das Estruturas de Segurança em Tribunais Estaduais. *NAVUS Revista de Gestão e Tecnologia*, 2024.

- DA SILVA, E. G.; MOREIRA, F. R.; NZE, G. D. A.; GONDIM, J. J. C.; NUNES, R. R. Revisão Sistemática sobre Frameworks de Modelagem de Ameaças em Segurança Cibernética. *Revista Ibérica de Sistemas e Tecnologias de Informação* (RISTI), 2025. (Aceito para publicação)

Ressalta-se que as publicações diretamente relacionadas contribuíram ativamente para a formulação do modelo proposto, análise dos critérios e validação dos resultados da dissertação. As demais publicações, embora resultantes do processo de desenvolvimento acadêmico e atuação em grupo de pesquisa, serviram como suporte complementar, contextualização metodológica ou ampliação do escopo investigativo dentro da área de cibersegurança e proteção de ativos críticos.

2 REFERENCIAL TEÓRICO

Este capítulo tem como objetivo estabelecer a fundamentação teórica necessária para compreender os conceitos centrais desta pesquisa, bem como situar o trabalho no contexto da literatura científica existente. A estruturação do referencial teórico foi organizada de forma a apresentar, de maneira progressiva e interconectada, os principais constructos teóricos que sustentam a proposta de modelo hierárquico para avaliação de criticidade em infraestruturas críticas brasileiras.

Inicialmente, são abordados os fundamentos da gestão de ativos (seção 2.1), estabelecendo a base conceitual para compreender como os ativos organizacionais são identificados, classificados e priorizados. Em seguida, explora-se o conceito de criticidade e infraestruturas críticas (seção 2.2), apresentando as diferentes perspectivas e abordagens para avaliar a importância estratégica desses elementos. A seção 2.3 aprofunda a conceituação e os critérios utilizados internacionalmente para definir infraestruturas críticas, fornecendo o arcabouço conceitual necessário para a análise comparativa que será desenvolvida nos capítulos subsequentes.

O método multicritério AHP (Analytic Hierarchy Process) é apresentado na seção 2.4, detalhando sua fundamentação teórica e aplicabilidade para estruturação de problemas de decisão hierárquicos, método que inspirou a construção do modelo proposto nesta pesquisa. As seções 2.5 e 2.6 contextualizam o ambiente de aplicação da pesquisa, apresentando a estrutura do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) e a origem do modelo PPSI, respectivamente.

A seção 2.7 estabelece uma distinção clara entre o referencial teórico propriamente dito e os trabalhos relacionados. Enquanto as seções anteriores apresentam os fundamentos teóricos e conceituais que embasam esta pesquisa, a seção de trabalhos relacionados realiza uma análise comparativa com estudos similares, identificando lacunas, convergências e divergências na literatura científica sobre proteção de infraestruturas críticas. Esta diferenciação é fundamental para situar a contribuição original desta dissertação no contexto do conhecimento existente, evidenciando como a pesquisa avança em relação aos trabalhos predecessores e quais aspectos inovadores são propostos.

Por fim, a seção 2.8 apresenta o marco normativo nacional relativo à segurança de infraestruturas críticas no Brasil, destacando os principais decretos, estratégias e planos que norteiam a atuação do Estado brasileiro na identificação, proteção e gestão desses ativos essenciais. Esta seção oferece uma visão estrutural e institucional do cenário regulatório nacional, servindo como base para compreender as diretrizes e instrumentos oficiais — como o PLANSIC, ENSIC e E-Ciber — que orientam o desenvolvimento de políticas públicas de resiliência e segurança, e que também embasam a proposta metodológica desenvolvida ao longo desta dissertação.

2.1 GESTÃO DE ATIVOS

A cibersegurança aborda a proteção de computadores, servidores, dispositivos móveis, sistemas digitais, redes e dados contra uma variedade de ataques. Sua abrangência evoluiu para incluir aspectos adicionais, como infraestrutura, ativos de informação, pessoas e processos [15].

A gestão de ativos emerge como uma função fundamental para administrar os ativos críticos de negócio, concentrando-se nas questões mais relevantes e importantes [16]. Esta abordagem estratégica prioriza a identificação e classificação de ativos de acordo com sua criticidade, fornecendo a base para uma eficaz avaliação de vulnerabilidades [17].

A identificação de ativos é essencial e deve ser iniciada antes da identificação de qualquer risco. O objetivo da identificação de ativos é apontar e priorizar os ativos de acordo com seus níveis de criticidade na organização. A lista resultante de ativos e sua categorização são então utilizadas como entrada para a avaliação de riscos, o que permite identificar as vulnerabilidades e ameaças. Isso a torna o conhecimento dos ativos imprescindível para proteger contra ataques cibernéticos e a subsequente destruição [17].

Questionamentos sobre a natureza do que é considerado crítico e como classificar a criticidade de ativos refletem desafios similares aos enfrentados na aplicação de frameworks de gestão, já que não existe uma definição única que seja universalmente aplicável a todas as organizações. No que diz respeito à definição de ativos críticos, não há uma abordagem padronizada que seja universalmente aplicável [13].

Embora pareça simples, há visões diferentes sobre o que são ativos para organizações. O Framework do NIST estabelece que o resultado da gestão de ativos é identificar e gerenciar os dados, funcionários, dispositivos, sistemas e instalações que possibilitam à organização alcançar seus objetivos de negócio, considerando a sua importância relativa para os objetivos empresariais e a estratégia da organização [5]. Já a ISO 27.005:2023 propõe uma categorização de ativos em primários ou de suporte. Os ativos primários são os processos essenciais, atividades e informações, enquanto os ativos de suporte incluem hardware, software, rede, pessoal, local e estrutura [7].

A abordagem proposta pela ISO parece ser mais aceita quando se fala em infraestrutura crítica. Luiijf, Burger e Klaver [18] ressaltam a importância de uma abordagem top-down na determinação da infraestrutura crítica das nações quando enfatizam a necessidade de identificar as cadeias de processos essenciais – ativos primários - que garantem a prestação contínua de serviços vitais à nação. Faria [19] propõe a identificação de ativos por meio de uma lista de funções (ativos primários), para determinar as categorias de ativos e sistemas associados a cada função (ativos de suporte).

Trindade, et al. [20], em seu modelo para identificação da infraestrutura crítica no setor de telecomunicações, estabelecem que a identificação e definição dos serviços oferecidos devem ser consideradas na primeira etapa – ativos primários, enquanto a atividade de identificação da infraestrutura que suporta os serviços considerados críticos – ativos de suporte - é realizada apenas nas fases finais do processo.

Conforme o National Cyber Security Center [21], é essencial compreender a necessidade de negócio apoiada pelos dados e sistemas que você gerencia. A gestão de ativos abrange o processo de estabelecer e manter o conhecimento necessário sobre esses ativos. É importante compreender seus serviços e funções críticas e identificar as dependências de dados e tecnologia associadas para priorizá-las adequadamente.

Esse processo pode ser bem demorado, e para simplificá-lo, pode-se priorizar a identificação dos ativos mais críticos ou prioritários antes de abordar os menos críticos. Sem isso, pode-se chegar facilmente à conclusão de que o escopo definido é muito amplo, o que significa avaliar muitos ativos o que pode inviabilizar a tarefa. Nesse caso, é aconselhável retornar à etapa de definição de prioridades no âmbito da estratégia [19].

2.2 CRITICIDADE EM INFRAESTRUTURAS CRÍTICAS

Uma infraestrutura crítica é definida como um serviço, instalação ou grupo de serviços ou instalações, cuja perda terá efeitos adversos graves no bem-estar físico, social, econômico ou ambiental ou na segurança da comunidade [22]. A proteção dessas infraestruturas demanda a avaliação de sua criticidade e a priorização dos ativos considerados críticos. Contudo, a análise de criticidade ainda carece de um padrão estabelecido. A maioria dos métodos enfoca as consequências de um evento, ou seja, o resultado de uma situação ou evento expresso qualitativa ou quantitativamente.

Avaliar a importância ou criticidade das infraestruturas é uma etapa essencial para a implementação de estratégias de proteção eficazes, como o reforço da segurança em locais específicos cuja interrupção resultaria em consequências particularmente graves [23]. Conforme apontado por Fekete [24], a avaliação da criticidade das infraestruturas suscita duas questões importantes: quais são os aspectos em que dependemos delas e quais seriam os impactos em caso de falha? Uma infraestrutura é considerada "crítica"quando sua interrupção resulta em disrupções significativas no funcionamento da sociedade, como destacado pelo Federal Ministry of the Interior of Germany [25].

O critério-chave para essa avaliação é a importância da infraestrutura no fornecimento de bens e serviços essenciais [25]. A maioria das abordagens de avaliação identifica elementos de risco ou processos que possuem grandes capacidades de fornecimento. Alguns estudos classificam certas infraestruturas como críticas, importantes ou até vitais [18].

De acordo com a Comissão Europeia [26], os limites dos critérios devem ser estabelecidos com base na gravidade do impacto resultante da interrupção ou destruição de uma infraestrutura específica, e esses limites exatos devem ser definidos caso a caso pelos Estados-Membros envolvidos em uma infraestrutura crítica específica. Durante a análise de riscos, observa-se que alguns dos riscos avaliados são baseados em tipos de impacto que não estão associados ao nível de criticidade de um sistema.

A criticidade pode ser considerada como um subconjunto do risco, sendo o impacto o elemento de conexão básico entre ambos. No entanto, para uma compreensão mais abrangente de como a análise de riscos pode ser aplicada na avaliação das Infraestruturas Críticas, é necessário considerar outras questões, como ressaltado por Theoharidou, Kotzanikolaou e Gritzalis [27]. Além disso, há diversos tipos de impacto, como mortalidade, ferimentos em pessoas, danos econômicos e perda de imagem, entre outros.

Nas infraestruturas críticas, as vulnerabilidades podem ser exploradas por uma ampla gama de agentes, incluindo fatores humanos, desastres naturais e, mais recentemente, sistemas autônomos baseados em inteligência artificial (IA) [28]. Esses sistemas, embora desenvolvidos por humanos, podem tomar decisões de forma autônoma, o que introduz um novo vetor de risco que não se enquadra exclusivamente nas categorias

tradicionais de ameaça natural ou humana.

Devido às potencialmente catastróficas consequências de falhas ou interrupções, é essencial planejar medidas de proteção robustas [11]. A criticidade dessas infraestruturas pode ser avaliada a partir das capacidades decisivas necessárias para prevenir, mitigar ou compensar impactos negativos, como sintetizado no modelo dos 4Rs da resiliência — robustez, redundância, recursos e rapidez — conforme proposto por Tierney e Bruneau [29].

O conceito por trás de uma avaliação de criticidade é semelhante a uma avaliação de risco típica. Especialmente para avaliações de infraestruturas críticas, no entanto, certos ajustes são necessários:

1) Apenas os impactos decorrentes de danos ou falhas na infraestrutura são considerados, não os impactos diretos de ameaças, como funcionários mortos por raios.

2) Os efeitos externos fora da área da ameaça são importantes. Por exemplo, uma inundação na região X pode afetar o fornecimento de energia na região Y.

3) As interdependências e os efeitos em cascata que levam a diferentes pontos de entrada de impacto devem ser avaliados [24].

Outro aspecto relevante é a ausência de um padrão na análise de criticidade. A maioria das documentações sobre Estratégias Nacionais para Proteção de Infraestruturas Críticas foi publicada no início dos anos 2000 e, em grande parte, não passou por atualizações significativas nos últimos anos.

2.3 CRITÉRIOS DE AVALIAÇÃO DE INFRAESTRUTURAS CRÍTICAS

A proteção das Infraestruturas Críticas (IC) como política pública autônoma ganhou destaque após a criação da Comissão de Proteção de Infraestruturas Críticas (CPIC) em 1996, por iniciativa do presidente Bill Clinton. O relatório "Critical Foundations"de 1997 solidificou as IC como uma questão de segurança nacional [30]. Os ataques de 11 de setembro de 2001 às Torres Gêmeas nos EUA marcaram um ponto importante, motivando uma revisão da abordagem de proteção física destas infraestruturas [31].

Na União Europeia (UE), a atenção para com as IC intensificou-se após os atentados de Madrid em março de 2004. Em junho do mesmo ano, o Conselho Europeu solicitou a elaboração de uma estratégia para a Proteção de Infraestruturas Críticas (PIC), que foi formalizada pela Diretiva 2008/114/CE, estabelecendo uma definição comum europeia para o conceito [32].

O conceito de IC é dinâmico e evolutivo, adaptando-se conforme as necessidades e peculiaridades de cada localidade. Por exemplo, as Infraestruturas Críticas são classificadas em setores como energia, água, telecomunicações, entre outros, onde a definição de quais processos são considerados críticos varia significativamente [33][34]. Netherlands National Coordinator for Counterterrorism and Security [35] enfatiza a importância de concentrar esforços nos processos críticos ao invés de setores inteiros.

A UE e outros organismos enfatizam a necessidade de desenvolver metodologias que levem em conta a criticidade e a interdependência das infraestruturas para identificar quais devem receber proteção prioritária [6][32]. A delimitação de infraestruturas críticas baseia-se na extensão geográfica afetada e no impacto

ambiental, público, político ou econômico. A identificação das interdependências entre infraestruturas é fundamental para priorizar as medidas de proteção [36].

Para aprofundar a compreensão dos diferentes enfoques adotados na avaliação de infraestruturas críticas, apresenta-se a seguir a tabela 2.1 que compara os critérios de criticidade sob diversas perspectivas. Essa sistematização torna evidente como diferentes atores — autoridades, operadores, seguradoras e a sociedade em geral — valorizam aspectos específicos durante situações de crise, o que reforça a necessidade de modelos abrangentes para análise e classificação dessas infraestruturas no contexto da pesquisa.

Tabela 2.1: Critérios baseados nas diferentes perspetivas [36]

Atores	**Situação de crise**	**Critérios de criticidade**
Autoridades nacionais e tomadores de decisão	Incapacidade de garantir os interesses nacionais, a segurança dos cidadãos, a continuidade do governo, gerando perda de confiança no poder e uma crise política.	Defesa nacional, Segurança da economia nacional, Saúde e segurança públicas, Moral da nação
Proprietários de infraestruturas e ativos	Incapacidade de fornecer um serviço com confiabilidade qualitativa e quantitativa, gerando perdas econômicas, perda de competitividade e perda da confiança dos clientes.	Confiabilidade técnica e de serviço, Competitividade do serviço, Continuidade dos negócios
Seguradoras	Incapacidade de fornecer fundos de seguro em caso de danos muito caros, gerando uma interrupção econômica na companhia de seguros.	Sustentabilidade da companhia de seguros, Continuidade dos negócios
Outros interessados e o público em geral	Disrupção de serviços, invalidando a contínua e confiável realização das atividades diárias e ameaçando os padrões de bem-estar econômico e de vida.	Continuidade do serviço de acordo com o grau de dependência.

De acordo com Bouchon [36] , a criticidade de uma infraestrutura depende da perspectiva do analista, resultando em múltiplas perspectivas de acordo com as preocupações principais de cada entidade. Os critérios para a classificação das IC são diversificados e aplicados distintamente em diferentes países, refletindo uma variedade de abordagens para o problema.

No entanto, cabe ressaltar que a literatura e as práticas internacionais analisadas nesta dissertação demonstram a existência de uma convergência substancial quanto aos grandes eixos de avaliação — como impactos sociais, econômicos e em serviços essenciais, além das interdependências entre setores críticos. Isso indica que, ainda que haja nuances contextuais e adaptações nacionais, o processo decisório do analista tende a ser balizado por diretrizes consolidadas e critérios aceitos globalmente, reduzindo a subjetividade e prevenindo escolhas arbitrárias.

Portanto, a definição dos critérios de criticidade não se dá de modo meramente individual ou circuns-

tancial, mas resulta de um alinhamento progressivo com referenciais normativos e metodológicos reconhecidos internacionalmente, conforme evidenciado pela comparação feita entre os países estudados em capítulos posteriores da dissertação.

Moteff [37] destaca que os critérios de criticidade servem como ferramentas essenciais para evitar que as listas de IC se tornem excessivamente extensas, facilitando uma concentração mais eficaz nos esforços de proteção. A classificação das IC, portanto, varia entre entidades de um mesmo grupo, como organizações ou países, de acordo com os critérios estabelecidos.

2.4 MÉTODO MULTICRITÉRIO AHP

Um tomador de decisão, impulsionado pela necessidade de prever ou controlar resultados, frequentemente enfrenta sistemas complexos compostos por componentes inter-relacionados, como recursos, metas, pessoas ou grupos. O foco principal está na análise detalhada desse sistema, partindo do pressuposto de que uma compreensão mais profunda da complexidade envolvida resultará em previsões e decisões mais precisas [38].

Saaty [39] acrescenta que os valores sociais em nossa sociedade complexa exigem um método conveniente de escalonamento para a tomada de decisões, permitindo a avaliação diária das compensações entre dinheiro, qualidade ambiental, saúde, felicidade e outras entidades similares. Essa abordagem deve facilitar a interação entre o julgamento e os fenômenos sociais aos quais é aplicada. Precisamos desse método porque não existem escalas de medição social amplamente utilizadas, apesar das diversas tentativas nas ciências sociais de estabelecer uma base para uma teoria de medição.

O método AHP (Analytic Hierarchy Process) desenvolvido pelo Professor Thomas Saaty em 1980 permite estruturar a decisão de forma hierárquica (para reduzir sua complexidade) e mostrar as relações entre os objetivos (ou critérios) e as possíveis alternativas. Talvez a maior vantagem deste método seja a inclusão de intangíveis, como experiência, preferências subjetivas e intuição, de maneira lógica e estruturada [40].

O AHP tornou-se amplamente popular na pesquisa devido à sua utilidade superior em comparação com outros métodos. Ele integra abordagens qualitativas e quantitativas em uma única investigação empírica [41]. O desenvolvimento do AHP foi motivado pela necessidade de alocação eficiente de recursos escassos e pelo planejamento estratégico no contexto militar [39].

O AHP consiste em três etapas: (1) formação da hierarquia - o primeiro nível contém o objetivo da decisão, e os níveis subsequentes incluem critérios, subcritérios e alternativas Figura 2.1; (2) comparações paritárias - especialistas comparam elementos em cada nível da hierarquia através de uma escala numérica de Saaty (de 1 a 9) Tabela 2.2; (3) verificação da consistência - necessária para garantir a importância relativa dos critérios e alternativas, assegurando um resultado otimizado, dado que o AHP permite julgamentos subjetivos [42].

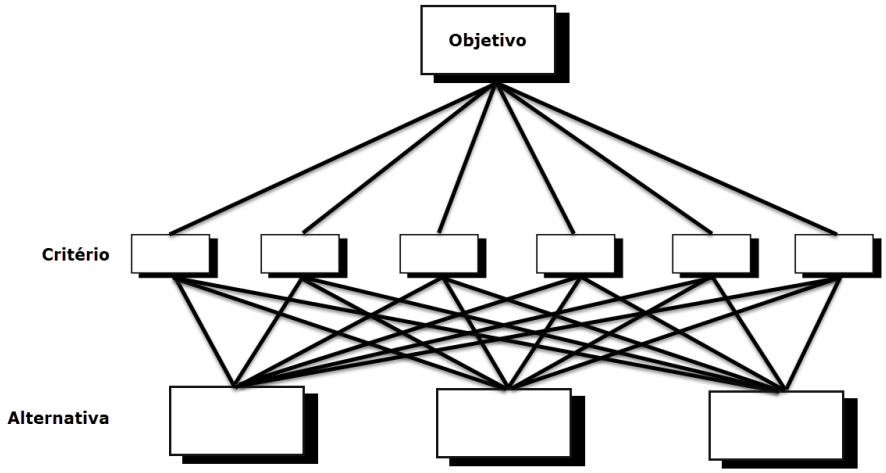


Figura 2.1: Hierarquia de três níveis [43]

Tabela 2.2: Escala Numérica de Saaty [44]

Intensidade da importância	**Definição**	**Explicação**
1	Igual importância	Ambos elementos contribuem com a propriedade de igual forma
3	Moderada importância de um elemento sobre o outro	A experiência e a opinião favorecem um elemento sobre o outro
5	Forte importância de um elemento sobre o outro	Um elemento é fortemente favorecido
7	Importância muito forte de um elemento sobre o outro	Um elemento é muito fortemente favorecido sobre o outro
9	Extrema importância de um elemento sobre o outro	Um elemento é favorecido pelo menos com uma ordem de magnitude de diferença
2, 4, 6, 8	Valores intermediários entre opiniões adjacentes	Usados como valores de consenso entre as opiniões

Além disso o AHP coleta opiniões de especialistas ou tomadores de decisão e possui duas vantagens principais. Primeiro, ele adota um processo de comparações paritárias, comparando dois objetos de cada vez para formular um julgamento sobre seu peso relativo. Segundo, com uma medição adequada, este método é mais preciso (com menos erro experimental) e atinge um nível mais alto de consistência, pois exige que os respondentes pensem com precisão antes de fornecer suas respostas. Geralmente, quanto mais uma pessoa conhece sobre uma situação, mais consistentes são os resultados esperados dessa pessoa [44].

Saaty [45] menciona que, para controlar a consistência das comparações paritárias, deve-se calcular a razão de consistência. Nesta etapa, os tomadores de decisão precisam revisar seus julgamentos iniciais se a razão de consistência calculada exceder o limite de 0,1. Após todas as comparações paritárias necessárias

e as revisões terem sido feitas, e a razão de consistência ser menor que 0,1, os julgamentos podem ser sintetizados para priorizar os critérios de decisão juntamente com seus subcritérios correspondentes. Os passos a seguir conduzem ao cálculo do índice de consistência:

$$\lambda_{\text{Max}} = \sum_{j=1}^{n} T_j \times P_j \quad (1)$$

$$CI = \frac{\lambda_{\text{Max}} - n}{n-1} \quad (2)$$

$$CR = \frac{CI}{RI} \quad (3)$$

Onde:

T_j: somatório da coluna j da matriz de julgamento

P_j: prioridade calculada para o critério localizado na linha j

RI: Random Index ou índice randômico. A Tabela 2.3 mostra os RI's.

Tabela 2.3: Indices Randômicos [46]

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
R	0.0	0.0	0.5	0.9	1.1	1.2	1.3	1.4	1.4	1.4	1.5	1.5	1.5	1.5	1.5
I	0	0	8	0	2	4	2	1	5	9	1	8	6	7	9

2.5 ESTRUTURA DO SISTEMA DE ADMINISTRAÇÃO DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO (SISP)

Os órgãos participantes da pesquisa fazem parte do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), instituído pelo Decreto nº 7.579, de 11 de outubro de 2011. O SISP tem como principal objetivo organizar, controlar e coordenar os recursos de tecnologia da informação da administração direta, autárquica e fundacional do Poder Executivo Federal, garantindo um suporte adequado e eficaz às atividades governamentais [47].

O SISP é estruturado da seguinte forma:

Órgão Central: Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos, responsável pela coordenação geral das políticas de TI.

Órgãos Setoriais: Unidades responsáveis pela administração de TI nos Ministérios e na Presidência da República.

Comissão de Coordenação: Um grupo composto por representantes dos órgãos setoriais, presidido por um representante do Órgão Central.

Órgãos Seccionais: Unidades que administram os recursos de TI em autarquias e fundações.

Órgãos Correlatos: Unidades formalmente constituídas para gerenciar os recursos de TI em órgãos setoriais e seccionais.

Objetivos do SISP:

Assegurar ao Governo Federal um suporte de TI adequado, confiável e dinâmico.

Promover a integração e articulação entre programas de governo, projetos e atividades para definição de políticas e diretrizes relacionadas à gestão de TI.

Estimular o uso racional dos recursos de TI, buscando melhorar a qualidade e produtividade do ciclo de informação no âmbito federal.

A estrutura e os objetivos do SISP refletem a importância estratégica da tecnologia da informação no funcionamento da administração pública brasileira, sendo essencial para garantir a continuidade dos serviços governamentais e a proteção de sistemas críticos de informação. Os sistemas listados nesta pesquisa foram consolidados com a colaboração dos órgãos do SISP, que desempenharam um papel essencial na identificação e priorização dos ativos tecnológicos de maior relevância [47].

2.6 ORIGEM E ADAPTAÇÃO DO MODELO PPSI

O modelo proposto pelo PPSI é uma adaptação do modelo originalmente desenvolvido pelo Tribunal de Contas da União (TCU), conforme delineado no Acórdão 1.889/2020-TCU-Plenário, cujo objetivo era realizar o levantamento de riscos em sistemas informacionais da Administração Pública Federal (APF). A adaptação do modelo do TCU permitiu ao PPSI incorporar critérios mais específicos voltados à segurança da informação e gestão de privacidade, ajustando-o para atender às necessidades de avaliação de sistemas críticos em diversas infraestruturas governamentais .

2.7 TRABALHOS RELACIONADOS

Embora a literatura sobre avaliação de infraestruturas críticas seja extensa, observa-se uma escassez de pesquisas que proponham modelos de decisão hierárquicos adaptados ao contexto nacional e alinhados a critérios internacionalmente reconhecidos. Modelos multicritério, em especial o Analytic Hierarchy Process (AHP), são raramente empregados nesse domínio, o que evidencia o caráter inovador deste trabalho. Esta dificuldade não é trivial: a definição de critérios, subcritérios e sua hierarquização exige aprofundamento conceitual e metodológico, sendo insuficiente recorrer apenas a listas genéricas encontradas na literatura.

A proteção das infraestruturas críticas (ICs) tem se tornado uma área de crescente interesse devido à sua importância estratégica para a segurança e o funcionamento das sociedades modernas. No trabalho de Moteff et al. (2003), as infraestruturas críticas são definidas como aquelas cujo colapso pode gerar impactos severos na economia, segurança nacional e na vida dos cidadãos. Esse conceito é fundamental para as políticas de proteção, especialmente no que tange à necessidade de priorizar quais infraestruturas

devem receber maior proteção, alinhando-se com a metodologia de avaliação de criticidade discutida nesta pesquisa [37].

O estudo de Myriam Dunn [34] aborda a dimensão sociopolítica da proteção de infraestruturas críticas, enfatizando que as decisões sobre segurança não se limitam apenas a fatores técnicos, mas também às implicações políticas e sociais. Ela ressalta que a infraestrutura informacional crítica (IIC) se sobrepõe a outros sistemas de ICs, criando um efeito multiplicador de vulnerabilidades. Este conceito está diretamente relacionado à esta pesquisa que também explora como diferentes tipos de interdependências entre sistemas podem aumentar a criticidade e a vulnerabilidade.

Ferreira [48], ao analisar a metodologia de identificação e caracterização de ICs em Portugal, propõe a criação de critérios e indicadores para priorizar a proteção dessas infraestruturas. Sua abordagem metodológica reforça a ideia de que a proteção de ICs deve ser personalizada de acordo com as especificidades nacionais, algo que também é discutido nesta pesquisa ao aplicar o modelo multicritério AHP em sistemas brasileiros. Essa personalização torna-se essencial para uma gestão eficaz das ICs.

Iturriza et al. [49] analisam metodologias de modelagem que avaliam as interdependências entre infraestruturas críticas, destacando como falhas em uma infraestrutura podem rapidamente afetar outras interconectadas. O estudo discute o uso de modelos baseados em dinâmicas de sistemas e agentes para simular os efeitos em cascata, permitindo uma melhor compreensão das vulnerabilidades e otimização de políticas de resposta a crises. Este trabalho complementa a presente pesquisa ao fornecer uma visão mais detalhada de como as interdependências entre infraestruturas podem agravar o impacto de eventos disruptivos e, assim, contribuir para a priorização de sistemas críticos.

Outro aspecto relevante é a análise da evolução das políticas de proteção das ICs, conforme discutido no estudo de Ferreira [48]. A implementação de políticas de proteção deve ser adaptada ao contexto específico de cada país, utilizando critérios que avaliem não apenas a criticidade, mas também as interdependências entre os sistemas. Este alinhamento entre políticas e critérios de avaliação é importante para o desenvolvimento de um modelo eficaz de proteção [48].

Por fim, Moteff et al. [37] destacam as dificuldades em definir de forma estática o que constitui uma Infraestrutura Crítica (IC), já que essa classificação pode variar ao longo do tempo e conforme o contexto geopolítico. Esse desafio é igualmente abordado nesta pesquisa, especialmente na análise dos critérios adotados por diferentes países para identificar infraestruturas críticas, considerando as variáveis contextuais e as necessidades específicas de cada região.

2.8 MARCO NORMATIVO NACIONAL DE SEGURANÇA DE INFRAESTRUTURAS CRÍTICAS

O arcabouço regulatório brasileiro sobre infraestruturas críticas (IC) consolidou-se ao longo da última década e fornece o pano de fundo institucional que sustenta esta pesquisa. A seguir apresentam-se os instrumentos centrais, em ordem cronológica, com ênfase nos conceitos, objetivos e setores priorizados.

Guia de Referência para a Segurança das Infraestruturas Críticas da Informação (GSI/PR, 2010). Publicado pelo Gabinete de Segurança Institucional, o documento foi o primeiro esforço técnico brasileiro dedicado a delinear *Infraestruturas Críticas da Informação* (ICI). Ele propõe metodologia de mapeamento de ativos, ciclos de gestão de riscos e requisitos mínimos de segurança (disponibilidade, integridade, confidencialidade e autenticidade) para órgãos da Administração Pública Federal[50]. O Guia influenciou os conceitos de *serviço essencial* e de *interdependência* adotados posteriormente na esfera normativa.

Política Nacional de Segurança de Infraestruturas Críticas – PNSIC. Instituída pelo Decreto n.º 9.573/2018, a PNSIC define IC como *"instalações, serviços, bens e sistemas cuja interrupção ou destruição provoque sério impacto social, ambiental, econômico, político ou à segurança nacional"*[51]. O texto fixa seis objetivos estratégicos, entre eles a prevenção de interrupções, o desenvolvimento de consciência nacional sobre IC e a integração de dados de ameaças.

Estratégia Nacional de Segurança de Infraestruturas Críticas – ENSIC. Apropriada pelo Decreto n.º 10.569/2020, a ENSIC operacionaliza a PNSIC ao detalhar eixos, metas e indicadores de desempenho[52]. Os eixos estruturantes incluem: (i) governança e articulação institucional; (ii) gestão de riscos e resiliência; e (iii) desenvolvimento de capacidades, pesquisa e inovação. A ENSIC reforça a necessidade de listas setoriais de IC e de exercícios de simulação multiagência.

Plano Nacional de Segurança de Infraestruturas Críticas – PLANSIC. Aprovado pelo Decreto n.º 11.200/2022, o PLANSIC converte a ENSIC em ações concretas, distribuídas em curto, médio e longo prazos[53]. Ele confirma os seguintes **setores prioritários**: comunicações, energia, transportes, finanças, água, defesa, saúde e tecnologia da informação, além de prever grupos técnicos no âmbito da Câmara de Relações Exteriores e Defesa Nacional para revisar periodicamente essa lista. Também institui métricas de maturidade e designa o GSI/PR como órgão coordenador.

Estratégia Nacional de Segurança Cibernética – E-Ciber 2020. Embora focada em cibersegurança, a E-Ciber (Decreto n.º 10.222/2020) reconhece que a indisponibilidade de IC pode comprometer interesses vitais do Estado e determina que os setores críticos adotem políticas de proteção cibernética, gestão de riscos e resposta a incidentes [54]. O documento amplia o escopo da proteção ao destacar a convergência entre segurança física e lógica nos ambientes de IC.

3 CARACTERIZAÇÃO E JUSTIFICATIVA DO PROBLEMA DE PESQUISA

3.1 REVISÃO DA PROBLEMÁTICA ATUAL NA AVALIAÇÃO DA CRITICIDADE EM INFRAESTRUTURAS CRÍTICAS NO BRASIL

A avaliação criticidade de ativos em infraestruturas críticas (ICs) brasileiras permanece fragmentada, carente de uma metodologia consolidada que traduza, de forma coerente, as melhores práticas internacionais para o contexto nacional. Embora o Anexo I do Programa de Privacidade e Segurança da Informação (PPSI) represente um avanço institucional ao propor critérios para priorização de sistemas, sua adoção tem revelado limitações importantes: (i) inexistência de um arcabouço hierárquico padronizado que permita a comparação entre órgãos; (ii) ênfase em aspectos operacionais de vulnerabilidade em detrimento de critérios de impacto amplamente reconhecidos pela literatura e por normas como a CIP-002-1 da North American Electric Reliability Corporation (NERC), o Risk Management Framework do NIST e a ISO 27005:2023; e (iii) falta de mecanismos sistemáticos para alinhar a classificação nacional aos referenciais europeus (Diretiva 2008/114/CE) e norte-americanos (PPD-21).

Estudos comparativos realizados nesta dissertação evidenciam que países de referência convergem para modelos com cinco a sete grandes critérios (impactos humano, social, econômico, geográfico, ambiental e de interdependência), enquanto o PPSI distribui assertivas de forma não hierarquizada, dificultando a visão holística dos riscos (Seção 5.2). Além disso, o levantamento empírico em órgãos do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) demonstrou interpretações díspares dos mesmos critérios, comprometendo a padronização dos resultados de criticidade e, consequentemente, a priorização de investimentos em segurança cibernética.

3.2 DETALHAMENTO DO PROBLEMA DE PESQUISA

O parágrafo 1.2 da Introdução delineia a pergunta central: *"Como desenvolver e estruturar um modelo hierárquico de critérios e subcritérios, alinhado às necessidades e especificidades do contexto brasileiro, que possibilite a aplicação efetiva de métodos multicritério para identificar e classificar sistemas de infraestruturas críticas, proporcionando maior transparência, coe- rência e eficiência na alocação de recursos e na adoção de medidas de segurança?"*. A brevidade desse trecho, contudo, não explicita plenamente as consequências da ausência de um modelo robusto:

- **Riscos à continuidade de serviços essenciais**: a não uniformização dos critérios gera classificações inconsistentes, propiciando lacunas na resiliência operacional de setores como energia e telecomunicações.
- **Perda de alinhamento com boas práticas internacionais:**: a falta de uma metodologia formal-

mente adotada pelos órgãos brasileiros pode comprometer a incorporação de conhecimentos e experiências consolidadas globalmente, especialmente em contextos de interdependência sistêmica e ameaças cibernéticas sofisticadas.

- **Dificuldade de priorização e alocação eficiente de recursos**: existe o risco significativo de destinação inadequada dos recursos, com investimentos concentrados em sistemas de baixa criticidade enquanto ativos de maior impacto podem permanecer subfinanciados, evidenciando possíveis falhas na gestão estratégica do risco organizacional.

3.3 JUSTIFICATIVA E IMPLICAÇÕES PRÁTICAS

Frente a esse cenário, justifica-se a proposição de um modelo hierárquico de avaliação de ICs que:

1. **Integre critérios amplamente aceitos** (humano, social, econômico, ambiental, geográfico e interdependência), harmonizando-os com a realidade brasileira;
2. **Permita aplicação de métodos multicritério** (e.g., AHP) para gerar pontuações comparáveis entre órgãos, facilitando a governança centralizada de riscos cibernéticos;
3. **Ofereça rastreabilidade decisória**, evidenciando a ligação direta entre criticidade, priorização orçamentária e escolha de controles, mitigando o risco de subfinanciamento de ativos essenciais.

Do ponto de vista de gestão de ativos críticos, o modelo proposto viabiliza inventários unificados que mapeiam dependências cruzadas entre setores — por exemplo, demonstrando como a falha de um Sistema de Gestão de Energia impacta cadeias de abastecimento de água e processos judiciais eletrônicos. Em política pública, ele pode sustentar a atualização contínua do Plano Nacional de Segurança de Infraestruturas Críticas (PLANSIC), oferecendo métricas objetivas para a seleção de projetos estratégicos.

Em síntese, a adoção de um modelo hierárquico bem fundamentado representa um incremento de valor tangível para a modernização, alinhamento e resiliência das infraestruturas críticas brasileiras, posicionando o País em convergência com as melhores práticas internacionais e podendo promover eficiência na gestão de riscos.

4 METODOLOGIA

Este capítulo descreve de forma detalhada os procedimentos metodológicos adotados para o desenvolvimento desta pesquisa, evidenciando o rigor científico empregado na construção do modelo hierárquico proposto. A metodologia foi estruturada de forma sistemática e sequencial, garantindo a replicabilidade dos procedimentos e a validade dos resultados obtidos.

O capítulo inicia caracterizando a natureza da pesquisa (aplicada, exploratória e descritiva) e sua abordagem predominantemente qualitativa, justificando essas escolhas metodológicas em função dos objetivos propostos. Em seguida, são apresentadas as quatro etapas distintas que estruturam o desenvolvimento do estudo: identificação de definições e critérios de infraestruturas críticas (seção 4.1), análise documental e extração de critérios (seção 4.2), construção do modelo hierárquico de decisão (seção 4.3), e comparação metodológica para identificação das diferenças (seção 4.4).

Cada etapa metodológica é detalhadamente explicada, incluindo os procedimentos específicos adotados, as fontes de dados utilizadas, os critérios de seleção aplicados e as técnicas de análise empregadas. Particular atenção é dada à descrição dos métodos de coleta e tratamento dos dados, bem como aos instrumentos e ferramentas utilizados para garantir a sistematização e objetividade da análise. O capítulo também evidencia como as diferentes etapas se integram de forma coerente para responder ao problema de pesquisa formulado, demonstrando a adequação da abordagem metodológica aos objetivos estabelecidos.

Esta pesquisa é de natureza aplicada, com objetivos exploratórios e descritivos. Possui características exploratórias, pois visa aprimorar ideias e descobrir intuições, exigindo um planejamento flexível que considere diversos aspectos relacionados ao objeto de estudo [55]. Além disso, é descritiva, uma vez que consiste em investigações empíricas cujo principal propósito é delinear e analisar as características de fenômenos, avaliar programas e isolar variáveis principais ou chave [56].

A abordagem adotada é predominantemente qualitativa, buscando compreender e explorar "universos de significados, motivos, aspirações, crenças, valores e atitudes". Isso permite um mergulho mais profundo nas relações e fenômenos que não podem ser mensurados apenas pela operacionalização de variáveis [57].

Para assegurar uma avaliação sistemática e robusta dos critérios que podem compor um modelo hierárquico para a análise de infraestruturas críticas, esta pesquisa foi organizada em quatro fases distintas. Cada fase integra metodologias e ferramentas de análise complementares, desempenhando um papel fundamental desde a identificação dos critérios relevantes até a comparação entre o modelo proposto e o PPSI. A seguir, apresenta-se uma visão geral das quatro etapas que estruturam o desenvolvimento deste estudo:

Cada uma dessas etapas será detalhada nas subseções seguintes, conduzindo a um processo de tomada de decisão.

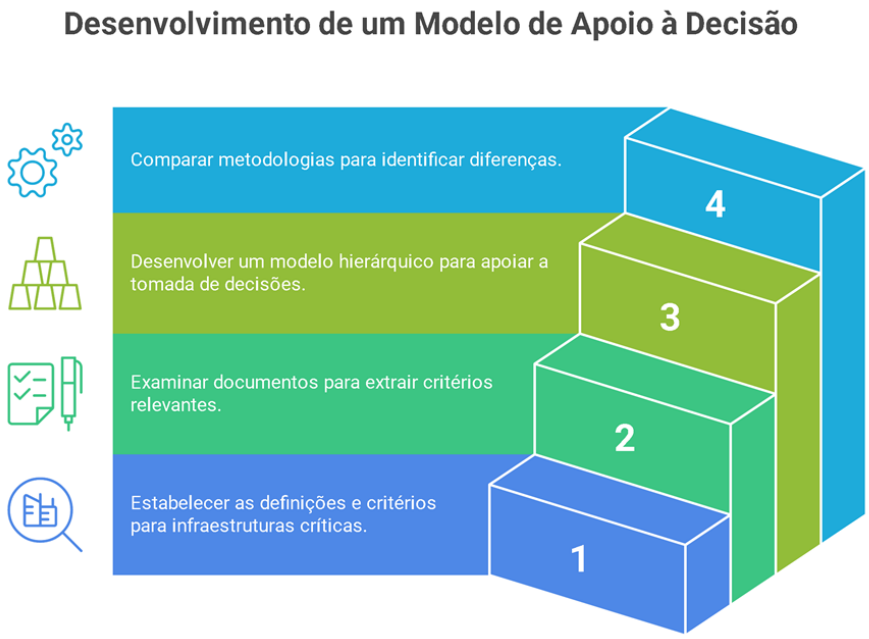


Figura 4.1: Etapas da Pesquisa

4.1 IDENTIFICAÇÃO DE DEFINIÇÕES E CRITÉRIOS DE INFRAESTRUTURAS CRÍTICAS

Nesta fase a pesquisa foi estruturada com o objetivo de identificar e destacar os pontos comuns presentes nas definições e nos critérios utilizados na análise de infraestruturas críticas. Para isso, foram analisadas exclusivamente as conceituações e os critérios de avaliação de infraestruturas críticas disponibilizados de forma completa por diversos países e organizações, incluindo: UE, Espanha, Portugal, Holanda, Reino Unido, Estados Unidos, Canadá, Austrália, Japão, Catar, Irlanda e Estônia.

Esta investigação está delimitada temporalmente ao período pós-ataques de 11 de setembro de 2001 até os dias de hoje. Assim, para a determinação da metodologia de identificação e caracterização de Infraestruturas Críticas, a análise será conduzida de acordo com os seguintes aspectos (A):

A1 – Definição de Infraestrutura Crítica: Este aspecto é considerado estruturante, pois a definição de infraestrutura crítica não é consensual entre as diversas organizações e países, refletindo as prioridades de cada um deles.

A2 – Critérios e Indicadores: Este aspecto determina a criticidade das infraestruturas e varia de país para país.

A3- Interdepêndencias: Este Aspecto expressa a posição e a preocupação em relação aos impactos tanto dentro dos próprios setores, quanto em outros setores ou em outros países

No contexto da Definição de Infraestrutura Crítica, foi conduzida uma análise detalhada dos componentes que constituem uma definição crítica. De acordo com Bouchon (2006), esses componentes são categorizados em Elementos, Condições e Critérios de Criticidade, conforme exemplos demonstrados na Tabela 3.1 .

Tabela 4.1: Elementos da definição de Infraestruturas Críticas [36]

Elementos	Condições	Critérios de criticidade
Recursos indispensáveis, Elementos vitais, Redes, Serviços, Ativos, Sistemas e ativos físicos ou virtuais, Instalações de TI, Redes de comunicação, Funções de suporte de TIC, Sistemas físicos e cibernéticos e Infraestruturas interdependentes.	Interrupção ou Destruição, A incapacidade ou destruição de tais sistemas e ativos, Se degradados ou indisponíveis por um período prolongado, Desabilitar qualquer um deles e Operação não contínua e confiável.	Grave impacto debilitante que incapacitaria elementos vitais essenciais para o sistema inteiro, saúde pública nacional, segurança, defesa nacional, segurança econômica, operações mínimas da economia, funcionamento eficaz do governo, bem-estar social ou econômico dos cidadãos ou da nação, qualidade de vida, ou qualquer combinação desses fatores.

Para aprimorar a visualização da análise, foram utilizadas nuvens de palavras para cada uma das categorias apresentadas. Os termos exibidos nas nuvens de palavras representam as principais palavras-chave empregadas pelos países para descrever suas definições de infraestruturas críticas.

A análise dos critérios foi conduzida utilizando estatística descritiva, visando classificar a ordem dos critérios com base em um rating de 12 pontos. A pontuação máxima é alcançada quando todos os 12 países e organizações avaliados utilizam o critério analisado.

4.2 ANÁLISE DOCUMENTAL E EXTRAÇÃO DE CRITÉRIOS

Nesta etapa, o método de análise empregado concentrou-se na avaliação documental com o objetivo de identificar e extrair os critérios descritos no Anexo 1 do PPSI. A análise documental foi realizada por meio de uma análise de conteúdo, que permitiu a categorização temática dos dados extraídos.

Elementos Extraídos:

Assertivas Utilizadas: Referem-se às questões elaboradas especificamente para a avaliação e priorização dos sistemas considerados críticos. Essas assertivas orientam o processo de avaliação, garantindo que aspectos relevantes sejam devidamente considerados.

Importante destacar que, para ampliar a abrangência e a relevância da análise, foi incorporada a avaliação do Tribunal de Contas da União (TCU) referente aos órgãos do SISP, a qual utilizou como base o Anexo 1 do PPSI. Dessa avaliação do TCU, foram acrescentadas três assertivas que não constavam no Anexo 1 original do PPSI, configurando um aporte adicional para o conjunto de questões analisadas.

Critérios: Os critérios foram agrupados e classificados de maneira subjetiva, com base nas assertivas estabelecidas no Anexo 1 do PPSI. Para mitigar a subjetividade, a classificação foi realizada por meio de

consenso entre os pesquisadores da Universidade de Brasília (UnB).

A análise detalhada desses elementos permite uma compreensão mais profunda do processo de priorização, fornecendo uma base sólida para a tomada de decisões em relação aos sistemas críticos

4.3 CONSTRUÇÃO DO MODELO HIERÁRQUICO DE DECISÃO

Com base nos critérios identificados na etapa anterior, será desenvolvido um modelo hierárquico de apoio à decisão, estruturando e organizando os critérios em diferentes níveis para facilitar a ponderação e a priorização durante o processo decisório. Essa abordagem visa reduzir a subjetividade, permitindo uma avaliação mais objetiva e transparente dos elementos envolvidos na classificação de infraestruturas críticas

O modelo hierárquico será composto por três níveis principais:

Nível 1 – Objetivo: Classificação das infraestruturas críticas.

Nível 2 – Critérios Principais: Resultantes da análise documental e da revisão de literatura.

Nível 3 – Subcritérios: Detalhamentos específicos vinculados a cada critério principal, permitindo maior granularidade na avaliação.

A adoção dessa estrutura hierárquica, inspirada em métodos multicritério como o AHP (Analytic Hierarchy Process), proporciona clareza e sistematização ao processo de tomada de decisão, tornando-o mais robusto e alinhado às melhores práticas de avaliação e priorização de ativos críticos

4.4 COMPARAR AS METODOLOGIAS E IDENTIFICAR AS DIFERENÇAS

Esta seção descreve o procedimento metodológico para comparar o modelo hierárquico proposto com o framework PPSI, com foco exclusivo na identificação, estruturação e categorização dos critérios, sem avançar para etapas de ponderação ou aplicação de pesos.

Objetivo da Comparação

O objetivo central desta etapa é analisar e comparar os critérios e a estrutura hierárquica adotados no modelo proposto em relação ao framework PPSI. Busca-se identificar convergências e divergências metodológicas, bem como possíveis pontos de aprimoramento, considerando as melhores práticas internacionais e o contexto brasileiro.

Procedimento de Comparação

A comparação será conduzida em duas frentes principais:

Análise das Diferenças Metodológicas: Inicialmente, será realizada uma análise detalhada das metodologias empregadas em ambos os modelos, concentrando-se na forma como os critérios são definidos, agrupados e hierarquizados. Serão identificados pontos de convergência (critérios comuns, abordagens similares de categorização) e de divergência (critérios exclusivos, diferenças na granularidade ou abran-

gência dos critérios, estrutura hierárquica adotada).

Identificação de Possíveis Melhorias: Em seguida, será avaliado como o modelo hierárquico proposto pode incorporar elementos positivos do framework PPSI, especialmente no que diz respeito à clareza na formulação das assertivas e à abrangência dos critérios. Da mesma forma, serão identificados aspectos do PPSI que podem ser aprimorados ou adaptados, considerando as recomendações da literatura internacional e a experiência de outros países na definição e categorização de infraestruturas críticas.

Escopo da Comparação

Vale ressaltar que, nesta pesquisa, a comparação limita-se à identificação e organização dos critérios e subcritérios, sem avançar para a etapa de atribuição de pesos ou aplicação prática do modelo. O foco está na construção do modelo hierárquico e na análise qualitativa das diferenças estruturais e conceituais entre as abordagens, fornecendo subsídios para futuras aplicações e aprimoramentos metodológicos.

5 RESULTADOS

Este capítulo apresenta os achados empíricos da pesquisa, organizados de forma lógica e sequencial para facilitar a compreensão dos resultados obtidos e sua interpretação. A estruturação dos resultados segue a mesma organização metodológica apresentada no capítulo anterior, evidenciando a coerência entre os procedimentos adotados e os produtos gerados.

A apresentação dos resultados inicia-se com uma ampla análise dos critérios e indicadores utilizados por diferentes países e organizações internacionais para avaliação de criticidade em infraestruturas críticas (seção 5.1). Esta seção oferece um panorama detalhado das práticas adotadas por doze jurisdições, incluindo União Europeia, Espanha, Portugal, Holanda, Reino Unido, Estados Unidos, Canadá, Austrália, Japão, Catar, Irlanda e Estônia, evidenciando tanto as convergências quanto as divergências nas abordagens metodológicas.

Subsequentemente, a seção 5.2 apresenta uma análise comparativa sistemática das definições de infraestruturas críticas e seus critérios, utilizando técnicas de categorização e análise de conteúdo para identificar padrões e diferenças significativas. A seção 5.3 aprofunda especificamente a questão das interdependências entre infraestruturas críticas, aspecto fundamental para compreender a complexidade desses sistemas.

A seção 5.4 consolida os achados anteriores na construção do modelo hierárquico proposto, detalhando o processo de análise documental do framework PPSI e demonstrando como os critérios identificados na literatura internacional foram estruturados em um modelo de hierarquização de decisão. Esta seção também apresenta uma análise comparativa detalhada entre o modelo proposto e o PPSI, identificando limitações e sugerindo melhorias para aprimoramento das práticas nacionais de avaliação de criticidade.

5.1 CRITÉRIOS E INDICADORES PARA AVALIAÇÃO DE CRITICIDADE UTILIZADOS PELAS NAÇÕES

5.1.1 União Européia

A1 – Definição de Infraestrutura Crítica:
Na UE, para a identificação e caracterização de Infraestruturas Críticas (IC), é importante visitar os conceitos europeus de IC e de Infraestruturas Críticas Europeias (ICE). Assim, uma IC é definida como:
Elemento, sistema ou parte deste situado nos Estados-Membros que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar econômico ou social, e cuja perturbação ou destruição teria um impacto significativo num Estado-Membro, dada a impossibilidade de continuar a assegurar essas funções [58].

> O conceito de Infraestruturas Críticas Europeias (ICE) considera a infraestrutura crítica localizada nos Estados-Membros, cuja perturbação ou destruição teria um impacto significativo em, pelo menos, dois Estados-Membros [58].

A2 – Critérios e Indicadores:

Para a União Europeia, existem duas tipologias de critérios: setoriais e transversais. Os critérios setoriais destinam-se a agrupar as Infraestruturas Críticas por afinidades funcionais. Os critérios transversais são utilizados para identificar impactos, comuns a todos os setores, em caso de perturbação ou destruição de uma Infraestrutura Crítica. Os indicadores são as formas pelas quais esses critérios são avaliados.

Tabela 5.1: Critérios Transversais (UE) [58]

Critério	**Indicador(es)**
Ocorrência de acidentes	Número potencial de feridos
	Número potencial de vítimas mortais
Impacto Econômico	Importância dos prejuízos econômicos
	Importância da degradação dos produtos ou serviços
	Potenciais Efeitos Ambientais
Efeitos no domínio público	Impacto na confiança das populações
	Sofrimento físico e perturbação da vida cotidiana
	Perda de serviços essenciais

No entanto, em 2004, antes dos critérios anteriormente apresentados, a União Europeia havia estabelecido outros critérios de avaliação de Infraestruturas Críticas, pois o foco na época era a proteção das infraestruturas críticas no âmbito da luta contra o terrorismo.

Tabela 5.2: Critérios Transversais (UE) [59]

Critério	**Indicador(es)**
Alcance	Extensão da área geográfica que pode ser afetada (internacional, nacional, provincial/territorial ou local)
Magnitude	O impacto no público (número de pessoas afetadas, perda de vidas, doença, prejuízos graves, evacuação)
	Os efeitos econômicos (impactos no PIB, importância das perdas econômicas e/ou degradação de produtos ou serviços)
	A incidência ambiental (impacto no público e em áreas vizinhas)
	A interdependência (em relação a outros elementos de infraestrutura crítica)
	Efeitos políticos (confiança na capacidade do governo)
Efeitos no Tempo	Imediato, 24-48 horas, uma semana, um mês, um ano, etc.

A3 – Interdepêndencias:

A questão das interdependências é fundamental para a União Europeia, manifestando-se não apenas dentro de setores específicos, mas também entre diferentes setores e atores estatais. Existem diversos exemplos de projetos europeus que evidenciam essas interdependências, como o Eurocontrol, o Galileo, a rede elétrica europeia e a rede europeia de gasodutos, que conecta os vários Estados-Membros. Esses quatro exemplos, inclusive, foram escolhidos como Infraestruturas Críticas para a implementação de uma nova estratégia voltada ao enfrentamento das interdependências [60].

5.1.2 Espanha

A1 – Definição de Infraestrutura Crítica:

Na Espanha, de acordo com o Centro Nacional de Proteção de Infraestruturas Críticas [61], as Infraestruturas Críticas (IC) são definidas como elementos essenciais para o funcionamento do Estado, da sociedade e dos cidadãos. Estas instalações proporcionam serviços essenciais à população, cujo funcionamento é indispensável e não possui soluções alternativas. Assim, a perturbação, interrupção ou destruição dessas instalações teria um grave impacto sobre os serviços essenciais. Outro conceito que auxilia na compreensão de como a Espanha define Infraestruturas Críticas (IC) é o de infraestruturas estratégicas. Estas são definidas como as instalações, redes, sistemas e equipamentos físicos e de tecnologia da informação sobre os quais repousa o funcionamento dos serviços essenciais [62].

A2 – Critérios e Indicadores:

Na Espanha, o Ministério do Interior, por meio da Secretaria de Estado de Segurança, é responsável por classificar uma infraestrutura como estratégica e, se for o caso, como infraestrutura crítica ou infraestrutura crítica europeia, após a comprovação de que cumpre um ou mais dos critérios horizontais de criticidade [63]. Os critérios horizontais de criticidade são definidos como os parâmetros pelos quais se determinam a criticidade, a gravidade e as consequências da perturbação ou destruição de uma infraestrutura crítica, e com base nos quais devem ser avaliados [62].

Tabela 5.3: Critérios Horizontais (Espanha) [62]

Critério	**Indicador(es)**
Número de pessoas afetadas	Número potencial de vitimas mortais
	Número potencial de feridos graves
	Consequências para a saúde pública
Impacto Econômico	Magnitude das perdas econômicas
	Deterioração de produtos e serviços
Impacto no meio ambiente	Degradação do local e arredores
Impacto público e social	Incidência na confiança da população
	Incidência na capacidade da Administração Pública
	Sofrimento físico e alteração da vida cotidiana
	Perda e grave deterioração dos serviços essenciais

A3 – Interdepêndencias:

De acordo com a Ley 8/2011, de 28 de abril [62], o conceito de interdependência refere-se ao conjunto de efeitos gerados por uma perturbação no funcionamento normal de uma infraestrutura ou serviço, que pode também impactar outras infraestruturas ou serviços. Conforme essa mesma legislação, as interdependências podem ocorrer tanto dentro de um mesmo setor quanto entre setores distintos. As consequências dessas inter-relações podem manifestar-se em níveis local, autonômico, nacional ou internacional.

5.1.3 Portugal

A1 – Definição de Infraestrutura Crítica:
Portugal define infraestruturas críticas como um componente, sistema ou parte deste situado em território nacional, que é essencial para a manutenção de funções vitais para a sociedade, saúde, segurança e bem-estar econômico ou social, e cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções [64].
A2 – Critérios e Indicadores:

Tabela 5.4: Critérios e Indicadores (Portugal) [64]

Critério	**Indicador(es)**
Número de pessoas afetadas	Número potencial de vítimas mortais)
	Número potencial de feridos graves
Impacto Econômico	Prejuízos Econômicos
	Degradação dos Serviços
	Efeitos Ambientais
Impacto no meio ambiente	Degradação do local e arredores
Impacto público e social	Confiança das Populações
	Sofrimento Físico e alteração da vida cotidiana
	Perda de Serviços Essenciais

A3 – Interdepêndencias:
A análise de interdependências é feita de forma transversal e pode alterar dados de criticidade estabelecidos pelos critérios e indicadores. Assim, uma infraestrutura, apesar de não ser considerada crítica, pode passar a sê-lo se dela depender uma que seja considerada crítica, independentemente do setor ou subsetor a que pertença [65].

5.1.4 Holanda

A1 – Definição de Infraestrutura Crítica:
Na Holanda, infraestrutura crítica é definida como processos que são extremamente críticos para a sociedade holandesa. A falha ou interrupção desses processos resultaria em uma grave perturbação social e representaria uma ameaça à segurança nacional. Esses processos, juntos, formam a infraestrutura crítica dos Países Baixos [35]. O Coordenador Nacional para Contraterrorismo e Segurança dos Países Baixos (2018a) complementa que o termo "setores críticos"foi utilizado no passado e, como nem todos os processos em um setor são críticos, o foco atual está nos processos críticos. Identificá-los permite o uso de ferramentas e recursos escassos de maneira mais eficiente e direcionada.

A2 – Critérios e Indicadores:
A avaliação de infraestruturas críticas na Holanda distingue duas categorias críticas, A e B. A falha de

processos críticos da categoria A tem efeitos potenciais maiores do que a falha de processos críticos da categoria B. Embora o conjunto de critérios seja quase o mesmo, exceto pelo critério de efeitos em cascata, os indicadores se diferem [66]. A Categoria A inclui infraestruturas cuja interrupção, dano ou falha atende a pelo menos um dos três critérios de impacto e ao critério de efeitos em cascata. Por outro lado, a Categoria B inclui infraestruturas cuja interrupção, dano ou falha atende a pelo menos um dos três critérios de impacto [24].

Tabela 5.5: Escala de Criticidade (Holanda) [66]

Categoria	**Indicador(es)**	**Critério**
A	Impacto Econômico	Aproximadamente €50 bilhões em danos ou uma queda de aproximadamente cinco por cento na renda real.
	Impacto Físico	Mais de 10.000 mortos, gravemente feridos ou doentes crônicos.
	Impacto Social	Mais de um milhão de pessoas afetadas por problemas emocionais ou sérios problemas de sobrevivência básica.
	Efeitos em cascata	A falha resulta na quebra de pelo menos dois outros setores.
B	Impacto Econômico	Aproximadamente €5 bilhões em danos ou uma queda de aproximadamente um por cento na renda real.
	Impacto Físico	Mais de 1.000 mortos, gravemente feridos ou doentes crônicos.
	Impacto Social	Mais de 100.000 pessoas afetadas por problemas emocionais ou sérios problemas de sobrevivência básica.

A3 – Interdepêndencias:
A questão das interdependências é fundamental para os Países Baixos, manifestando-se não apenas dentro de setores específicos, mas também entre diferentes setores e processos críticos. O Coordenador Nacional para Segurança e Contraterrorismo (NCTV) reconhece que "o impacto de incidentes envolvendo infraestrutura crítica, a velocidade dos desenvolvimentos tecnológicos, a mudança nas ameaças e ameaças cibernéticas e a crescente interdependência mútua da infraestrutura crítica necessita um foco permanente no aumento e salvaguarda de sua resiliência"[66].

5.1.5 Reino Unido

A1 – Definição de Infraestrutura Crítica:
No Reino Unido, o conceito de Infraestrutura Nacional (IN) antecede o conceito de Infraestrutura Nacional Crítica (INC), conforme descrito pelo Cabinet Office (2010) como sendo constituído por instalações, sistemas, locais e redes necessários para o funcionamento do país e para a prestação dos serviços essenciais de que depende a vida diária no Reino Unido [67]. O Cabinet Office (2010) acrescenta que determinados elementos "críticos"da infraestrutura nacional, cuja perda acarretaria graves consequências econômicas ou sociais, ou perda de vidas no Reino Unido, integram a Infraestrutura Nacional Crítica (INC), e que esses ativos podem ser tanto físicos quanto digitais [67].

A2 – Critérios e Indicadores:

O Reino Unido não identifica explicitamente critérios e indicadores para caracterizar as Infraestruturas Críticas. A infraestrutura é categorizada de acordo com seu valor ou "criticidade"e o impacto de sua perda. Essa categorização é realizada utilizando a "Escala de Criticidade"do governo, que atribui categorias conforme os diferentes graus de severidade do impacto. A Escala de Criticidade inclui três dimensões de impacto: impacto na prestação dos serviços essenciais da nação; impacto econômico (decorrente da perda de serviços essenciais); e impacto na vida (decorrente da perda de serviços essenciais) [67].

Tabela 5.6: Escala de Criticidade (RU)[67]

Escala	**Descrição**
Categoria 5	Esta é uma infraestrutura cuja perda teria um impacto catastrófico no Reino Unido. Esses ativos serão de importância nacional única, cuja perda teria efeitos nacionais de longo prazo e poderia afetar diversos setores. Espera-se que relativamente poucos atendam aos critérios da Categoria 5.
Categoria 4	A infraestrutura de máxima importância para os setores deve se enquadrar nesta categoria. O impacto da perda desses ativos nos serviços essenciais seria severo e poderia afetar a prestação de serviços essenciais em todo o Reino Unido ou a milhões de cidadãos.
Categoria 3	Infraestrutura de grande importância para os setores e a prestação de serviços essenciais, cuja perda poderia afetar uma vasta região geográfica ou muitas centenas de milhares de pessoas.
Categoria 2	Infraestrutura cuja perda teria um impacto significativo na entrega de serviços essenciais, resultando em perda ou interrupção do serviço para dezenas de milhares de pessoas ou afetando condados inteiros ou equivalentes.
Categoria 1	Infraestrutura cuja perda poderia causar uma interrupção moderada na prestação de serviços, provavelmente de forma localizada e afetando milhares de cidadãos.
Categoria 0	Infraestrutura cuja perda teria um impacto menor (em escala nacional).

O Reino Unido definiu um limiar crítico na escala, representando o nível acima do qual os impactos da perda são considerados tão graves que a infraestrutura enquadrada deve ser considerada como parte da Infraestrutura Nacional Crítica. Atualmente, este limiar está estabelecido como CAT 3.

A3 – Interdepêndencias:

O Reino Unido identifica interdependências críticas entre o setor Energético e os setores de Transportes, Comunicações, Saúde, Água e Serviços de Emergência. O setor Energia é reconhecido como transversal a todos os demais setores, uma vez que a eletricidade é fundamental para o funcionamento de infraestruturas críticas, sendo que as telecomunicações dependem de energia com sistemas de backup de pelo menos 3 dias de duração independente da rede elétrica principal [68].

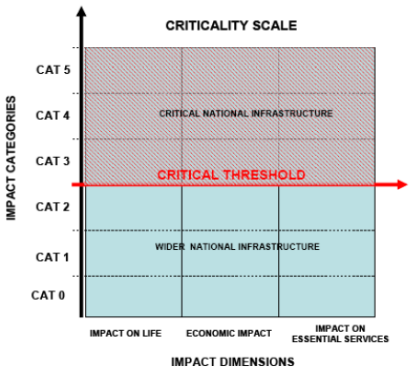


Figura 5.1: As três dimensões da escala de criticidade (RU) [67]

5.1.6 Estados Unidos da América

A1 – Definição de Infraestrutura Crítica:

Nos EUA, a definição de Infraestrutura Crítica (IC) abrange os meios e sistemas, físicos ou virtuais, cuja incapacitação ou destruição resultaria em um impacto debilitante na segurança nacional, na economia, na saúde pública ou em qualquer combinação dessas áreas [69]. Esta definição surgiu após os ataques de 11 de setembro de 2001 às Torres Gémeas, com a implementação do Patriot Act de 2001 [70].

A2 – Critérios e Indicadores:

A Diretiva Presidencial de Política 21 (PPD-21) Segurança e Resiliência da Infraestrutura Crítica orienta o esforço nacional para fortalecer e manter a infraestrutura crítica segura, funcional e resiliente [71]. Conforme a PPD-21, a infraestrutura nacional está dividida em 16 setores [72]. Nos Estados Unidos, os critérios são estabelecidos de forma específica por cada setor e são definidos de maneira precisa apenas pelos setores de Sistema de Água e Esgoto, Tecnologias da Informação, Barragens e o Setor Financeiro.

Tabela 5.7: Escala de Criticidade Sistema de Água e Resíduos (EUA)[73]

Setor	**Critério**	**Indicador**
Sistema de Água e Resíduos	População Atendida	• Nível 1 – Mais de 1 Milhão de pessoas • Nível 2 – 25.000 a 1 Milhão de pessoas • Nível 3 – 3.300 a 25.000 pessoas • Nível 4 – Menos de 3.300 pessoas

Continua na Próxima Página

Continuação da Tabela 5.7

Setor	**Critério**	**Indicador**
	Quantidade de cloro armazenado no local	• Nível 1 – Mais de 40 toneladas • Nível 2 – 20 a 40 toneladas • Nível 3 – 1 a 20 toneladas • Nível 4 – Menos de 1 tonelada
	Impacto Econômico	• Nível 1 – Mais de $100 Bilhões • Nível 2 – $5 a $100 Bilhões • Nível 3 – $100 Milhões a $5 Milhões • Nível 4 – Menos de $100 Milhões
	Clientes Críticos Atendidos	• Nível 1 – Definido pelo governo • Nível 2 – Definido pelo governo • Nível 3 – Duas ou mais ocorrências: Trauma nível 1; Local com capacidade para mais de 10.000 pessoas; Ícones Nacionais; Instalações Chave de Defesa; Indústrias Chave de Defesa • Nível 4 – Não se aplica

Tabela 5.8: Escala de Criticidade Tecnologia da Informação (EUA)[74]

Setor	**Critério**	**Indicador**
Tecnologia da Informação	Impacto na Governança	Efeitos nos governos federal, estadual e local
	Impacto na Segurança Econômica	Efeitos nos usuários e na economia em geral
	Impacto na Saúde e Segurança Públicas	Efeitos na saúde humana devido a lesões e perda de vidas

Continua na Próxima Página

Tabela 5.8: Escala de Criticidade Tecnologia da Informação (EUA)[74]

Setor	**Critério**	**Indicador**
	Impacto na Confiança Pública	Efeitos na moral do público causados por impactos reais ou percebidos nas funções críticas do Setor de TI (esses efeitos podem resultar da visibilidade do impacto, do número de pessoas afetadas e do tempo necessário para mudar para fontes alternativas)

No setor de barragens, somente aquelas designadas como tendo potencial de risco alto ou significativo devem ser incluídas no Inventário Nacional de Barragens (NID), assim como as barragens de potencial de risco baixo que atendem aos critérios de tamanho [75].

Tabela 5.9: Escala de Criticidade Setor de Barragens (EUA) [75]

Setor	**Critério**	**Classificação Potencial de Perigo**
Setor de Barragens	Perda de Vidas Humanas	Potencial de risco baixo: Nenhuma esperada
		Potencial de risco significativo: Nenhuma esperada
		Potencial de risco alto: Provável, uma ou mais esperadas
	Perdas Econômicas, Ambientais ou em Infraestruturas Essenciais	Potencial de risco baixo: Baixa, geralmente limitada ao proprietário
		Potencial de risco significativo: Sim
		Potencial de risco alto: Sim

No setor financeiro, instituições financeiras, agências do poder executivo, reguladores financeiros e outros colaboram para documentar sistemas, infraestrutura e instituições críticas, avaliando a infraestrutura crítica contra a possibilidade de um incidente de cibersegurança [76]. Embora a documentação do setor mencione os critérios que devem ser avaliados os impactos, não há referência aos indicadores de medição.

Tabela 5.10: Critérios Setor Financeiro (EUA)[76]

Setor	**Critério**
Setor Financeiro	Saúde Pública
	Segurança Pública
	Segurança Econômica
	Segurança Nacional

A3 – Interdepêndencias:

Os Estados Unidos reconhecem oficialmente a natureza interconectada de suas infraestruturas críticas através do Plano Nacional de Proteção de Infraestrutura (NIPP 2013) e da Diretiva de Política Presidencial 21 (PPD-21) [77] [71]. O governo americano identifica que "todas as infraestruturas críticas dependem de funções fornecidas pelos setores de energia, comunicações, transporte e água, entre outros"[77]. Esta dependência é particularmente evidente na relação entre o setor das Comunicações e os setores Energético, Tecnologias de Informação, Serviços Financeiros e Serviços de Emergência, onde "as interdependências fluem em ambas as direções, como na dependência dos sistemas de energia e comunicações um do outro e de outras funções"[77].

5.1.7 Canadá

A1 – Definição de Infraestrutura Crítica:

Para o Canadá, a infraestrutura crítica refere-se a processos, sistemas, instalações, tecnologias, redes, ativos e serviços essenciais para a saúde, segurança e bem-estar econômico dos canadenses, bem como para o funcionamento eficaz do governo. A infraestrutura crítica pode ser independente ou interconectada e interdependente dentro e entre províncias, territórios e fronteiras nacionais. Interrupções na infraestrutura crítica podem resultar em perda catastrófica de vidas, efeitos econômicos adversos e danos significativos à confiança pública [78].

A2 – Critérios e Indicadores:

No Canadá, o Programa Nacional de Garantia da Infraestrutura Crítica (NCIAP) fornece ferramentas para identificar e classificar ativos de IC, com a perspectiva de que um processo comum de gerenciamento de riscos incentivará os parceiros a abordar a IC de maneira consistente [79]. Embora a documentação mencione os critérios para avaliação dos impactos, não há referência aos indicadores de medição.

Tabela 5.11: Critérios (Canadá)[79]

Critério
Impacto na concentração de pessoas e meios
Impacto econômico
Impacto no setor da IC
Interdependência (Consequências nos outros setores)
Continuidade do Serviço
Confiança pública

A3 – Interdepêndencias:

O Canadá adota uma abordagem holística de riscos para a proteção de suas Infraestruturas Críticas (IC) [80], partindo do princípio de que apenas um conhecimento aprofundado sobre riscos, ameaças, vulnerabilidades e interdependências constitui o primeiro passo para a elaboração de planos de proteção realmente eficazes. A posição canadense é de que a análise das interdependências deve ser integrada às decisões de gestão de riscos, às estratégias de mitigação e às ações de resposta e recuperação após qualquer perturbação ou destruição [81].

5.1.8 Austrália

A1 – Definição de Infraestrutura Crítica:
A Austrália define Infraestruturas críticas como, instalações físicas, sistemas, ativos, cadeias de suprimento, tecnologias da informação e redes de comunicação que, se destruídas, degradadas, comprometidas ou tornadas indisponíveis por um período prolongado, impactariam significativamente o bem-estar social ou econômico da Austrália como nação ou de seus estados ou territórios, ou afetariam a capacidade da Austrália de conduzir a defesa nacional e garantir a segurança nacional [82].

A2 – Critérios e Indicadores:
Embora a documentação do Governo da Austrália relacione os critérios que devem ser avaliados os impactos, não há referência aos indicadores de medição.

Tabela 5.12: Critérios (Austrália)[82]

Critério
Segurança Pública
Segurança Nacional
Impacto Econômico
Competitividade Internacional
Continuidade dos Serviços Essenciais
Confiança pública

A3 – Interdepêndencias:
A Austrália identifica interdependências críticas entre o setor Energético e os setores de Comunicações, Transportes, Água e Esgoto, Saúde e Serviços de Emergência [83]. O governo australiano reconhece que as infraestruturas críticas são cada vez mais interconectadas e interdependentes, proporcionando eficiências e benefícios económicos às operações, mas criando vulnerabilidades que podem resultar em falhas em cascata [84]. O setor Energia é transversal a todos os demais setores porque é fundamental para o funcionamento das infraestruturas críticas, sendo que uma falha prolongada e generalizada no setor energético teria impactos nacionalmente significativos, incluindo perturbações nas redes de transportes e telecomunicações, instabilidade no fornecimento de alimentos e mercearias, e impactos na prestação de serviços de saúde [83].

5.1.9 Japão

A1 – Definição de Infraestrutura Crítica:
O Japão define Infraestruturas críticas como a base das vidas sociais e das atividades econômicas das pessoas, formada por empresas que prestam serviços extremamente difíceis de serem substituídos por outros. Se sua função for suspensa, deteriorada ou se tornar indisponível, isso pode ter impactos significativos nas vidas sociais e nas atividades econômicas das pessoas [85].

A2 – Critérios e Indicadores:
Embora a documentação do Japão detalhe os critérios a serem avaliados para mensurar os impactos, ela não especifica os indicadores a serem utilizados nessa mensuração.

Tabela 5.13: Critérios (Japão)[85]

Critério
Impacto público e social
Impacto Econômico
Impacto nos Serviços Essenciais

A3 – Interdepêndencias:
O Japão identifica interdependências críticas entre o setor Energético (eletricidade e gás) e os setores de Comunicações, Transportes (ferroviário e aéreo), Serviços Financeiros, Serviços Governamentais e Administrativos, Serviços Médicos, Abastecimento de Água e Logística [86]. A análise de interdependência conduzida pelo Comitê Técnico de Infraestrutura Crítica do Centro Nacional de Segurança da Informação (NISC) confirmou que as comunicações, energia elétrica e abastecimento de água são os principais setores de apoio para muitos outros setores de infraestrutura crítica [86].

O setor de energia elétrica desempenha o papel mais importante no apoio a outras infraestruturas críticas, sendo reconhecido como transversal a todos os demais setores porque é fundamental para o funcionamento das infraestruturas críticas, enquanto uma grande suspensão da operação de fornecimento de energia, linhas de comunicação e suprimentos de água pode propagar problemas para outros setores [85]. A análise de interdependência "estática"revelou principalmente como os sistemas críticos dependem de outras infraestruturas críticas, e a análise "dinâmica"revelou como o relacionamento entre os setores pode mudar ao longo do tempo em caso de ocorrência de disfunções de TI [85].

5.1.10 Catar

A1 – Definição de Infraestrutura Crítica:
No Catar, infraestrutura crítica é definida como ativos físicos, sistemas ou instalações, que, se interrompidos, comprometidos ou destruídos, teriam um impacto sério na saúde, segurança ou bem-estar econômico do Catar, ou no funcionamento eficaz do governo catariano [87].

A2 – Critérios e Indicadores:
De acordo com a Qatar National Cyber Security Strategy (2014), a classificação dos ativos como críticos deve seguir as seguintes orientações: utilizar a tabela de gravidade do impacto para determinar a pontuação de impacto pela perda ou não funcionamento de cada ativo principal; e classificar todos os ativos como críticos quando a pontuação de criticidade for superior a vinte [87].

Tabela 5.14: Escala de Criticidade (Catar)[87]

Critério	**Indicador**
Impacto na População (Potencial de perda de vidas)	Low (1)- <10
	Medium (3)- 10–100
	High (5)- 100–500
	Severe (15)- >500
Impacto Econômico/QAR (Dano direto e custo de restauração, incluindo redes/sistemas de infraestrutura crítica)	Low (1)- <20M
	Medium (3)- 20M–200M
	High (5)- 200M–1B
	Severe (15)- >1B
Impacto de Interdependência	Low (1)- Minor Impact
	Medium (3)- Moderate Impact/Disruption
	High (5)- Significant Impact/Disruption
	Severe (15)- Debilitation Impact
Impacto de Escopo	Low (1)- Local
	Medium (3)- Large Local or Multiple Sectors (Partially)
	High (5)- National or Single Sector (Fully)
	Severe (15)- International or Multiple Sectors (Fully)
Impacto no Serviço	Low (1)- <1
	Medium (3)- 1–30
	High (5)- 30–180
	Severe (15)- >180
Impacto na Confiança Pública	Low (1)- Public perceives low national risk, high ability to control
	Medium (3)- Public perceives moderate national risk, Moderate ability to control
	High (5)- Public perceives high national risk, low ability to control
	Severe (15)- Public perceives severe national risk, ability to control in doubt

A3 – Interdepêndencias:

No Catar, as infraestruturas críticas são altamente interdependentes, especialmente entre os setores de energia, água, transportes, finanças, saúde e tecnologia da informação e comunicações (TIC) [88]. O governo catariano reconhece que a resiliência nacional depende do funcionamento contínuo e seguro desses setores, pois uma falha significativa em um pode provocar efeitos em cascata nos demais. Por exemplo, a dependência de sistemas de transporte, hospitais e serviços financeiros da energia e das TIC evidencia a transversalidade desses setores, sendo que interrupções na energia elétrica ou nas comunicações podem comprometer o fornecimento de água, a operação de hospitais e a prestação de serviços governamentais es-

senciais. Para mitigar esses riscos, o Catar adota avaliações regulares de dependências e interdependências entre setores críticos, promovendo a colaboração entre governo, setor privado e demais partes interessadas para garantir a continuidade dos serviços essenciais [88].

5.1.11 Irlanda

A1 – Definição de Infraestrutura Crítica:
A Irlanda define como um ativo, sistema ou parte dele que é essencial para a manutenção de funções sociais vitais, saúde, segurança, bem-estar econômico ou social das pessoas, e cuja interrupção ou destruição teria um impacto significativo no Estado como resultado da falha em manter essas funções [89].

A2 – Critérios e Indicadores:
De acordo com o Departamento de Defesa (2019), o cálculo de criticidade na Irlanda é dividido em três escalas: Escala de Escopo, Escala de Severidade e Escala de Tempo. O produto das pontuações obtidas nessas escalas é posicionado na Escala de Criticidade, onde a partir do nível 3 as infraestruturas nacionais são categorizadas como infraestruturas críticas [89].

Tabela 5.15: Escala de Escopo (Irlanda)[89]

Critério	**Muito Baixo (1)**	**Baixo (2)**	**Moderado (3)**	**Alto (4)**	**Muito Alto (5)**
Pessoas Afetadas	< 75.000	> 75.000	> 150.000	> 225.000	> 350.000
Concentração de Pessoas	< 10 pessoas/km²	> 10 pessoas/km²	> 50 pessoas/km²	> 250 pessoas/km²	> 1.250 pessoas/km²
Alcance	Rural	Urbano /Cidade	Condado	Regional	Nacional

Tabela 5.16: Escala de Severidade (Irlanda)[89]

Fator de Impacto	**Muito Baixo (1)**	**Baixo (2)**	**Moderado (3)**	**Alto (4)**	**Muito Alto (5)**
Impactos Públicos	Mortes menores que 1 em 250.000 pessoas Lesões Leves	Mortes maiores que 1 em 250.000 Lesões Graves	Mortes maiores que 1 em 100.000 Lesões Graves	Mortes maiores que 1 em 40.000 Lesões Graves	Mortes maiores que 1 em 20.000 Lesões Graves
Impacto Econômico	Até 1% do Orçamento Anual	> 1% do Orçamento Anual	> 2% do Orçamento Anual	> 4% do Orçamento Anual	> 8% do Orçamento Anual

Continua na Próxima Página

Fator de Impacto	Muito Baixo (1)	Baixo (2)	Moderado (3)	Alto (4)	Muito Alto (5)
Impacto Ambiental	Contaminação simples Localizada	Contaminação simples Regional Curta duração	Contaminação pesada Localizada Longa duração	Contaminação pesada Generalizada Longa duração	Contaminação muito pesada Generalizada Longa duração
Dependência	Impacto muito baixo em outras infraestruturas	Impacto baixo em outras infraestruturas	Impacto moderado em outras infraestruturas	Impacto alto em outras infraestruturas	Impacto muito alto em outras infraestruturas
Relações Internacionais	Impacto muito baixo nas relações internacionais	Impacto baixo nas relações internacionais	Impacto moderado nas relações internacionais	Impacto alto nas relações internacionais	Impacto muito alto nas relações internacionais
Serviços Essenciais	Disrupção muito baixa Serviços públicos/privados	Disrupção baixa Serviços públicos/privados	Disrupção média Serviços públicos/privados	Disrupção alta Serviços públicos/privados	Perda na entrega de serviços públicos/privados
Segurança	Disrupção muito baixa Eficácia operacional	Disrupção baixa Eficácia operacional	Disrupção moderada Eficácia operacional	Disrupção alta Eficácia operacional	Perda da eficácia operacional

Tabela 5.17: Escala de Tempo (Irlanda)[89]

Fator de Impacto	Muito Baixo (1)	Baixo (2)	Moderado (3)	Alto (4)	Muito Alto (5)
Tempo de Recuperação	Minutos	Horas	Dias	Semanas	Meses
Duração do Impacto	Minutos	Horas	Dias	Semanas	Meses
Pico de Impacto do Incidente ou Ponto Crítico da Escala	Dentro de Meses	Dentro de 4 Semanas	Dentro de 7 Dias	Dentro de 24 Horas	Imediato

A3 – Interdepêndencias:

Na Irlanda, as infraestruturas críticas apresentam interdependências significativas entre setores como energia, comunicações, transportes, água, saúde e finanças [90]. O documento estratégico nacional destaca que a complexidade crescente dessas interdependências pode gerar riscos de efeitos em cascata, como a dependência do setor de abastecimento de água e saneamento em relação ao fornecimento contínuo de energia elétrica, ou a necessidade de comunicações robustas para a operação dos serviços de emergência

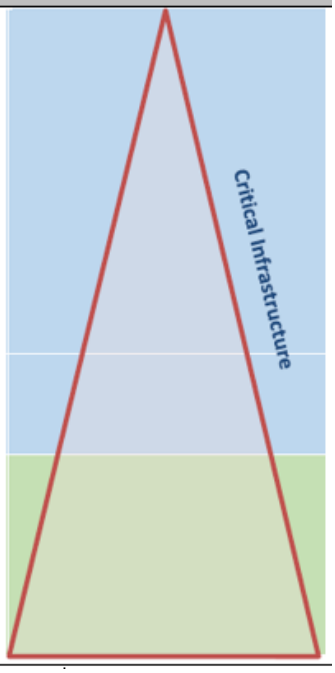
Nível	Descrição	Pirâmide de Infraestrutura Nacional
5	Esta é a infraestrutura cuja perda teria um impacto muito alto sobre o Estado. Esses ativos serão de importância nacional, cuja perda teria efeitos nacionais significativos e pode impactar vários setores. Relativamente poucos são esperados atender aos critérios do Nível 5, conhecidos como Infraestrutura Nacional Crítica (CNI). (>80 Pontuação de Criticidade)	
4	Infraestruturas de alta importância para os setores devem se enquadrar nesta categoria. O impacto da perda desses ativos nos serviços essenciais seria alto e pode impactar a provisão de serviços essenciais em toda a Irlanda. (>50 Pontuação de Criticidade)	
3	Infraestruturas importantes para os setores e para a entrega de serviços essenciais, cuja perda teria um impacto moderado. (>36 Pontuação de Criticidade)	
2	Infraestruturas cuja perda teria um baixo impacto na entrega de serviços essenciais. (>27 Pontuação de Criticidade)	
1	Infraestruturas cuja perda causaria uma disrupção muito baixa na entrega de serviços, provavelmente de forma localizada. (<27 Pontuação de Criticidade)	

Figura 5.2: Tabela de Criticidade (Irlanda)[89]

e transporte [90]. O setor energético é considerado transversal, pois sua interrupção pode comprometer o funcionamento de diversos outros setores essenciais, evidenciando a necessidade de identificar e gerenciar essas relações para garantir a resiliência e a continuidade dos serviços vitais à sociedade irlandesa [90].

5.1.12 Estônia

A1 – Definição de Infraestrutura Crítica:

A Estônia adota a definição da União Europeia para determinar suas infraestruturas críticas como sendo um elemento, sistema ou parte deste situado nos Estados-Membros que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar econômico ou social, e cuja perturbação ou destruição teria um impacto significativo num Estado-Membro, dada a impossibilidade de continuar a assegurar essas funções [91].

A2 – Critérios e Indicadores:

Embora a documentação da Estônia delineie os critérios a serem avaliados para medir os impactos, ela não especifica os indicadores a serem utilizados nessa avaliação.

Tabela 5.18: Critérios (Estônia)[91]

Critério
Pessoas Afetadas
Duração das Interrupções de Serviço
Complexidade de Restauração do Serviço

Continua na Próxima Página

Critério
Extensão da área afetada

A3 – Interdepêndencias:
Na Estônia, as infraestruturas críticas apresentam interdependências marcantes entre setores como energia, comunicações, transportes, serviços financeiros, saúde, água e alimentação [92]. O funcionamento da sociedade depende fortemente da operação contínua e segura da infraestrutura de informação, que serve de base para os demais setores críticos, como energia e transportes, tornando o setor de tecnologia da informação transversal a todos os outros [92]. Uma interrupção significativa nos sistemas de energia ou comunicações pode gerar efeitos em cascata, afetando a prestação de serviços essenciais, como abastecimento de água, saúde e operações financeiras. Por isso, a Estônia enfatiza a necessidade de coordenação centralizada, avaliações regulares de riscos e colaboração entre setores público e privado para garantir a resiliência e a continuidade dos serviços críticos [92].

5.2 COMPARAÇÃO DA DEFINIÇÃO DAS INFRAESTRUTURAS CRÍTICAS E SEUS CRITÉRIOS

Com base na investigação conduzida sobre as diversas metodologias adotadas por organizações e países de referência, este capítulo tem como objetivo fornecer subsídios técnicos para a avaliação do Modelo de Avaliação de Criticidade de Sistemas do PPSI, com foco na identificação de infraestruturas críticas. Para tal, serão analisadas as particularidades dos países apresentados na seção anterior, comparando-as entre si, utilizando uma abordagem metodológica comparativa conforme os aspectos de análise previamente identificados.

Os resultados da análise dos conceitos de infraestruturas críticas nos países selecionados, cujas informações estavam integralmente disponíveis em fontes públicas, estão apresentados na Tabela 5.19. Notou-se uma maior convergência na categoria de condições, em comparação aos elementos e critérios de criticidade.

Tabela 5.19: Comparativo Definições Infraestrutura Críticas

País	Elemento	Condição	Critérios de Criticidade
UE	Elemento, sistema ou parte deste	Perturbação ou destruição	Funções vitais para a sociedade, a saúde, a segurança e o bem-estar econômico ou social

Continua na Próxima Página

País	Elemento	Condição	Critérios de Criticidade
Espanha	Instalações que proporcionam serviços essenciais à população, cujo funcionamento é indispensável e não possui soluções alternativas	Perturbação, Interrupção ou Destruição	Serviços Essenciais
Portugal	Componente, Sistema ou parte deste	Perturbação ou Destruição	Funções vitais para a sociedade, saúde, segurança e bem-estar econômico ou social
Holanda	Processos Críticos	Falha ou Interrupção	Grave perturbação social e representaria uma ameaça à segurança nacional
Reino Unido	Elementos "críticos"da infraestrutura nacional	Perturbação ou Destruição	Consequências econômicas ou sociais, e perda de vidas
Estados Unidos	Meios e sistemas, físicos ou virtuais	Incapacitação ou Destruição	Impacto debilitante na segurança nacional, na economia e saúde pública
Canadá	Processos, sistemas, instalações, tecnologias, redes, ativos e serviços essenciais	Descrição positiva e não possui ações	Saúde, segurança e bem-estar econômico
Austrália	Instalações físicas, sistemas, ativos, cadeias de suprimento, tecnologias da informação e redes de comunicação	Destruição, Degradação e Comprometimento	Bem-estar social, econômico, defesa nacional e segurança nacional
Japão	Empresas que prestam serviços extremamente difíceis de serem substituídos por outros	Suspensão, Deterioração e Indisponibilidade	Vida Social e Atividade Econômica
Catar	Ativos físicos, sistemas ou instalações	Interrupção, Comprometimento e Destruição	Saúde, segurança e bem-estar econômico
Irlanda	Ativo, sistema ou parte dele	Interrupção ou Destruição	Funções sociais vitais, saúde, segurança, bem-estar econômico ou social das pessoas
Estônia	Elemento, sistema ou parte deste	Perturbação ou Destruição	Funções vitais para a sociedade, a saúde, a segurança e o bem-estar econômico ou social

Da análise da tabela, pode-se observar algumas diferenças na forma como as IC são definidas. A primeira grande diferença está nos elementos da definição. A Espanha optou por uma abordagem onde instalações que fornecem serviços essenciais são consideradas críticas [61]. No Reino Unido, embora haja alguma semelhança, a terminologia utilizada é "Elementos Críticos"da infraestrutura nacional, em vez de "instalações"[67].

Portugal e Estônia optaram por transcrever diretamente a definição da UE [64], [91], [58]. Em contrapartida, outros países expandem os elementos, não se limitando apenas aos termos elemento, componente, sistema ou parte deste. Nos EUA, logo na definição, destaca-se que o elemento pode ser físico ou virtual, conferindo-lhe uma maior abrangência [69]. Outra diferença principal identificada no caso do Canadá é a utilização de uma descrição positiva; ou seja, as Infraestruturas Críticas não são definidas em termos de importância relativa as condições de perturbação ou destruição [78].

Irlanda e Catar incorporam o conceito de "Ativo"em suas definições, demonstrando uma abrangência similar à dos Estados Unidos [89], [93]. A Austrália, por outro lado, adota uma abordagem detalhada, especificando todos os elementos, incluindo instalações, cadeias de suprimento, redes e comunicações, entre outros [82].

No Japão, foi incluído o termo "empresas que prestam serviços essenciais", conferindo um caráter mais detalhado, embora menos abrangente que o da Austrália [85]. A Holanda adotou uma abordagem diferente, introduzindo o termo "Processos Críticos"[35]. Embora o termo "processo"já apareça na definição canadense, a Holanda especificou "críticos"e restringiu o elemento a essas duas palavras.

O panorama das palavras que representam os elementos pode ser verificado na Figura 5.3, que destaca uma maior ênfase nos termos "Ativo", "Instalações", "Elemento", "Sistema"e "Serviços". No que diz respeito às condições Figura 5.4, não foram identificadas diferenças significativas com implicações relevantes nas definições, sendo "perturbação", "destruição"e interrupção"as principais palavras encontradas.

Figura 5.3: Nuvem dos principais elementos

Em relação aos critérios de criticidade, verificou-se que a maioria dos países se concentra principalmente na saúde, segurança, bem-estar econômico e social, figura 5.5.

A Figura 5.6 ilustra a inter-relação entre os componentes da definição de infraestruturas críticas. Nela, observa-se que sistemas, instalações e serviços, quando sujeitos a perturbações ou destruição, podem de-

Figura 5.4: Nuvem das principais condições

Figura 5.5: Nuvem dos principais critérios de criticidade

sencadear impactos econômicos, de segurança, saúde e sociais.

5.2.1 Comparação e Categorização dos Critérios e Indicadores

Dentro do contexto dos Critérios e Indicadores, foi realizado um agrupamento de todos os critérios utilizados pelos países estudados, visando alcançar uniformidade. Os indicadores desempenham um papel auxiliar na criação dessa conexão sempre que os critérios não apresentarem uma aproximação clara entre si.

Tabela 5.20: Critérios e Indicadores usados no agrupamento

Critérios	**Indicadores**	**Critérios Agrupadores**
Ocorrência de acidentes, Número de pessoas Afetadas, Impacto Físico, Perda de Vidas Humanas, Impacto na Concentração de Pessoas, Impacto na População	Número potencial de feridos, Número potencial de vítimas mortais	Impacto nas Pessoas

Continua na Próxima Página

Critérios	Indicadores	Critérios Agrupadores
Impacto Econômico	Importância dos prejuízos econômicos, Importância da degradação dos produtos ou serviços	Impacto Econômico
Efeitos no domínio público, População Atendida, Impacto na Confiança Pública, Saúde Pública, Segurança Pública, Continuidade do Serviço	Impacto na confiança das populações, Sofrimento físico e perturbação da vida cotidiana, Perda de serviços essenciais	Impacto Social
Alcance, Extensão da área afetada	Extensão da área geográfica que pode ser afetada (internacional, nacional, provincial/territorial ou local)	Impacto Geográfico
Efeitos no Tempo	Imediato, 24-48 horas, uma semana, um mês, um ano, etc.	Duração no Impacto
Impacto no Meio Ambiente	Degradação do local e arredores, Contaminação	Impacto Ambiental
Efeitos em Cascata	A falha resulta no impacto em outros setores	Impacto de Interdependência

Após a categorização de todos os critérios, foi contabilizada a quantidade e o percentual de presença de cada um dos critérios e indicadores em relação ao total de países analisados.

Dos sete critérios elencados, cinco se destacaram em termos de relevância. Os impactos nas pessoas e os impactos sociais foram mencionados por todos os 12 países pesquisados. O impacto econômico foi citado por 11 países, seguido pelos impactos geográfico e de interdependência, ambos mencionados por 5 países, respectivamente conforme demonstrado na Figura 5.7.

Na Figura 5.8, é possível verificar a distribuição dos critérios escolhidos por cada país. A Irlanda utilizou todos os sete critérios, demonstrando uma abordagem mais abrangente em comparação aos demais. Por outro lado, Portugal, Estados Unidos, Japão, Austrália e Estônia utilizaram apenas três critérios. Os intermediários, como UE, Reino Unido e Catar, selecionaram cinco critérios. Finalmente, Holanda e Canadá consideraram quatro critérios, pois não incluíram o impacto geográfico. A média dos critérios avaliados pelos 12 países/organizações analisados é de quatro critérios.

5.2.2 Discussão sobre a Priorização dos Critérios

Apesar da menção ao dano ambiental na literatura e nos discursos institucionais sobre avaliação de criticidade em infraestruturas críticas, a análise dos referenciais internacionais revela que, na prática, a priorização dos ativos críticos por gestores e agentes decisórios tende a concentrar-se em três grandes dimensões: impactos sobre vidas humanas, impactos econômicos (financeiros) e impactos sociais relacionados à ordem pública. O critério ambiental, embora presente em algumas normativas e reconhecido em discursos, aparece de maneira relevante como critério efetivo de tomada de decisão em poucos países.

Figura 5.6: Nuvem de inter-relação dos elementos da definição crítica

Critérios	Quantidade	Percentual
Impacto nas Pessoas	**12**	**100,00%**
Impacto Social	**12**	**100,00%**
Impacto Econômico	**11**	**91,67%**
Impacto Geográfico	**5**	**41,67%**
Impacto de Interdependência	**5**	**41,67%**
Impacto Ambiental	2	**16,67%**
Duração do Impacto	2	**16,67%**
Total de Países	**12**	

Figura 5.7: Mensuração da Quantidade de Críterios

Essa constatação reflete a experiência acumulada em situações reais de crise, nas quais, diante de eventos disruptivos graves, os esforços e recursos são direcionados prioritariamente para a preservação de vidas, a contenção de impactos econômicos de grande monta e a manutenção da ordem social.

Desse modo, ao analisar e propor modelos de avaliação de criticidade, é essencial distinguir entre a abrangência conceitual dos critérios e suas efetivas prioridades em contextos reais de tomada de decisão. O reforço dessa diferenciação contribui para a aderência do modelo proposto às necessidades dos gestores e melhora a capacidade de resposta diante de cenários de alta pressão, tornando o processo de classificação mais realista, prático e alinhado aos padrões internacionais observados nos estudos de caso comparados.

5.3 ANÁLISE COMPARATIVA DAS INTERDEPENDÊNCIAS EM INFRAESTRUTURAS CRÍTICAS (ASPECTO A3)

Com base na análise dos dados, foi realizada uma extração sistemática das informações sobre interdependências (aspecto A3) dos 12 países e organizações estudados. Esta seção apresenta um quadro comparativo conciso Tabela 5.21 seguido de uma análise dos principais padrões identificados nas abordagens internacionais para o tratamento das interdependências entre infraestruturas críticas.

	Quadro comparativo de critérios por países												
Critérios	UE	ESP	POR	HOL	RU	EUA	CAN	AUS	JAP	QAT	IRL	EST	Total
Impacto nas Pessoas	X	X	X	X	X*	X	X	X	X	X	X	X	12
Impacto Social	X	X	X	X	X*	X	X	X	X	X	X	X	12
Impacto Econômico	X	X	X	X	X*	X	X	X	X	X	X		11
Impacto Geográfico	X				X*					X	X	X	5
Impacto de Interdependência				X	X*		X			X	X		5
Impacto Ambiental		X									X		2
Duração no Impacto	X										X		2
Total	5	4	3	4	5	3	4	3	3	5	7	3	49

*Deduzidos pelo autor com base nas categorias da escala de criticidade.

Figura 5.8: Distribuição de Critérios por País

5.3.1 Quadro Comparativo das Interdependências

A Tabela 5.21 resume as abordagens adotadas pelos países analisados quanto às interdependências entre infraestruturas críticas, destacando setores transversais priorizados e observações específicas para cada contexto nacional.

Tabela 5.21: Abordagens de Interdependências em Infraestruturas Críticas (A3)

País/Organização	**Abordagem de Interdependências**	**Setor Transversal Prioritário/Observações**
União Europeia	Interdependências intra e intersetoriais, projetos transnacionais	Energia, Comunicações, Transportes, Água
Espanha	Efeitos em cascata intra e intersetoriais, legislação específica	Infraestruturas estratégicas, Energia
Portugal	Abordagem holística, transversalidade entre setores	Todos os setores, análise pode alterar criticidade
Holanda	Efeitos em cascata, foco em processos críticos	Energia, Comunicações, Transportes
Reino Unido	Setor energético transversal, dependências explícitas	Energia (transversal), Comunicações, Saúde, Água
Estados Unidos	Interdependências bidirecionais, integração em políticas nacionais	Energia, Comunicações, Transportes, Água
Canadá	Abordagem holística, integração à gestão de riscos	Todos os setores, análise integrada
Austrália	Setor energético transversal, riscos de cascata	Energia (transversal), Comunicações, Transportes
Japão	Energia e comunicações como setores de apoio, análise dinâmica	Energia, Comunicações, Água
Catar	Efeitos em cascata, avaliações regulares de dependências	Energia, TIC, Saúde, Água
Irlanda	Energia transversal, riscos de cascata, análise detalhada	Energia (transversal), Comunicações, Saúde, Água
Estônia	Setor de TI transversal, forte dependência digital	Tecnologia da Informação (transversal), Energia, Transportes, Saúde

5.3.2 Análise dos Resultados

Setores Transversais Predominantes: Conforme pode ser observado na Tabela 5.21, a análise revela convergência internacional na priorização dos setores de Energia, Comunicações/TIC, Água, Transportes e Saúde como centrais para a resiliência das infraestruturas críticas. Energia é transversal na maioria dos países, exceto na Estônia, onde a Tecnologia da Informação ocupa papel central devido à forte digitalização nacional.

Abordagens Metodológicas:

- **Setores Transversais:** Reino Unido, Austrália, Japão, Irlanda e Estônia reconhecem um setor dominante (Energia ou TI) como base para os demais.
- **Abordagem Holística:** Portugal, Canadá e Holanda consideram todos os setores de forma transversal, com integração à gestão de riscos.
- **Efeitos em Cascata:** Catar, Austrália, Irlanda, Holanda e Espanha enfatizam riscos de propagação entre setores.
- **Bidirecionalidade:** Estados Unidos destacam que as interdependências fluem em ambas as direções entre setores.

Convergências:

- Reconhecimento universal da importância das interdependências para a segurança nacional.
- Energia como setor transversal em 6 de 12 países; TIC na Estônia.
- Preocupação comum com efeitos em cascata e necessidade de colaboração público-privada.

Divergências:

- Setor prioritário: maioria prioriza Energia, Estônia prioriza Tecnologia da Informação.
- Granularidade: alguns países detalham setores e critérios, outros adotam abordagem genérica.
- Integração com gestão de riscos: Canadá e Portugal integram explicitamente interdependências à gestão de riscos.

Particularidade da Estônia: A Estônia se diferencia por considerar a Tecnologia da Informação como setor transversal, reflexo de sua sociedade altamente digitalizada. O funcionamento contínuo e seguro da infraestrutura de informação é considerado fundamental para todos os demais setores críticos, tornando o país especialmente sensível a interrupções digitais e cibernéticas.

A análise comparativa demonstra que as melhores práticas internacionais convergem para: (1) identificação de setores transversais como Energia e TIC; (2) avaliação sistemática de efeitos em cascata; (3) abordagens holísticas para dependências intra e intersetoriais; (4) integração das análises de interdependência à gestão de riscos e à resiliência nacional.

5.4 ANÁLISE DOCUMENTAL E CONSTRUÇÃO DO MODELO DE HIERARQUIZAÇÃO DE DECISÃO

Nesta fase da pesquisa, foi realizada uma análise aprofundada das assertivas extraídas do modelo de avaliação de criticidade de sistemas do Programa de Privacidade e Segurança da Informação (PPSI), categorizando-as em critérios e subcritérios. A análise documental buscou, em primeiro lugar, verificar a aderência das assertivas do framework do PPSI aos critérios previamente identificados na literatura. As assertivas foram organizadas e estruturadas com o auxílio do aplicativo Microsoft Access, conforme ilustrado na Figura 5.9, que apresenta a categorização de critérios e subcritérios baseados na avaliação de criticidade proposta pelo Programa de Privacidade e Segurança da Informação (PPSI).

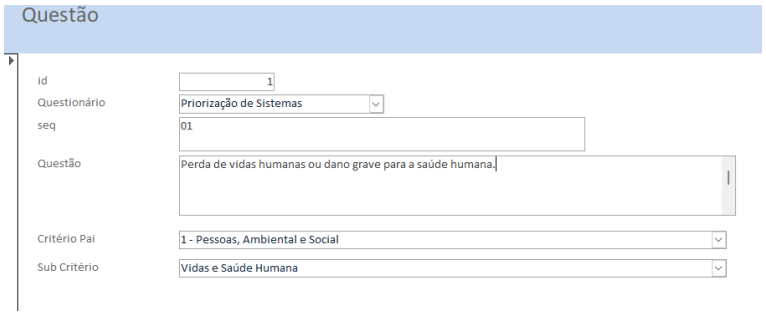


Figura 5.9: Categorização de criterios/subcritérios a partir do framework do PPSI

Cada assertiva identificada no framework do PPSI foi associada a um critério principal e um subcritério, utilizando parâmetros obtidos a partir da revisão de literatura e das adaptações metodológicas realizadas por esta pesquisa. A Tabela 5.22 a seguir demonstra essa associação, listando os critérios e subcritérios em correspondência com as questões do PPSI. Observa-se que as assertivas 3 e 9 foram desmembradas para permitir uma classificação mais precisa, uma vez que abordam aspectos relacionados a diferentes critérios identificados na literatura. Ademais, as assertivas de número 23 a 24.2 foram incluídas a partir da planilha de avaliação utilizada pelo TCU para os órgãos do SISP, a qual contempla não apenas as 22 assertivas originalmente previstas no framework do PPSI, mas também 3 questões adicionais que foram consideradas relevantes pelo TCU para avaliação.

Tabela 5.22: Relação Critérios e Assertivas do Modelo de Avaliação de Criticidade de Infraestruturas Críticas - Ordenada pelo Código da Assertiva

Nr.	**Assertiva do PPSI**	**Critério**	**Nr.**	**Subcritério**
1	Perda de vidas humanas ou dano grave para a saúde humana.	1 - Pessoas, Ambiental e Social	1.4	Vidas e Saúde Humana
2	Danos ambientais graves.	1 - Pessoas, Ambiental e Social	1.1	Danos Ambientais Graves
3.01	Degradação significativa na prestação de serviço essencial ao cidadão.	1 - Pessoas, Ambiental e Social	1.2	Degradação de Serviço Essencial ao Cidadão

Continua na Próxima Página

Nr.	Assertiva do PPSI	Critério	Nr.	Subcritério
3.02	Caso SIM, informe a abrangência do serviço.	3 - Geográfico e Interdependência	3.1	Abrangência do Serviço
4	Danos financeiros significativos à Administração Pública ou aos cidadãos.	2 - Econômico	2.1	Danos Financeiros
5	Danos significativos à reputação ou à credibilidade da organização.	3 - Geográfico e Interdependência	3.4	Reputação / Credibilidade Organizacional
6	Impedimento do funcionamento de atividade finalística da organização.	4 - Organizacional - Negócio, Processos, Gestão	4.1	Atividade Finalística
7	Degradação significativa da produtividade dos servidores/funcionários da organização que utilizam ou dependem do sistema.	4 - Organizacional - Negócio, Processos, Gestão	4.6	Produtividade dos Servidores / Funcionários
8	Degradação significativa do funcionamento de atividades ou processos com características multi-institucionais e que envolvam diferentes esferas da administração ou dos poderes.	3 - Geográfico e Interdependência	3.2	Degradação de Atividades ou Processos
9.01	Soberania e integridade territorial nacionais.	6 - Estado	6.5	Soberania e Integridade Territorial
9.02	Planos e operações militares.	6 - Estado	6.3	Planos e Operações Militares
9.03	Sistemas, instalações, programas, projetos, planos ou operações de interesse da defesa nacional.	6 - Estado	6.1	Defesa Nacional
9.04	Relações internacionais do país.	6 - Estado	6.4	Relações Internacionais
9.05	Assuntos diplomáticos e de inteligência (informações secretas ou ultrassecretas).	6 - Estado	6.2	Diplomacia e Inteligência
10	Exposição indevida de dados pessoais sensíveis e que possa causar dano ao titular.	1 - Pessoas, Ambiental e Social	1.3	Exposição de Dados Pessoais Sensíveis
11	Efeito negativo na execução da política econômica do Brasil (fiscal, monetária e cambial).	2 - Econômico	2.2	Danos na Economia

Continua na Próxima Página

Nr.	Assertiva do PPSI	Critério	Nr.	Subcritério
12	Degradação significativa do funcionamento de atividades ou serviços relacionados às infraestruturas críticas do Brasil (definidas na Política Nacional de Segurança de Infraestruturas Críticas).	3 - Geográfico e Interdependência	3.3	Degradação dos Serviços relacionados às IC´s
13	O sistema está coberto por solução de continuidade de serviços de TI (alta disponibilidade, recuperação de desastres e planos de contingência)?	4 - Organizacional - Negócio, Processos, Gestão	4.8	Solução de Continuidade
14	O sistema é suportado por equipe de respostas a incidentes?	4 - Organizacional - Negócio, Processos, Gestão	4.3	ETIR
15	As vulnerabilidades e os riscos de TI relacionados ao sistema e à infraestrutura que o sustenta estão identificados, classificados, analisados e tratados?	4 - Organizacional - Negócio, Processos, Gestão	4.5	Gestão de Riscos
16	O sistema possui tecnologia obsoleta ou desatualizada (hardware e software)?	5 - Aspectos do Sistema	5.7	Tecnologia Obsoleta
17	O sistema está hospedado em sala segura ou sala cofre?	5 - Aspectos do Sistema	5.5	Sala Segura
18	O sistema ou a infraestrutura que o suporta estão cobertos por processo de gestão de patches de segurança?	5 - Aspectos do Sistema	5.6	Segurança
19	São realizados testes de invasão ou auditorias de segurança no sistema ou na infraestrutura que o sustenta?	5 - Aspectos do Sistema	5.8	Testes de Invasão e Auditoria
20	O sistema é alvo de frequentes ataques?	5 - Aspectos do Sistema	5.1	Ataques Cibernéticos
21	O sistema possui controles para a proteção dos dados e do código (criptografia, backup, controle de acesso, trilhas de auditoria, etc.)?	5 - Aspectos do Sistema	5.2	Controles de Proteção de Dados
22	O sistema e a infraestrutura que o suporta estão incluídos em processo de gestão de ativos de TI (ITAM)?	4 - Organizacional - Negócio, Processos, Gestão	4.4	Gestão de Ativos
23	Custo anual de sustentação do sistema (correção, adaptação e evolução dos sistemas).	5 - Aspectos do Sistema	4.2	Custo anual de sustentação

Continua na Próxima Página

Nr.	Assertiva do PPSI	Critério	Nr.	Subcritério
24.01	Local de hospedagem do sistema.	5 - Aspectos do Sistema	5.3	Local de Hospedagem
24.02	Responsável pela hospedagem.	5 - Aspectos do Sistema	5.4	Responsável Hospedagem

Para garantir uma análise mais eficiente, a estrutura dos critérios foi refinada para refletir as inter-relações entre os subcritérios e os impactos previstos. O agrupamento dos critérios foi essencial para simplificar o modelo hierárquico, mantendo, contudo, a consistência com os principais fatores de criticidade identificados na literatura.

5.4.1 Desenvolvimento e Ajustes do Modelo Hierárquico de Decisão

Com a categorização das Assertivas em critérios e subcritérios concluída, foi estruturado um modelo hierárquico de decisão com base no método AHP. Esse modelo foi desenvolvido a partir de seis grandes critérios, conforme ilustrado na Figura 5.10. Cada critério foi desdobrado em subcritérios específicos, organizados de forma a refletir tanto a relevância das questões apresentadas no framework do PPSI quanto os achados teóricos identificados na revisão de literatura. Cabe destacar que os critérios 4, 5 e 6, embora não tenham sido explicitamente mencionados na literatura analisada, foram incluídos no modelo inicial com o propósito de possibilitar uma análise ampliada e criteriosa. Essa inclusão evidencia que o guia do PPSI propõe uma abordagem mais abrangente do que apenas a definição de infraestruturas críticas, como pode ser observado na Tabela 5.22, que reúne as assertivas 13 a 22, voltadas à caracterização da vulnerabilidade dos sistemas avaliados.

Figura 5.10: Modelo inicial de hierarquização de critérios e subcritérios

5.4.2 Reclassificação e Modelo Final

Para alinhar o modelo de forma mais precisa às descobertas da literatura, os subcritérios foram ajustados, assegurando uma aplicação mais adequada do modelo hierárquico. Por exemplo, na Figura 5.10, os critérios e subcritérios relacionados ao critério 6, ligados ao Estado, e aos critérios 4 e 5, relacionados à organização e destacados em azul, foram desconsiderados devido à ausência de correspondência clara com os critérios estabelecidos na literatura.

Além disso, houve a reclassificação do subcritério 4.7 - Reputação, que foi transferido para o critério 3 - Geográfico e Interdependência, por apresentar maior relação com os subcritérios encontrados. Destaca-se ainda a inclusão dos subcritérios 2.3 e 2.4 no critério Econômico, detalhando os efeitos negativos na execução da política econômica do Brasil (fiscal, monetária e cambial) e em programas econômicos. Essa alteração decorreu do desdobramento da assertiva 11 do PPSI, que originalmente abordava de forma ampla os impactos econômicos. Ao especificar esses subcritérios, o modelo final Figura 5.11 passou a refletir de maneira mais precisa a relevância dos efeitos sistêmicos sobre a condução da política econômica nacional e sobre programas estruturantes.

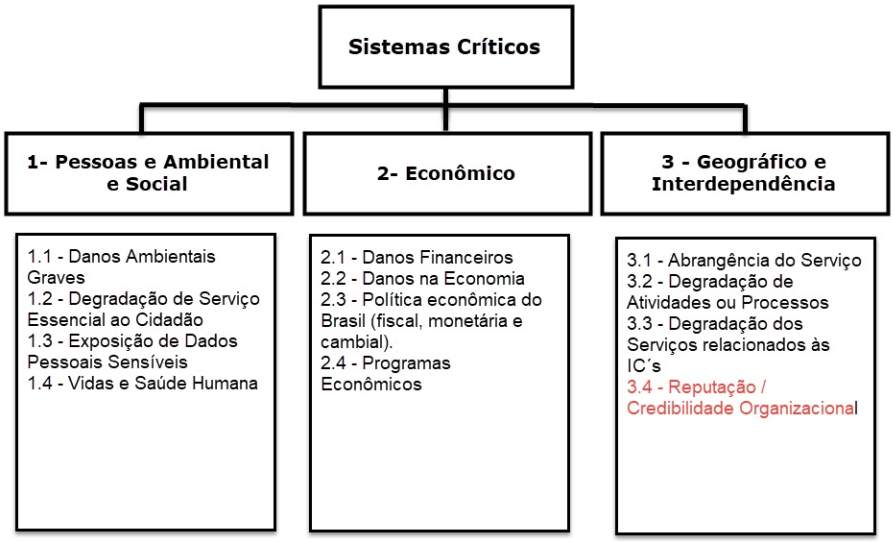


Figura 5.11: Modelo final de hierarquização de critérios e subcritérios

Esse processo de análise e ajustes foi fundamental para garantir que o modelo proposto tenha aderência tanto ao framework do PPSI quanto aos critérios de criticidade estabelecidos na literatura.

5.4.3 Análise das Diferenças Metodológicas entre o PPSI e o Modelo Proposto

Existem distinções relevantes entre o método do PPSI e o modelo proposto nesta pesquisa. A metodologia do PPSI fundamenta-se em uma abordagem centrada no impacto e na vulnerabilidade, com o uso das assertivas que, em alguns casos, não foram diretamente identificadas na literatura analisada. Isso, contudo, não invalida o valor da metodologia, já que novos modelos podem propor abordagens complementares e inovadoras, mesmo que ainda não tenham sido amplamente discutidas academicamente. Especificamente, o modelo do PPSI inclui questões sobre impactos não mapeados na revisão de literatura e contempla vulnerabilidades avaliadas com base em assertivas relacionadas à existência de controles de segurança — aspecto que, embora não observado nos estudos dos países analisados, pode representar uma contribuição original e relevante do método.

Em contraste, o modelo hierárquico proposto nesta pesquisa foi desenvolvido para aplicação em métodos multicritério, estruturando critérios e subcritérios de avaliação exclusivamente com base em fundamentos consolidados na literatura internacional sobre infraestruturas críticas. Diferentemente do modelo

do PPSI, que incorpora assertivas relacionadas à existência de controles de segurança e à avaliação de vulnerabilidades — elementos típicos da gestão operacional e não da definição de criticidade —, o modelo hierárquico proposto limita-se a critérios puramente associados aos diversos impactos potenciais, como aqueles decorrentes da interrupção ou degradação de serviços essenciais.

Assim, a principal diferença reside no fato de que o modelo hierárquico exclui critérios vinculados a controles ou à avaliação de vulnerabilidades, concentrando-se apenas em aspectos de impacto (como consequências sociais, econômicas, ambientais e de continuidade de serviços), em total alinhamento com as melhores práticas internacionais para definição de infraestruturas críticas. Essa abordagem assegura maior aderência conceitual ao objetivo de identificar o que é, de fato, uma infraestrutura crítica, sem misturar questões de maturidade de controles ou gestão de riscos operacionais, que são etapas posteriores e distintas no ciclo de proteção desses ativos.

5.4.4 Limitações e Sugestões de Melhoria para o Modelo PPSI

Ao concluir a análise, foram identificados alguns pontos no modelo do PPSI que podem ser aprimorados para tornar a identificação e priorização de sistemas críticos mais eficaz e alinhada com a literatura internacional.

Em primeiro lugar, o modelo do PPSI inclui assertivas relacionadas a critérios que ainda não foram observados na literatura dos países estudados. Embora a inclusão de critérios sem correspondência direta na literatura possa trazer desafios quanto ao alinhamento com práticas internacionais, ela também pode representar uma abordagem inovadora, contribuindo com novas perspectivas para a avaliação de segurança. Assim, é importante considerar que a adoção de critérios originais deve ser acompanhada de uma análise crítica, buscando assegurar que as avaliações resultantes estejam sensíveis tanto às necessidades específicas do contexto quanto às melhores práticas já estabelecidas.

Além disso, o modelo do PPSI contempla assertivas relacionadas a controles de segurança para avaliar vulnerabilidades. No entanto, não há precedentes na literatura consultada para esse tipo de avaliação no contexto da identificação de infraestruturas críticas. Avaliar vulnerabilidades com base apenas na existência de controles pode ser problemático, pois a mera presença de um controle de segurança não garante a mitigação de uma vulnerabilidade. Somente após a realização de testes e avaliações aprofundadas é possível determinar se há riscos residuais. Dessa forma, incorporar essa abordagem pode levar a uma falsa sensação de segurança ou a subestimar a criticidade de determinados sistemas.

Por fim, a distribuição dos pesos no modelo do PPSI não reflete os achados na literatura internacional, e não há documentação clara sobre o método utilizado. A falta de transparência na atribuição dos pesos pode comprometer a confiabilidade e a replicabilidade do modelo. Sem uma justificativa sólida ou uma metodologia claramente definida, torna-se difícil assegurar que a priorização dos sistemas críticos esteja alinhada com os critérios mais relevantes e reconhecidos internacionalmente.

Diante desses pontos, recomenda-se uma revisão do modelo do PPSI para alinhá-lo mais estreitamente com as práticas internacionais e com os critérios identificados na literatura. Isso inclui a reavaliação das assertivas utilizadas e a reconsideração da inclusão de avaliações de vulnerabilidades, independentemente de serem baseadas apenas na existência de controles ou não, pois a identificação de infraestruturas críticas

está relacionada aos impactos conforme os achados na literatura.

Além disso, é fundamental uma definição clara e justificada dos pesos atribuídos a cada critério. Ao implementar essas melhorias, o modelo poderá oferecer uma identificação e priorização de sistemas críticos mais precisa e eficaz, contribuindo para a segurança e a resiliência.

6 CONCLUSÃO

O presente capítulo finaliza a dissertação apresentando uma reflexão integrada sobre os principais resultados obtidos, destacando as contribuições, limitações e implicações do estudo. Diferentemente das demais seções, aqui buscou-se não apenas retomar os objetivos inicialmente traçados, mas também oferecer uma visão ampla e crítica sobre o alcance e a aplicabilidade do modelo desenvolvido. Ademais, são indicadas as perspectivas de continuidade da pesquisa, fortalecendo seu papel no avanço da gestão e proteção das infraestruturas críticas no contexto nacional.

Ao longo desta conclusão, serão sintetizados os insights metodológicos, as evidências internacionais comparativas, as inovações científicas, e a aplicabilidade prática do trabalho. Também são apresentadas as restrições identificadas e as oportunidades para aprofundamento futuro, explicitando o compromisso com a rigidez acadêmica e com as demandas do campo de segurança cibernética e gestão de riscos. Dessa forma, o capítulo encerra a dissertação com um panorama consolidado, garantindo uma compreensão clara, sistêmica e reflexiva dos temas abordados.

6.1 SÍNTESE DOS PROCEDIMENTOS E ROBUSTEZ METODOLÓGICA

O trabalho partiu de uma abordagem metodológica, combinando análise documental extensa (englobando normativos, diretrizes e relatórios técnicos de doze países e do PPSI), técnicas de categorização e refinamento hierárquico. Essa trajetória permitiu alcançar um modelo hierárquico para avaliação de criticidade, estruturado em três níveis e compatível com métodos multicritério como o AHP. O modelo excluiu critérios não validados pela literatura, demonstrando alinhamento metodológico internacional.

6.2 ALINHAMENTO E COMPARAÇÃO INTERNACIONAL

A análise comparada revelou convergência entre países em torno dos grandes eixos de impacto (pessoas, social, econômico), mas também disparidades quanto ao detalhamento e à composição de setores transversais — destacando o papel central dos setores de energia e TIC e a particularidade estoniana da informação digital como fator crítico. A ausência de um modelo universal indica que, apesar dos padrões globais, a aplicação nacional exige adaptação contextual baseada em evidências.

6.3 INOVAÇÃO E CONTRIBUIÇÃO CIENTÍFICA

Como principal avanço conceitual da pesquisa, foi apresentada a primeira síntese sistematizada dos critérios e subcritérios de doze jurisdições, adaptando-os ao contexto brasileiro em 12 subcritérios opera-

cionais. Ao propor uma estrutura compatível com técnicas multicritério, este trabalho preenche lacunas identificadas na literatura nacional e sinaliza oportunidades para novas pesquisas empíricas, superando a predominância dos modelos qualitativos.

6.4 APLICABILIDADE PARA POLÍTICAS PÚBLICAS E SETORES ESTRATÉGICOS

O modelo desenvolvido serve como referencial prático para órgãos públicos (notadamente o SISP) e reguladores setoriais, permitindo maior padronização na priorização de ativos críticos, facilitando auditorias do TCU, revisões do Anexo I do PPSI e subsidiando decisões de alocação de recursos. Na esfera privada, especialmente em setores como energia, finanças e telecomunicações, o modelo pode guiar escolhas mais racionais de investimentos em segurança, evitando a multiplicidade de controles redundantes.

6.5 LIMITAÇÕES E RESTRIÇÕES DO ESTUDO

Reconhece-se que o presente estudo, embora contribua metodologicamente, não realizou a atribuição de pesos nem a validação do modelo por meio de estudos de caso reais, limitando inferências sobre efetividade operacional. A ênfase em fontes documentais pode ter suprimido particularidades setoriais, sobretudo naqueles domínios com baixa transparência normativa. Outro ponto de ressalva é a mistura de critérios de impacto e vulnerabilidade no modelo PPSI, identificando a necessidade de separação mais nítida entre avaliação de criticidade e maturidade de controles — aspecto ainda em desenvolvimento no Brasil.

6.6 PROPOSTAS PARA PESQUISA APLICADA E PERSPECTIVAS FUTURAS

Diante das oportunidades e desafios identificados, sugere-se como próximos passos:

1. **Validação empírica** do modelo em setores estratégicos (energia, água, saúde);
2. **Atribuição de pesos** por métodos participativos, gerando índices comparáveis (*benchmarking*) entre órgãos e setores;
3. **Revisão periódica** do modelo, acompanhando as rápidas mudanças tecnológicas, regulatórias e geopolíticas do cenário nacional e internacional.

Em síntese, este estudo propõe ao Brasil migrar de abordagens reativas — baseadas em listas genéricas e controles fragmentados — para uma gestão proativa e científica da resiliência das infraestruturas críticas, em alinhamento com o PLANSIC, E-Ciber e diretrizes globais. Ao articular fundamentação teórica internacional, rigor metodológico, análise empírica e aplicabilidade, o trabalho oferece um referencial evolutivo e prático para a classificação de ativos e para a modernização da governança em segurança, contribuindo para apoiar decisões baseadas em critérios transparentes e reconhecidos.

REFERÊNCIAS BIBLIOGRÁFICAS

1 LIMA, E. O.; MOREIRA, F. R.; DEUS, F. E. G.; NZE, G. D. A.; JúNIOR, R. T. S.; NUNES, R. R. Avaliação da rotina operacional do operador nacional do sistema elétrico brasileiro (ons) em relação às ações de gerenciamento de riscos associados à segurança cibernética. 2022.

2 JUUSO, S. *Evaluation of threat modeling methodologies: A case study*. Dissertação (Mestrado), 2019.

3 BROOKS, C. Cybersecurity trends statistics for 2023; what you need to know. *Forbes*, 2023.

4 MAVROEIDIS, V.; BROMANDER, S. Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence. In: IEEE. *2017 European Intelligence and Security Informatics Conference (EISIC)*. [S.l.], 2017. p. 91–98.

5 BRUMFIELD, C.; HAUGLI, B. *Cybersecurity Risk Management: Mastering the fundamentals using the NIST Cybersecurity Framework*. [S.l.]: John Wiley & Sons, Inc., Hoboken, NJ, 2023.

6 Presidência da República. *Decreto nº 11.200, de 15 de setembro de 2022. Plano Nacional de Segurança de Infraestruturas Críticas - Plansic*. 2022. Secretaria-Geral, Subchefia para Assuntos Jurídicos.

7 KISSOON, T. *Optimal spending on cybersecurity measures: Risk Management*. [S.l.]: Routledge, Abingdon, Oxon, 2022.

8 BARAN, L. R.; TROJAN, F.; KOVALESKI, J. L.; PIECHINICKI, A. S. Métodos e ferramentas aplicados na análise de criticidade em sistemas industriais. In: *III Congresso Brasileiro de Engenharia de Produção*. Ponta Grossa, PR, Brasil: [s.n.], 2013. Ponta Grossa, PR, Brasil, 04 a 06 de dezembro de 2013. Disponível em: <mailto:leandro.baran@ifpr.edu.br>.

9 PúBLICOS, S. de Governo Digital do Ministério da Gestão e da Inovação em S. *Guia do Framework de Privacidade e Segurança da Informação*. Brasília, 2024.

10 North American Electric Reliability Corporation. *Cyber Security – Critical Asset Identification*. Washington, DC: [s.n.], 2006.

11 STERGIOPOULOS, G.; KOTZANIKOLAOU, P.; THEOCHARIDOU, M.; GRITZALIS, D. Risk mitigation strategies for critical infrastructures based on graph centrality analysis. *Int. J. Crit. Infrastruct. Protect.*, v. 10, p. 34–44, 2015.

12 KOHNKE, A.; SHOEMAKER, D.; SIGLER, K. *The Complete Guide to Cybersecurity Risks and Controls*. Boca Raton: Auerbach, 2022.

13 LEIRVIK. *Understand, Manage, and Measure Cyber Risk: Practical Solutions for Creating a Sustainable Cyber Program*. [S.l.]: Apress L. P., Berkeley, CA, 2023.

14 CORALLO, A.; LAZOI, M.; LEZZI, M. Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Computers in Industry*, v. 114, p. 103165, 2020.

15 BARCLAY, C. Sustainable security advantage in a changing environment: The cybersecurity capability maturity model (cm2). In: *IEEE*. [S.l.: s.n.], 2014. p. 6858466.

16 ANTONI, M.; AMMAD, N. Argus project-harnessing asset management to do cyber security to an uic guideline for railways. In: *Congrès Lambda Mu 21 «Maîtrise des risques et transformation numérique: opportunités et menaces»*. [S.l.: s.n.], 2018.

17 MATSUMOTO, N.; FUJITA, J.; ENDOH, H.; YAMADA, T.; SAWADA, K.; KANEKO, O. Asset management method of industrial iot systems for cyber-security countermeasures. *Information*, v. 12, n. 11, p. 460, 2021.

18 LUIIJF, E.; BURGER, H.; KLAVER, M. Critical (information) infrastructure protection in the netherlands. *9-19*, 2003.

19 FARIA, N. C. *Estratégia de Cibersegurança*. Dissertação (Mestrado) — Universidade do Minho, Portugal, 2022. Disponível em: <https://repositorium.sdum.uminho.pt/bitstream/1822/84478/1/Nelson%20Correia%20Faria.pdf>.

20 TRINDADE, M. B.; TOME, S. M. C.; RIBEIRO, S. L.; CUCULO, C. M. S.; LAGE, L. M.; MARTINO, E.; SOUZA, R. M. F. Metodologia para identificação da infraestrutura crítica de telecomunicações e sua aplicação em estudo de caso. In: *Conferencia Ibero-Americana de Ingeniería e Innovación Tecnológica: CIIIT*. [S.l.: s.n.], 2009. III.

21 National Cyber Security Centre. *Asset management*. 2024. Disponível em: <https://www.ncsc.gov.uk/collection/10-steps/asset-management>.

22 Emergency Management Australia. *Critical Infrastructure Emergency Risk Management and Assurance Handbook*. [S.l.]: Mount Macedon, Australia, 2003.

23 FARAMONDI, L.; OLIVA, G.; SETOLA, R. Multi-criteria node criticality assessment framework for critical infrastructure networks. *International Journal of Critical Infrastructure Protection*, v. 100338, 2020.

24 FEKETE, A. Common criteria for the assessment of critical infrastructures. *International Journal of Disaster Risk Science*, v. 2, p. 15–24, 2011.

25 Federal Ministry of the Interior of Germany. *National Strategy for Critical Infrastructure Protection (CIP Strategy)*. [S.l.]: Berlin, 2009.

26 Comissão Europeia. *Estabelece um procedimento de identificação e designação das infra-estruturas críticas europeias e uma abordagem comum relativa à avaliação da necessidade de melhorar a sua protecção (Diretiva n.º 2008/114/CE de 8 de Dezembro)*. [S.l.]: Bruxelas: Jornal Oficial da União Europeia, 2008.

27 THEOHARIDOU, M.; KOTZANIKOLAOU, P.; GRITZALIS, D. Risk-based criticality analysis. In: *Critical Infrastructure Protection III. Proceedings. Third Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection. Hanover, New Hampshire, USA*. [S.l.: s.n.], 2009. p. March 23–25.

28 SETOLA, R.; SFORZA, A.; VITTORINI, V.; PRAGLIOLA, C. *Railway Infrastructure Security*. [S.l.]: Springer, 2015.

29 TIERNEY, K.; BRUNEAU, M. Conceptualizing and measuring resilience: A key to disaster loss reduction. *TR News May-June*, p. 14–17, 2007.

30 COLLIER, S.; LACKOFF, A. The vulnerability of vital systems: how "critical infrastructure"became a security problem. In: *Securing "the Homeland": critical infrastructure, risk and (in)security*. [S.l.]: Dunn, Myriam; Kristensen, Kristian. Londres, 2008.

31 NATáRIO, R. *O Ciberespaço e a Vulnerabilidade das Infraestruturas Críticas: Contributos para um Modelo Nacional de Análise e Gestão do Risco Social*. [S.l.]: Academia Militar, Lisboa, 2014.

32 Comissão Europeia. *COM 702 Protecção das infra-estruturas críticas no âmbito da luta contra o terrorismo*. [S.l.]: Bruxelas: Comissão Europeia, 2004.

33 Presidência da República do Brasil. *Guia de referência para a segurança das infraestruturas críticas da informação. Versão 01 – Nov./2010*. 2010. Organizado por Claudia Canongia, Admilson Gonçalves Júnior e Raphael Mandarino Junior, Brasília - DF.

34 DUNN, M. The socio-political dimensions of critical information infrastructure protection (ciip). *International Journal of Critical Infrastructures*, v. 1, n. 2-3, p. 258–268, 2005.

35 Netherlands National Coordinator for Counterterrorism and Security. *Factsheet Critical Infrastructure ENG 2018*. 2018. Disponível em: <https://english.nctv.nl/binaries/nctv-en/documenten/publications/2018/02/01/factsheet-criticalinfrastructure/Factsheet+Critical+Infrastructure+ENG+2018.pdf>.

36 BOUCHON, S. *The Vulnerability of interdependent Critical Infrastructures Systems: Epistemological and Conceptual State of the Art*. [S.l.]: Ispra: Institute for the Protection and Security of the Citizen, 2006.

37 MOTEFF, J.; COPELAND, C.; FISCHER, J. *Critical Infrastructures: What Makes an Infrastructure Critical?* [S.l.], 2003.

38 ANGELONI, M. T. Elementos intervenientes na tomada de decisão. *Ciência da Informação*, v. 32, p. 17–22, 2003.

39 SAATY, T. L. *The Analytic Hierarchy Process*. New York: McGraw-Hill, 1980.

40 MU, E.; PEREYRA-ROJAS, M. *Practical Decision Making*. [S.l.]: Springer, 2017. (SpringerBriefs in Operations Research).

41 CHENG, E. W.; LI, H. Information priority-setting for better resource allocation using analytic hierarchy process (ahp). *Information Management & Computer Security*, v. 9, n. 2, p. 61–70, 2001.

42 DARKO, A.; CHAN, A. P. C.; AMEYAW, E. E.; OWUSU, E. K.; PäRN, E.; EDWARDS, D. J. Review of application of analytic hierarchy process (ahp) in construction. *International Journal of Construction Management*, v. 19, n. 5, p. 436–452, 2019.

43 SAATY, T. L. *Fundamentals of Decision Making and Priority Theory With the Analytic Hierarchy Process - Ebook Edition*. [S.l.]: RWS Publications, 2013.

44 ROCHE, H.; VEJO, C. *Analisis multicriterio en la toma de decisiones. Métodos Cuantitativos aplicados a la administración. Analisis multicritério – AHP*. 2004. Material apoio AHP, 11 f.

45 SAATY, T. L. *Fundamentals of Decision Making and Priority Theory with the Analytic Hierarchy Process*. Pittsburgh: RWS Publications, 2000.

46 FREITAS, A. L. P.; MARINS, C. S.; SOUZA, D. de O. A metodologia de multicritério como ferramenta para a tomada de decisões gerenciais: um estudo de caso. *GEPROS - Gestão da Produção, Operações e Sistemas*, v. 1, n. 3, p. 51–60, 2006.

47 BRASIL. *Sobre o SISP*. n.d. Ministério da Gestão e da Inovação em Serviços Públicos. Disponível em: <https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/sisp/sobre-o-sisp>.

48 FERREIRA, H. J. D. *Identificação e Caraterização de Infraestruturas Críticas – Uma Metodologia*. Pedrouços: [s.n.], 2016. Trabalho de Investigação Individual do Curso de Estado-Maior Conjunto, Instituto Universitário Militar. Orientador: Major de Infantaria Hugo Miguel Moutinho Fernandes.

49 ITURRIZA, M.; LABAKA, L.; SARRIEGI, J. M.; HERNANTES, J. Modelling methodologies for analysing critical infrastructures. *Journal of Simulation*, v. 12, n. 2, p. 128–143, 2018.

50 Gabinete de Segurança Institucional da Presidência da República. *Guia de Referência para a Segurança das Infraestruturas Críticas da Informação*. Brasília, 2010. Versão 1. Disponível em: <https://www.itu.int/en/itu-d/cybersecurity/documents/national_strategies_repository/brazil_2010_orig_2_guia_sici.pdf>.

51 Brasil. *Decreto n.º 9.573, de 22 de Novembro de 2018 – Aprova a Política Nacional de Segurança de Infraestruturas Críticas (PNSIC)*. 2018. <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9573.htm>. Diário Oficial da União, 23 nov. 2018.

52 Brasil. *Decreto n.º 10.569, de 9 de Dezembro de 2020 – Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas (ENSIC)*. 2020. <https://www.planalto.gov.br/cCivil_03/_Ato2019-2022/2020/Decreto/D10569.htm>. Diário Oficial da União, 10 dez. 2020.

53 Brasil. *Decreto n.º 11.200, de 15 de Setembro de 2022 – Aprova o Plano Nacional de Segurança de Infraestruturas Críticas (PLANSIC)*. 2022. <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/Decreto/D11200.htm>. Diário Oficial da União, 16 set. 2022.

54 Brasil. *Decreto n.º 10.222, de 5 de Fevereiro de 2020 – Aprova a Estratégia Nacional de Segurança Cibernética (E-Ciber)*. 2020. <https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Decreto/d10222.htm>. Diário Oficial da União, 6 fev. 2020.

55 GIL, A. C. *Como elaborar projetos de pesquisa*. 4. ed. [S.l.]: Atlas, São Paulo, 2009.

56 MARCONI, M. A.; LAKATOS, E. M. *Fundamentos de metodologia científica*. 5. ed. [S.l.]: Atlas, 2003.

57 MINAYO, M. C. D. S. *Pesquisa Social: Teoria, Método e Criatividade*. 21. ed. [S.l.]: Editora Vozes, Petrópolis, 2002.

58 European Commission. *COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection*. 2008. 75–82 p. Disponível em: <http://eur-lex.europa.eu/JOIndex.do>.

59 Comissão Europeia. *Protecção das infra-estruturas críticas no âmbito da luta contra o terrorismo*. Bruxelas: Comissão Europeia, 2004.

60 Comissão Europeia. *SWD(2013) 318 A new approach to the European Programme for Critical Infrastructure Protection: Making European Critical Infrastructures more secure*. Bruxelas, 2013.

61 Centro Nacional para la Protección de las Infraestructuras Críticas. *CNPIC - Importancia de las Infraestructuras*. 2024. Disponível em: <https://cnpic.interior.gob.es/es/que-hace-el-cnpic/importancia-de-las-infraestructuras/>.

62 Jefatura del Estado. *Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas*. Madrid: Boletín Oficial del Estado, 2011.

63 Ministerio del Interior. *Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas*. Madrid: Boletín Oficial del Estado, 2011.

64 Ministério da Defesa Nacional. *Estabelece os procedimentos de identificação e de protecção das infraestruturas essenciais para a saúde, a segurança e o bem-estar económico e social da sociedade nos sectores da energia e transportes (Decreto-Lei n.º 62/2011 de 9 de maio)*. Lisboa: Diário da República, 2011.

65 PAIS, I. *Proteção de Infraestruturas Críticas - A Classificação e Identificação de Infraestruturas Críticas Nacionais*. Lisboa, 2015.

66 Netherlands National Coordinator for Counterterrorism and Security. *Critical infrastructure protection*. 2018. Acesso em: 22 maio 2024. Disponível em: <https://english.nctv.nl/topics/critical-infrastructure-protection>.

67 Cabinet Office. *Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards*. [S.l.]: Londres: Crown, 2010.

68 Cabinet Office. *A Summary of the Sector Resilience Plans for Critical Infrastructure 2010/2011*. London, UK, 2011. Disponível em: <https://assets.publishing.service.gov.uk/media/5a7c7da840f0b626628ac6fc/sector-resilience-plan-2011.pdf>.

69 GORDON, K.; DION, M. *Protection of 'Critical Infrastructure' and the role of Investment Policies Relating to National Security*. [S.l.]: Paris: Organisation for Economic Co-operation and Development, 2008.

70 House of Representatives of the United States of America. *USA PATRIOT ACT 2001*. Washington: House of Representatives, 2001.

71 The White House. *PPD-21 Critical Infrastructure Security and Resilience*. Washington: Office of the Press Secretary, 2013.

72 Department of Homeland Security. *Dam Sector-Specific Plan*. Washington: s.n., 2015.

73 Department of Homeland Security. *Water Sector-Specific Plan*. Washington: s.n., 2010.

74 Department of Homeland Security. *Information Technology Sector-Specific Plan*. Washington: s.n., 2010.

75 Department of Homeland Security. *Dam Sector-Specific Plan*. Washington: s.n., 2015.

76 Department of Homeland Security. *Financial Services-Specific Plan*. Washington: s.n., 2015.

77 Department of Homeland Security. *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*. Washington, DC, 2013. Disponível em: <https://www.nist.gov/system/files/documents/cybercommission/-DHS-_National_Infrastructure_Protection_Plan_-NIPP.pdf>.

78 Government of Canada. *National Strategy for Critical Infrastructure*. 2009.

79 National Critical Infrastructure Assurance Program. *Selection Criteria to Identify and Rank Critical Infrastructures Assets*. [S.l.]: Public Safety and Emergency Preparedness Canada, 2004.

80 BRUNNER, E. M.; SUTER, M. *International CIIP Handbook 2008/2009*. Zurique: Center for Security Studies, 2008.

81 Government of Canada. *Position Paper on a National Strategy for Critical Infrastructure Protection*. s.l.: Government of Canada, 2004.

82 Cyber and Infrastructure Security Centre (CISC). *Critical Infrastructure Resilience Strategy 2023*. 2023. Disponível em: <https://www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-resilience-strategy-2023.pdf>.

83 Department of Home Affairs. *Critical Infrastructure Resilience Strategy*. Canberra, Australia, 2023. Disponível em: <https://www.cisc.gov.au/resources-subsite/Documents/critical-infrastructure-resilience-strategy-2023.pdf>.

84 Department of Home Affairs. *Protecting Critical Infrastructure and Systems of National Significance: Consultation Paper*. Canberra, Australia, 2019. Disponível em: <https://www.homeaffairs.gov.au/reports-and-pubs/files/protecting-critical-infrastructure-systems-consultation-paper.pdf>.

85 National Center of Incident Readiness and Strategy for Cybersecurity (NISC). *The Second Action Plan of Information Security Measures for Critical Infrastructures*. Japão: [s.n.], 2009. Acesso em: 23/05/2024. Disponível em: <https://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v2.pdf>.

86 AUNG, Z. Z.; WATANABE, K. A framework for modeling interdependencies in japan's critical infrastructures. In: *IFIP Advances in Information and Communication Technology*. Springer, 2009. p. 243–257. Disponível em: <https://dl.ifip.org/db/conf/ifip11-10/cip2009/AungW09.pdf>.

87 Qatar National Cyber Security Strategy. *National Cyber Security Strategy*. 2014. Disponível em: <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Qatar_2014_national_cyber_security_strategy.pdf>.

88 INFORMATION, M. of; TECHNOLOGY, C. *Qatar National Cyber Security Strategy*. Doha, Qatar, 2014. Disponível em: <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Qatar_2014_national_cyber_security_strategy.pdf>.

89 Department of Defense. *Strategic Emergency Management Guideline 3*. 2019. Disponível em: <https://assets.gov.ie/90982/957a78f1-5fd9-46a9-adfd-4af75a725c3e.pdf>.

90 (OEP), O. of E. P.; (GIS), G. I. S. *Strategic Emergency Management Guideline 3 – Critical Infrastructure Resilience*. Dublin, Ireland, 2019. Disponível em: <https://ppl-ai-file-upload.s3.amazonaws.com/web/direct-files/attachments/33722433/2c9880a4-7177-4045-83b3-278e942236ec/irlanda.pdf>.

91 Republic of Estonia Information System Authority (RIA). *Requirements for risk analysis of network and information systems and description of security measures*. 2018. Acesso em: 26 maio 2024. Disponível em: <https://www.ria.ee/en/cyber-security/cyber-defence-critical-infrastructure/cyber-defence-critical-infrastructure>.

92 AFFAIRS, M. of E.; COMMUNICATIONS. *Cybersecurity strategy 2024–2030: Cyber-conscious Estonia*. Tallinn, Estonia, 2024. Disponível em: <https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/EE_NCSS_2024_en.pdf>.

93 Qatar National Cyber Security Strategy. *Qatar National Cyber Security Strategy*. 2014. Disponível em: <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Qatar_2014_national_cyber_security_strategy.pdf>.