risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 15/02/2025
Aceitação/Acceptance: 12/06/2025

Tomada de Decisão em Segurança Cibernética: Modelo para Identificação de Joias da Coroa

Edvan Gomes da Silva[1], Marcus Aurélio Carvalho Georg[1],
Luiz Antônio Ribeiro Júnior[2], Leonardo Rodrigo Ferreira[3], Rafael Rabelo Nunes[1,4]

**edvan402@gmail.com; georg@stj.jus.br; ribeirojr@unb.br;
leonardo.r.ferreira@gestao.gov.br; rafaelrabelo@unb.br**

[1] Programa de Pós-Graduação Profissional em Engenharia Elétrica – PPEE - Universidade de Brasília, Faculdade de Tecnologia, Departamento de Engenharia Elétrica, Brasília, Brasil - Zipcode 70910-900.

[2] Laboratório de Materiais Computacionais, LCCMat, Instituto de Física, Universidade de Brasília, Brasília, Distrito Federal, Brasil.

[3] Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (MGI), Brasil.

[4] Centro Universitário UniAtenas, Paracatu-MG, Brasil – Zipcode 38602-108 .

Pages: 60-73

Resumo: A crescente dependência de organizações em sistemas críticos de tecnologia da informação, conhecidos como "Joias da Coroa", torna essencial o desenvolvimento de métodos eficazes para sua identificação e avaliação. Este estudo propõe uma abordagem estruturada para classificar ativos críticos no contexto dos órgãos do Poder Executivo Federal brasileiro. A metodologia adotada envolveu revisão de literatura, aplicação de questionários a 57 gestores do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) e sessões colaborativas de brainstorming para definir e validar critérios e subcritérios. Como resultado, foram identificados cinco critérios principais: Missão da Organização, Imagem e Reputação, Volume de Usuários Afetados, Impacto Financeiro e Impacto Legal/Regulatório, organizados em um modelo hierárquico. A principal contribuição deste estudo é a formulação de uma metodologia estruturada que integra bases teóricas e validação empírica, proporcionando um modelo adaptável a diferentes contextos organizacionais e aprimorando a gestão de riscos e segurança cibernética.

Palavras-chave: Gestão de Riscos, Infraestrutura críticas, Resiliência Organizacional, Análise multicritério, Priorização de ativos.

Decision-Making in Cybersecurity: A Model for Identifying Crown Jewels

Abstract: The increasing reliance of organizations on critical information technology systems, known as "Crown Jewels," underscores the need for effective methods for their identification and evaluation. This study presents a structured approach to classifying critical IT assets within the Brazilian Federal Executive

Branch. The methodology involved a literature review, surveys with 57 System for the Administration of Information Technology Resources (SISP) managers, and collaborative brainstorming sessions to define and validate criteria and subcriteria. The findings identified five key criteria: Organizational Mission, Image and Reputation, Affected User Volume, Financial Impact, and Legal/Regulatory Impact, organized into a hierarchical model. The main contribution of this study is the development of a structured methodology that integrates theoretical foundations with empirical validation, providing an adaptable model for various organizational contexts while enhancing risk management and cybersecurity practices.

Keywords: Risk Management, Critical Infrastructure, Organizational Resilience, Multicriteria Analysis, Criticality Assessment.

1. Introdução

Os ataques cibernéticos representam uma ameaça significativa às infraestruturas críticas, impactando diretamente a estabilidade social e econômica (Glenn, Sterbentz & Wright, 2016; Varga, Brynielsson & Franke, 2021). Empresas e organizações dependem cada vez mais de sistemas essenciais de tecnologia da informação (TI), frequentemente chamados de "Joias da Coroa", cuja criticidade pode ser definida pelas funções e dados que hospedam (Brunner & Suter, 2008). Segundo o MITRE (2025), a Análise de Joias da Coroa (AJC) é um método para identificar ativos críticos de TI baseados na missão da organização, sendo parte de um conjunto mais amplo de abordagens para avaliação de criticidade.

Nesse contexto, a gestão de riscos torna-se fundamental para garantir a segurança cibernética. Como destacado por Brumfield e Haugli (2023), o planejamento estratégico e a gestão de riscos são passos essenciais para orientar uma organização em direção à segurança digital. A identificação de riscos e a avaliação do valor crítico dos ativos são indispensáveis para um gerenciamento eficaz da segurança da informação, permitindo a implementação de medidas para mitigar ameaças e assegurar a continuidade das operações.

A identificação adequada dos ativos críticos requer métodos estruturados que considerem apetite ao risco, medidas de mitigação, impacto nos negócios e contramedidas específicas (Kissoon, 2022). No setor público brasileiro, uma das principais lacunas na gestão de segurança cibernética é a baixa percepção da alta administração sobre a importância estratégica do tema, resultando em uma governança frágil e, em muitos casos, inexistente. Essa deficiência leva a um distanciamento entre gestores técnicos e tomadores de decisão, dificultando a implementação de políticas eficazes de segurança cibernética (Georg, Rodrigues, Júnior, Nunes, 2022).

Considerando esse cenário, este estudo tem como objetivo identificar critérios que podem ser utilizados para classificar um ativo como Joia da Coroa no âmbito dos órgãos do Poder Executivo Federal brasileiro. Para isso, a pesquisa foi estruturada em diversas seções. Além desta introdução, a Seção 2 apresenta o referencial teórico sobre gestão de ativos e análise de Joias da Coroa, abordando conceitos essenciais e critérios de identificação. A Seção 3 descreve a metodologia adotada, detalhando as etapas da pesquisa. A Seção 4 expõe os resultados obtidos, incluindo a análise dos critérios

identificados. Por fim, a Seção 5 apresenta as conclusões, consolidando os principais achados e sugerindo direções para estudos futuros.

2. Referencial Teórico

2.1. Gestão de Ativos

O Objetivo da cibersegurança é proteger sistemas e dados contra ameaças, abrangendo infraestrutura, ativos de informação, pessoas e processos (Barclay, 2014). No contexto da gestão de ativos, a identificação e classificação dos ativos críticos são etapas fundamentais para garantir a segurança organizacional, permitindo a priorização da avaliação de vulnerabilidades e a implementação de medidas protetivas (Antoni & Ammad, 2018; Matsumoto et al., 2021).

A definição de ativos críticos é um desafio, pois não há uma abordagem universalmente aceita para essa categorização (Leirvik, 2023). O Framework do NIST enfatiza a importância da gestão de dados, dispositivos e sistemas com base em sua relevância estratégica para a organização (Brumfield & Haugli, 2023). Da mesma forma, a ISO 27.005:2023 classifica ativos em primários (essenciais para a missão organizacional) e de suporte (como hardware, software e recursos humanos) (Kissoon, 2022).

É importante ressaltar que a priorização dos ativos críticos é um aspecto central da gestão de ativos. A adoção de critérios bem definidos evita escopos excessivamente amplos, permitindo que a organização foque na proteção dos ativos mais estratégicos (Faria, 2022). A compreensão das funções críticas e das interdependências tecnológicas facilita a alocação eficiente de recursos e o fortalecimento da resiliência organizacional (National Cyber Security Center, 2024).

2.2. Identificação e Priorização de Ativos Críticos: A Análise de Joias da Coroa

A crescente sofisticação das ameaças cibernéticas exige metodologias inovadoras para proteger os ativos mais críticos das organizações. Nesse contexto, a Análise de Joias da Coroa (AJC) surge como uma abordagem estruturada para identificar e priorizar ativos cibernéticos essenciais para a missão organizacional (Singh, 2024; Musman et al., 2011). Esses ativos incluem dados sensíveis, propriedade intelectual e infraestruturas críticas, cujo comprometimento pode gerar impactos severos na continuidade operacional e na resiliência da organização (Kraven Security, 2024).

Vale ressaltar que a AJC vai além da simples identificação de ativos, avaliando seu valor estratégico em relação à missão da organização. Esse modelo permite a alocação eficiente de recursos, garantindo que as medidas de proteção sejam direcionadas aos ativos mais relevantes (Musman et al., 2011). O processo da AJC pode ser dividido em três etapas principais: I. Identificação dos ativos críticos, com base na importância estratégica do sistema ou dado para a organização; II. Avaliação do impacto de seu comprometimento, considerando fatores como consequências financeiras, operacionais e reputacionais; Modelagem de ameaças, visando estabelecer estratégias eficazes de proteção e mitigação de riscos (Kraven Security, 2024).

A caracterização dos ativos críticos é frequentemente realizada por meio de critérios qualitativos e quantitativos, que permitem avaliar os riscos e impactos associados. Modelos amplamente utilizados, como os adotados pela Comissão Europeia e pelo Plano Nacional de Proteção de Infraestruturas dos EUA, utilizam métricas como perdas financeiras, danos à reputação e interrupções operacionais para definir a criticidade dos ativos (Emergency Management Australia, 2003; European Commission, 2006; Theoharidou et al., 2009).

Além disso, metodologias multicritério têm se mostrado eficazes para a priorização de ativos essenciais, atribuindo pesos específicos aos fatores que sustentam a operação da organização (Center for Threat-Informed Defense, 2025). A definição de critérios objetivos evita que a organização liste um número excessivo de ativos como críticos, garantindo que os esforços sejam direcionados de maneira estratégica e eficiente (Moteff et al., 2003).

3. Metodologia

Este estudo adota uma abordagem aplicada, exploratória e descritiva. Sua natureza exploratória se justifica pelo objetivo de aprimorar conceitos e identificar padrões na classificação de Joias da Coroa, exigindo um planejamento flexível (Gil, 2009, p. 41). Já seu caráter descritivo reside na análise empírica das características dos ativos críticos e na avaliação de programas e variáveis-chave (Marconi & Lakatos, 2003, p. 187).

Além disso, a pesquisa tem uma abordagem predominantemente qualitativa, pois busca compreender e explorar significados, crenças e valores organizacionais, indo além da simples operacionalização de variáveis (Minayo, 2002, p. 21). O objetivo principal é propor critérios para classificar ativos críticos no contexto do Poder Executivo Federal brasileiro, combinando revisão de literatura, coleta de dados via questionários e desenvolvimento colaborativo de critérios e subcritérios.

A metodologia seguiu um processo estruturado em três etapas principais: (1) revisão de literatura, para identificar critérios validados cientificamente aplicáveis ao contexto organizacional; (2) coleta de dados, com aplicação de questionários a 57 gestores do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), permitindo a priorização dos critérios mais relevantes; e (3) desenvolvimento e validação de critérios e subcritérios, por meio de brainstorming estruturado, culminando na construção de um modelo hierárquico de avaliação. A Figura 1 ilustra essas etapas metodológicas.

A primeira etapa da pesquisa revelou uma lacuna na literatura: a ausência de estudos dedicados à definição sistemática de critérios para avaliar ativos críticos. Para preencher essa lacuna, foram analisadas publicações sobre impactos organizacionais em diversas áreas, permitindo a identificação inicial de um conjunto de critérios potenciais. A Tabela 1 apresenta os critérios identificados e suas respectivas referências.

Com o objetivo de validar esses critérios no contexto do SISP, aplicou-se um questionário a 57 gestores. Os participantes foram solicitados a indicar até cinco critérios que, em sua avaliação, são determinantes para classificar um sistema como crítico no âmbito do Poder Executivo Federal. A análise das respostas revelou os cinco critérios mais selecionados: Missão da Organização (85,2%), Imagem e Reputação (59,3%), Impacto

na Segurança (55,6%), Volume de Usuários Afetados (48,1%) e Impacto Financeiro (37,0%). Além disso, o critério Legal/Regulatório foi incluído na estrutura final do modelo, pois a legislação vigente exige sua consideração. A Figura 2, apresentada na próxima seção, illustra a priorização desses critérios.

Figura 1 – Etapas da pesquisa para definição dos critérios de Joias da Coroa. O estudo seguiu um processo estruturado que combinou revisão de literatura, questionários aplicados a gestores do SISP e desenvolvimento colaborativo de critérios e subcritérios.

Critério	Definição	Referência
1 - Impacto na Missão da Organização	Considera a importância do sistema para cumprir a missão institucional da organização. Sistemas são classificados como críticos se sua falha comprometer a entrega de serviços essenciais ao público.	(Fekete, 2011), (Hinchey & Margaria, 2014), (Aal & Martin, 2012)
2 - Impacto Legal e Regulatório	Examinar se o sistema é necessário para cumprir obrigações legais ou regulatórias.	(Fekete, 2011), (Rao & Krishna, 2015), (Davis, 1995), (Burnett, 1996)
3 - Impacto na Segurança	Avaliar o papel do sistema na segurança da informação e física da organização.	(Panzieri & Setola, 2008), (Cox & Robinson, 2004), (Burnett, 1996), (Ficco, 2016)
4 - Impacto Financeiro	Medir as consequências financeiras de falhas do sistema.	(Walls & Harley, 2022), (Bisogni & Cavallini, 2010), (Jonkeren et al., 2012), (Hyatt & Santos, 2022), (Lis & Mendel, 2019)
5 - Impacto na Imagem e Reputação	Avaliar como falhas do sistema afetariam a percepção pública da organização.	(Bennett et al., 1994), (Tervo & Wiander, 2010), (Pang, 2017)

Critério	Definição	Referência
6 - Dependência Interorganizacional	Considerar a importância do sistema em fornecer serviços essenciais colaborativos.	(Walls & Harley, 2022), (Li et al., 2022), (Schweikert, L'Her & Deinert, 2021)
7 - Complexidade e Exclusividade	Analisar a complexidade do sistema e a dificuldade de substituição ou recuperação.	(Onwubiko, 2012), (Bologna & Beer, 2003)
8 - Volume de Usuários Afetados	Avaliar o impacto de falhas do sistema com base no número de usuários internos e externos.	(Walls & Harley, 2022)
9 - Tempo de Recuperação Aceitável (RTO)	Definir o tempo máximo que um sistema pode estar inoperante após um incidente.	(Baginda, Affandi & Pratomo, 2018)
10 - Ponto de Recuperação Aceitável (RPO)	Estabelecer a quantidade máxima de perda de dados aceitável durante uma interrupção.	(Baginda, Affandi & Pratomo, 2018)
11 - Capacidade de Escalabilidade	Avaliar a capacidade do sistema de manejar aumentos significativos no volume de transações.	(Breaz & Jaradat, 2024)
12 - Integridade dos Dados	Considerar a importância da precisão e integridade dos dados gerenciados pelo sistema.	(Rao & Krishna, 2015)
13 - Redundância e Resiliência	Examinar a existência de redundâncias no sistema e sua capacidade durante falhas parciais.	(Hardy, 2014)
14 - Exclusividade de Recursos	Determinar se o sistema utiliza recursos que são exclusivos ou difíceis de substituir.	(Langemeier, 2016)
15 - Interconectividade e Interfaces	Avaliar a extensão da integração do sistema com outros sistemas.	(Walls & Harley, 2022)
16 - Impacto no Ambiente de Trabalho	Analisar como a falha do sistema afeta a capacidade dos funcionários de realizar suas funções.	(Shoniregun, 2004)

Tabela 1 – Critérios potenciais para identificação de Joias da Coroa. A tabela apresenta critérios extraídos da literatura, organizados por relevância em termos de impacto organizacional, legal, financeiro e operacional.

Partindo dos critérios priorizados pelos gestores, foi desenvolvida uma árvore de decisão hierárquica para facilitar a avaliação da criticidade dos ativos e sistemas. Esse modelo visa tornar a análise mais objetiva, permitindo a aplicação de métodos multicritério para avaliação de riscos e segurança cibernética. A estrutura hierárquica resultante está representada na Figura 3 (ver próxima seção) e oferece um framework adaptável a diferentes contextos organizacionais, contribuindo significativamente para a gestão de riscos no setor público.

A definição de subcritérios foi realizada de forma colaborativa, utilizando técnicas de brainstorming estruturado entre pesquisadores e gestores. Essas sessões tiveram como objetivo desenvolver e validar subcritérios específicos para cada critério principal, além

de discutir e definir indicadores mensuráveis que garantam uma categorização clara e objetiva dos impactos possíveis. Como resultado dessas discussões, foi elaborada uma tabela que organiza os critérios principais em agrupamentos mais amplos, permitindo uma aplicação prática do modelo hierárquico proposto.

4. Resultados e Discussões

4.1. Pesquisa e Critérios para o Modelo Organizacional

Com base na análise das respostas de 57 gestores vinculados ao Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), foram priorizados cinco critérios principais, conforme ilustrado na Figura 2. Os critérios destacados foram Missão da Organização, com 85,2% de relevância, seguido por Imagem e Reputação, com 59,3%, Impacto na Segurança, com 55,6%, Volume de Usuários Afetados, com 48,1%, e Impacto na Integridade dos Dados, com 40,7%. O critério Financeiro também foi considerado, com 37,0%. Além disso, o Impacto Legal e Regulatório foi apontado por 33,3% dos gestores. Como a legislação brasileira já contempla o impacto na integridade dos dados e na segurança, esse critério foi incorporado à lista principal para garantir uma abordagem abrangente.

A partir dessa priorização, foi desenvolvido um modelo hierárquico que organiza os critérios e seus respectivos subcritérios, apresentado na Figura 3. Esse modelo estrutura as dimensões avaliadas no contexto organizacional, com subcritérios definidos e refinados por meio de um processo colaborativo entre os pesquisadores, utilizando técnicas de brainstorming orientadas por uma análise crítica.

Durante essas sessões, foram discutidos aspectos específicos para detalhar e tornar mais objetiva a avaliação dos ativos críticos identificados como Joias da Coroa. No critério Missão da Organização, foram estabelecidos subcritérios como impacto na continuidade operacional, impacto em processos estratégicos e dependência de outros sistemas ou processos internos. O critério Imagem e Reputação foi detalhado com base em fatores como exposição midiática negativa, perda de confiança pública e impacto em parcerias estratégicas. Já o critério Volume de Usuários Afetados foi estruturado considerando a quantidade absoluta de usuários impactados diretamente, bem como a criticidade desses usuários, como cidadãos, servidores públicos ou gestores estratégicos.

Para o critério financeiro, os subcritérios definidos incluem custos diretos de recuperação após incidentes, perdas indiretas associadas à interrupção das operações e possíveis multas ou penalidades financeiras decorrentes do descumprimento regulatório. No critério Legal/Regulatório, foram incluídos aspectos como conformidade com legislações específicas, como a LGPD, obrigações contratuais com terceiros e implicações jurídicas associadas ao vazamento ou comprometimento de dados protegidos pela legislação vigente.

O modelo hierárquico desenvolvido sintetiza os resultados da pesquisa ao estruturar os critérios e subcritérios de forma visual, facilitando sua aplicação no contexto organizacional. Esse modelo pode servir como base para a avaliação dos ativos críticos por meio de métodos multicritérios. Para complementar a análise dos critérios e subcritérios definidos, foi elaborada uma categorização que organiza os critérios principais em

agrupamentos mais amplos, associando indicadores específicos a cada um deles. A Tabela 2 apresenta essa estrutura, destacando como os critérios foram detalhados em indicadores mensuráveis, permitindo uma avaliação mais objetiva e prática dos ativos críticos.

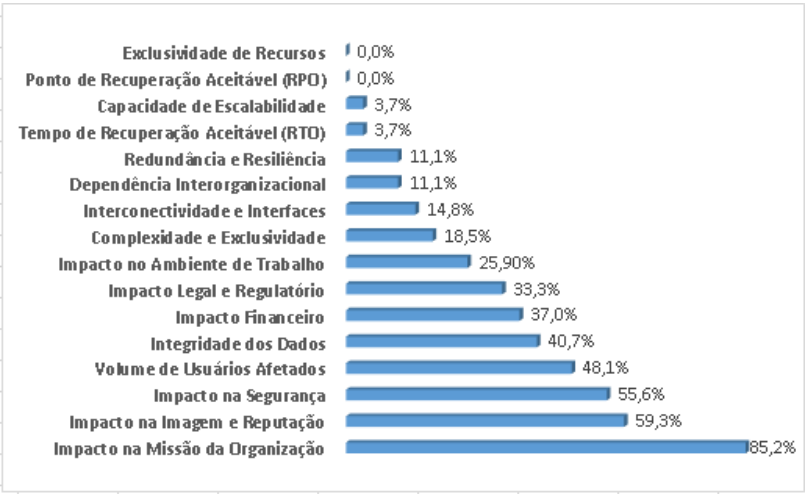

Figura 2 – Resultado da pesquisa sobre critérios para identificação de Joias da Coroa. Representação da frequência com que cada critério foi selecionado pelos 57 gestores do SISP no questionário aplicado, refletindo sua percepção sobre a criticidade dos ativos organizacionais.

Figura 3 – Modelo hierárquico para avaliação das Joias da Coroa. A estrutura organiza critérios e subcritérios em um modelo visual que auxilia a identificação e classificação de ativos críticos.

Critério	Indicadores	Critérios Agrupadores
Missão da Organização	Impacto na continuidade operacional, Impacto em processos estratégicos, Dependência de sistemas	Impacto na Missão Organizacional
Imagem e Reputação	Exposição midiática negativa, Perda de confiança pública, Impacto em parcerias estratégicas	Impacto Reputacional
Volume de Usuários Afetados	Quantidade absoluta de usuários impactados, Criticidade dos usuários afetados	Impacto nos Usuários
Impacto Financeiro	Custos diretos de recuperação, Perdas indiretas, Multas ou penalidades regulatórias	Impacto Econômico
Legal/Regulatório	Conformidade com leis (ex.: LGPD), Obrigações contratuais, Consequências jurídicas	Impacto Legal

Tabela 2 – Critérios e Indicadores para Avaliação de Ativos Críticos. Descrição dos critérios principais e seus respectivos indicadores utilizados na avaliação de ativos críticos. A estrutura apresentada permite uma categorização mais objetiva e mensurável dos ativos organizacionais, facilitando a aplicação do modelo hierárquico na gestão de riscos e segurança cibernética.

O critério Missão da Organização foi associado a indicadores como impacto na continuidade operacional e dependência de sistemas internos, refletindo diretamente o papel estratégico dos ativos na sustentação das funções essenciais da organização. Da mesma forma, o critério Imagem e Reputação inclui indicadores como exposição midiática negativa e perda de confiança pública, aspectos que podem comprometer significativamente a percepção externa da organização. Além disso, os critérios relacionados ao impacto financeiro e legal/regulatório foram detalhados com base em métricas práticas que facilitam sua aplicação no contexto organizacional. No caso do impacto financeiro, foram considerados custos diretos e indiretos associados a incidentes cibernéticos, enquanto no impacto legal/regulatório destacaram-se indicadores relacionados à conformidade com legislações específicas, como a LGPD.

5. Conclusão

Este estudo teve como objetivo identificar critérios que podem ser utilizados para classificar um ativo como Joia da Coroa no contexto do Poder Executivo Federal brasileiro. Para isso, foi adotada uma abordagem metodológica que combinou revisão de literatura, aplicação de questionários a gestores do SISP e desenvolvimento colaborativo de subcritérios por meio de brainstorming estruturado. A pesquisa buscou preencher uma lacuna na literatura ao propor um modelo estruturado e validado para a avaliação e priorização de ativos críticos.

Os resultados indicaram que os critérios mais relevantes para a classificação de ativos críticos são Missão da Organização, Imagem e Reputação, Volume de Usuários Afetados, Impacto Financeiro e Impacto Legal/Regulatório. A priorização desses critérios foi fundamentada na análise das respostas dos 57 gestores do SISP, refletindo sua percepção

sobre os fatores que mais influenciam a criticidade dos ativos organizacionais. Com base nessa priorização, foi estruturado um modelo hierárquico que organiza os critérios e subcritérios de forma sistemática, permitindo sua aplicação na gestão de riscos e segurança cibernética.

Além da contribuição teórica ao consolidar um modelo estruturado para a classificação de ativos críticos, o estudo oferece uma ferramenta prática para apoiar gestores na tomada de decisão. A metodologia adotada permite adaptação a diferentes contextos organizacionais, tornando-se um recurso útil para aprimorar estratégias de proteção de ativos estratégicos e mitigação de riscos.

No entanto, a pesquisa apresenta algumas limitações, sendo a principal delas a restrição da amostragem aos gestores do SISP, o que pode limitar a generalização dos resultados para outros contextos. Como trabalhos futuros, recomenda-se a aplicação do modelo proposto em estudos que explorem sua implementação prática em diferentes setores organizacionais, a fim de validar e expandir sua aplicabilidade. Os achados deste estudo reforçam a importância de uma abordagem estruturada para a identificação e proteção das Joias da Coroa, contribuindo para a melhoria da gestão de riscos no setor público e para o fortalecimento da resiliência organizacional frente às ameaças cibernéticas.

Agradecimentos

Esta pesquisa foi apoiada pelo projeto TED 33/2023 “Pesquisa Aplicada em Privacidade e Segurança da Informação na Diretoria de Privacidade e Segurança da Informação da Secretaria De Governo Digital (SGD)” – Diretoria de Privacidade e Segurança da Informação da Secretaria de Governo Digital – Centro de Excelência em Privacidade e Segurança da Informação (CEPS).

Referências

Aal, A., & Martin, A. (2012). Discussion group: Mission critical systems influence of component reliability on design decisions w.r.t. performance & robustness. International Integrated Reliability Workshop. https://doi.org/10.1109/IIRW.2012.6468964

Antoni, Marc, and Nadia Ammad. (2018). “Argus project-harnessing asset management to do cyber security to an uic guideline for railways.” Congrès Lambda Mu 21 «Maîtrise des risques et transformation numérique: opportunités et menaces».

Baginda, Y. P., Affandi, A., & Pratomo, I. (2018). Analysis of RTO and RPO of a Service Stored on Amazon Web Service (AWS) and Google Cloud Engine (GCE). International Conference on Information Technology and Electrical Engineering. https://doi.org/10.1109/ICITEED.2018.8534758

Barclay, C. (2014). Sustainable Security Advantage In A Changing Environment: The Cybersecurity Capability Maturity Model (CM2). IEEE, 6858466.

Bennett, R. H., Fadil, P. A., & Greenwood, R. T. (1994). Cultural Alignment in Response to Strategic Organizational Change: New Considerations for a Change Framework. Journal of Managerial Issues.

Bisogni, F., & Cavallini, S. (2010). Assessing the Economic Loss and Social Impact of Information System Breakdowns. https://doi.org/10.1007/978-3-642-16806-2_13.

Bologna, S., & Beer, T. (2003). An Integrated Approach to Survivability Analysis of Large Complex Critical Infrastructures.

Breaz, T. O., & Jaradat, M. (2024). Strategic human resource management: aligning hr practices with organizational goals. https://doi.org/10.24818/imc/2023/04.01.

Brumfield, Cynthia and Bo Haugli. (2023). Cybersecurity Risk Management: Mastering the fundamentals using the NIST Cybersecurity Framework. John Wiley & Sons, Inc., Hoboken,NJ, 2023.

Brunner, E., & Suter, M. (2008). International CIIP Handbook 2008/2009: An Inventory of 25 National and 7 International Critical Infrastructure Protection Policies. Center for Security Studies, ETH Zurich, Zurich, Suíça.

Burnett, R. (1996). Anticipate and Prevent — Managing the Legal Risks in Safety Critical Systems. https://doi.org/10.1007/978-1-4471-1480-2_9

Center for Threat-Informed Defense. (2025). Threat Modeling with ATT&CK: Question 1 - What are we working on? Disponível em: https://center-for-threat-informed-defense.github.io/threat-modeling-with-attack/question-1/ [Acesso em 19 de fevereiro de 2025].

Cox, R. G., & Robinson, D. G. (2004). Vulnerability of critical infrastructures: identifying critical nodes (No. SAND2004-2696). Sandia National Laboratories (SNL), Albuquerque, NM, and Livermore, CA (United States).

Davis, D. (1995). Legal Aspects of Safety Critical Systems. In Safe Comp 95: The 14th International Conference on Computer Safety, Reliability and Security, Belgirate, Italy 11–13 October 1995 (pp. 156-170). London: Springer London.

Emergency Management Australia. (2003). Critical Infrastructure Emergency Risk Management and Assurance Handbook, Mount Macedon, Australia.

European Commission. (2006). Proposal for a Directive of the Council on the Identification and Designation of European Critical Infrastructure and the Assessment of the Need to Improve Their Protection. COM(2006) 787 Final, Bruxelas, Bélgica.

Faria, N. C. (2022). Estratégia de Cibersegurança. Dissertação de Mestrado. Universidade do Minho, Portugal. https://repositorium.sdum.um inho.pt/bitstream/1822/84478/1/Nelson%20Correia%20Faria.pdf.

Fekete, A. (2011). Common Criteria for the Assessment of Critical Infrastructures.*International Journal of Disaster Risk Science, 2*(1), 15–24. https://doi.org/10.1007/s13753-011-0002-y.

Ficco, M. (2016). security and reliability of critical systems. Journal of Ambient Intelligence and Humanized Computing, 7, 149-151.

Georg, M. A. C., Rodrigues, W. M. S., de Melo Alves, C. A., Júnior, A. S., & Nunes, R. R. (2022). Os desafios da Segurança Cibernética no setor público federal do Brasil: estudo sob a ótica de gestores de tecnologia da informação. *Revista Ibérica de Sistemas e Tecnologias de Informação*, (E54), 602-616.

Gil, A. C. (2009). Como elaborar projetos de pesquisa (4a ed.). São Paulo, Atlas.

Glenn, C., Sterbentz, D., & Wright, A. (2016). Cyber threat and vulnerability analysis of the US electric sector. Idaho National Lab. (INL), Idaho Falls, ID, EUA.

Hardy, T. L. (2014). Resilience: A holistic safety approach. In 2014 Reliability and Maintainability Symposium (pp. 1-6). IEEE.

Hinchey, M., & Margaria, T. (2014). Evolving Critical Systems-Track Introduction. In Leveraging Applications of Formal Methods, Verification and Validation. Technologies for Mastering Change: 6th International Symposium, ISoLA 2014, Imperial, Corfu, Greece, October 8-11, 2014, Proceedings, Part I 6 (pp. 1-3). Springer Berlin Heidelberg.

Hyatt, D., & Santos, J. R. (2022). An Input-Output Model to Determine the Operability and Economic Impacts of IT on Interdependent Industries. Systems and Information Engineering Design Symposium. https://doi.org/10.1109/sieds55548.2022.9799348.

Jonkeren, O. E., Dorneanu, B., Ward, D., & Giannopoulos, G. (2012). Regional economic assessment of Critical Infrastructure failure in the EU: A combined systems engineering and economic model. Research Papers in Economics.

Kissoon, Troy. (2022). Optimal spending on cybersecurity measures: Risk Management. Routledge, Abingdon, Oxon.

Kraven Security. (2024). Crown Jewel Analysis: How To Figure Out What To Protect. Disponível em: https://kravensecurity.com/crown-jewel-analysis/.

Langemeier, M. (2016). Identification of Unique Resources." farmdoc daily (6): 105. Department of Agricultural and Consumer Economics, University of Illinois at Urbana-Champaign.

Leirvik. (2023). Understand, Manage, and Measure Cyber Risk: Practical Solutions for Creating a Sustainable Cyber Program. Apress L. P., Berkeley, CA.

Li, N. X., Wang, F., Magoua, J. J., & Fang, D. (2022). Interdependent effects of critical infrastructure systems under different types of disruptions. International Journal of Disaster Risk Reduction. https://doi.org/10.1016/j.ijdrr.2022.103266.

Lima, E. D. O., Moreira, F. R., de Deus, F. E. G., Nze, G. D. A., de Sousa Júnior, R. T., & Nunes, R. R. (2022). Avaliação da Rotina Operacional do Operador Nacional do Sistema Elétrico Brasileiro (ONS) em Relação às Ações de Gerenciamento de Riscos Associados à Segurança Cibernética. *Revista Ibérica de Sistemas e Tecnologias de Informação*, (E49), 301-312.

Lis, P., & Mendel, J. (2019). Cyberattacks on critical infrastructure: An economic perspective. Economics & Business Review, 5(2).

Marconi, M. A., & Lakatos, E. M. (2003). Fundamentos de metodologia científica (5ª ed.). Atlas.

Matsumoto, N., Fujita, J., Endoh, H., Yamada, T., Sawada, K., & Kaneko, O. (2021). Asset management method of industrial IoT systems for cyber-security countermeasures. Information, 12(11), 460.

Minayo, M. C. D. S. (2002). Pesquisa Social: Teoria, Método e Criatividade. 21ª Edição. Petrópolis: Editora Vozes.

Ministry of the Interior and Kingdom Relations. (2008). National Risk Assessment Method Guide 2008. The Hague, Países Baixos.

MITRE. (2025). Mitre crown jewels analysis (CJA). Disponível em: https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/crown-jewels-analysis.

Moteff, J., Copeland, C. & Fischer, J. (2003). Critical Infrastructures: What Makes an Infrastructure Critical?, Washington: The Library of Congress.

Musman, S., Tanner, M., Temin, A., Elsaesser, E., & Loren, L. (2011). A systems engineering approach for crown jewels estimation and mission assurance decision making. In 2011 IEEE Symposium on Computational Intelligence in Cyber Security (CICS) (pp. 210-216). IEEE.

National Cyber Security Centre. (2024). Asset management. https://www.ncsc. gov.uk/collection/10-steps/asset-management.

Onwubiko, C. (2012). Challenges to Managing Privacy Impact Assessment of Personally Identifiable Data. In Information Assurance and Security Technologies for Risk Assessment and Threat Management: Advances (pp. 254-272). IGI Global Scientific Publishing.

Pang, A. (2017). Product Safety Failure and Restoring Reputation Across Markets: Fonterra's Management of the 2013 Bacterial Contamination Crisis. Journal of Marketing Channels. https://doi.org/10.1080/1046669X.2017.1393231

Panzieri, S., & Setola, R. (2008). Failures propagation in critical interdependent infrastructures. International Journal of Modelling, Identification and Control. https://doi.org/10.1504/IJMIC.2008.018186

Rao, G. V., & Krishna, D. J. (2015). Alignment of HR practices with organizational strategies. The Indian Journal of Industrial Relations, 666-679.

Reeder, J. R., & Hall, T. (2021). Cybersecurity's pearl harbor moment. The Cyber Defense Review, 6(3), 15-40.

Schweikert, A., L'Her, G. F., & Deinert, M. (2021). Simple method for identifying interdependencies in service delivery in critical infrastructure networks. Applied Network Science. https://doi.org/10.1007/S41109-021-00385-4

Shoniregun, C. A. (2004). An investigation of information systems project failure and its implication on organisations. International Journal of Services Technology and Management. https://doi.org/10.1504/IJSTM.2004.004024.

Singh, Sandeep. (2024). From NIST to Risk Model to Crown Jewels: The Evolution of Cybersecurity Models. LinkedIn. Disponível em: https://www.linkedin.com/pulse/from-nist-risk-model-crown-jewels-evolution-models-sandeep-singh.

Tervo, H., & Wiander, T. (2010). Failures and Image. European Conference on Information Systems.

Theoharidou, M., Kotzanikolaou, P., and Gritzalis, D. (2009). Risk-Based Criticality Analysis. In Critical Infrastructure Protection III. Proceedings. Third Annual IFIP (International Federation for Information Processing) WG 11.10 International Conference on Critical Infrastructure Protection. Hanover, New Hampshire, USA, March 23–25.

U.S. Department of Homeland Security. (2009). National Infrastructure Protection Plan 2009. Washington, DC, EUA.

Varga, S., Brynielsson, J., & Franke, U. (2021). Cyber-threat perception and risk management in the Swedish financial sector. Computers & Security, 105, 102239.

Walls, J., & Harley, B. (2022). Call for papers: Special issue of strategic organization: Impact driven strategy research for grand challenges. Strategic Organization, 20(1), 225-227.