Estrutura Hierárquica para Identificação de Ativos Críticos em Universidades Federais: Uma Abordagem Baseada na Análise de Joias da Coroa

Rodrigo Costa Duarte https://orcid.org/0009-0008-3836-8835	Mestre em Ciência da Computação. Universidade Federal de Juiz de Fora (UFJF) – Brasil. rodrigo.duarte@ufjf.br
Rafael Rabelo Nunes https://orcid.org/0000-0002-1538-4276	Doutor em Engenharia Elétrica. Universidade de Brasília (UnB) – Brasil. rafaelrabelo@unb.br

RESUMO

As Universidades Federais brasileiras enfrentam crescentes desafios relacionados à segurança cibernética, dada sua forte dependência de sistemas e ativos de tecnologia da informação e comunicação (TIC) críticos para o cumprimento de suas missões institucionais. Neste contexto, o presente artigo busca identificar e organizar de forma hierárquica critérios através dos quais seja possível reconhecer ativos críticos dentro de universidades. A pesquisa adotou uma abordagem qualitativa e exploratória, fundamentada na análise de Planos Diretores de Tecnologia da Informação e Comunicação (PDTICs) de Universidades Federais. A partir da categorização dos impactos documentados nesses planos e em estudo de referência, foram definidos cinco critérios principais: missão da organização, imagem e reputação, usuários, consequências financeiras e impactos legais e regulatórios. Com base nesses critérios, desenvolveu-se uma estrutura hierárquica que apresenta graficamente critérios e subcritérios que podem ser utilizados para avaliar a criticidade dos ativos através de métodos multicritérios. Os resultados indicam que a maior parte dos impactos se concentra na missão institucional, reforçando a necessidade de abordagens integradas e alinhadas aos objetivos estratégicos das universidades. A estrutura proposta oferece uma ferramenta útil para apoiar decisões no âmbito da segurança da informação e da gestão de riscos, contribuindo para decisões mais eficientes na alocação de recursos e para a resiliência institucional.

Palavras-chave: governança de TIC; análise de criticidade; gestão de riscos; classificação de ativos; ambiente universitário.

ABSTRACT

Brazilian Federal Universities face growing cybersecurity challenges, given their heavy reliance on information and communication technology systems and assets critical to fulfilling their institutional missions. In this context, this article seeks to identify and organize in a hierarchical manner the criteria through which it is possible to recognize critical assets within universities. The research adopted a qualitative and exploratory approach, based on the analysis of Information and Communication Technology Master Plans of Federal Universities. Based on the categorization of the impacts documented in these plans and in a reference study, five main criteria were defined: organizational mission, image and reputation, users, financial consequences, and legal and regulatory impacts. Based on these criteria, a hierarchical structure was developed that graphically presents the criteria and subcriteria used to assess the criticality of assets through multicriteria methods. The results indicate that most of the impacts are focused on the institutional mission, reinforcing the need for integrated approaches aligned

with universities' strategic objectives. The proposed framework offers a valuable tool for informing decisions regarding information security and risk management, thereby contributing to more efficient resource allocation and enhanced institutional resilience.

Keywords: ICT governance; criticality analysis; risk management; asset classification; university environment.

1 INTRODUÇÃO

Os ataques cibernéticos representam uma ameaça significativa ao funcionamento das Universidades Federais no Brasil, impactando diretamente a estabilidade e o cumprimento das missões destas instituições de ensino e pesquisa que enfrentam um cenário alarmante com aumento de 56% nas tentativas de ataques entre 2023 e 2024, conforme registrado pela Rede Nacional de Ensino e Pesquisa (RNP) (Schmidt, 2025). Essas instituições desempenham papel fundamental na missão de educar, produzir e disseminar o saber universal, preservar e difundir as artes e a cultura, e contribuir para o desenvolvimento humano (Fedato; Pires; Bresciani, 2025; Novaes; Fonseca, 2020), constituindo o maior sistema de formação de recursos humanos, produção de conhecimento, desenvolvimento tecnológico e prestação de serviços à sociedade do país (ANDIFES, 2017). Neste contexto, as Universidades públicas federais são responsáveis por mais da metade dos cursos e alunos de mestrado e doutorado do Brasil, produzindo cerca de 90% da produção científica nacional (ANDIFES, 2017), e têm papel fundamental na inclusão das populações desfavorecidas, contribuindo através da interiorização para a redução das assimetrias regionais e promovendo impactos positivos no desenvolvimento econômico e social local (Fedato; Pires; Bresciani,2025; Novaes; Fonseca, 2020; Da Silva, 2024).

As Universidades Federais brasileiras são cada vez mais dependentes de sistemas e ferramentas de tecnologia da informação e comunicação (TIC), cuja criticidade pode ser definida pelas funções acadêmicas, administrativas e de pesquisa que suportam, bem como pela importância dos dados que processam e armazenam (Bittencourt *et al.*, 2024; De Assis; Da Costa Filho, 2022). Nesse contexto, destacam-se sistemas considerados estratégicos para o funcionamento institucional, que abrangem desde plataformas de gestão acadêmica e sistemas de matrícula até infraestruturas voltadas à pesquisa científica, sistemas de controle de processos internos e bancos de dados relacionados à propriedade intelectual (Bittencourt *et al.*, 2024). Entre os diversos sistemas informacionais existentes, alguns são frequentemente denominados "Joias da Coroa", por representarem ativos cuja falha ou comprometimento pode impactar de maneira significativa ou até mesmo paralisar atividades essenciais de uma organização universidade (De Assis; Da Costa Filho, 2022).

Nestas condições, a gestão de riscos de segurança cibernética em universidades é uma atividade essencial, pois auxilia no mapeamento de vulnerabilidades e na proteção da confidencialidade, integridade e disponibilidade de sistemas essenciais (Singh; Joshi, 2017). Esse processo inicia-se pelo inventário detalhado de ativos de TI — físicos e virtuais — e sua classificação segundo o impacto potencial sobre atividades de ensino, pesquisa e processos administrativos entre outras (Ulven; Wangen, 2021). Ao desenvolver processos como a gestão de riscos e de segurança da informação, as instituições públicas brasileiras enfrentam desafios significativos, originados pela defasagem tecnológica, alta rotatividade de recursos humanos e pela complexidade dos processos de aquisição, que retardam a atualização de equipamentos e softwares essenciais, deixando-as vulneráveis a ameaças emergentes (Costa, 2019). Além disso, a estrutura de governança das instituições tende a ser fragmentada, sem um órgão central com autonomia executiva capaz de padronizar controles e articular responsabilidades, o que compromete a coordenação de políticas e a resposta a incidentes (De Souza; De Almeida, 2016). Soma-se a isso a ausência de diretrizes operacionais claras e de uma cultura de segurança consolidada, fatores que limitam tanto o

engajamento dos servidores quanto a efetividade das práticas preventivas e de monitoramento contínuo (Georg *et al*., 2023; Da Veiga *et al*., 2020).

A Análise de Joias da Coroa (AJC) emerge como um método fundamental para identificar ativos críticos de TI baseados na missão institucional das universidades, que tradicionalmente se fundamenta no tripé ensino, pesquisa e extensão (De Assis; Da Costa Filho, 2022). Esta abordagem constitui parte de um conjunto mais amplo de metodologias para avaliação de criticidade, considerando as particularidades do ambiente universitário, onde a disponibilidade, integridade e confidencialidade dos sistemas tecnológicos são essenciais para garantir a continuidade das atividades acadêmicas e a proteção de informações estratégicas da instituição (Bittencourt *et al*., 2024; Schmidt, 2025). Nas instituições de ensino, a criticidade desses ativos tecnológicos está diretamente relacionada ao impacto que sua indisponibilidade pode causar nas atividades fim da universidade, podendo afetar desde o processo de ensino-aprendizagem até projetos de pesquisa de relevância científica e social, bem como os processos administrativos e de credenciamento das instituições (Fedato; Pires; Bresciani,2025).

Diante desse cenário de crescente vulnerabilidade, torna-se essencial identificar os ativos mais críticos para proteção estratégica. Assim, este trabalho tem como objetivo identificar e organizar de forma hierárquica critérios através dos quais seja possível reconhecer ativos críticos dentro de universidades. Os critérios e sub-critérios identificados poderão ser utilizados em pesquisas futuras, sendo inseridos em métodos multicritérios para identificação de "Joias da Coroa. Para alcançar esse objetivo, o estudo foi organizado em diferentes seções. Após esta introdução, a Seção 2 traz o embasamento teórico sobre a segurança cibernética e a gestão de riscos contemplando as estratégias sugeridas pelo governo federal para adoção nos órgãos da administração pública federal, a gestão de ativos e identificação de ativos críticos através de abordagens multicritério, como a análise de Joias da Coroa e a apresentação de conceitos fundamentais sobre planejamento de TIC e planos diretores de tecnologia da Informação e comunicação (PDTICs). A Seção 3 trata da metodologia empregada, explicando detalhadamente as etapas da pesquisa. Já a Seção 4 apresenta os principais resultados, com ênfase na análise dos critérios levantados e a apresentação de uma estrutura hierárquica para auxiliar a identificação de ativos críticos TIC em universidades. Por fim, a Seção 5 reúne as considerações finais, sintetizando os achados mais relevantes e indicando sugestões para investigações futuras.

2 REFERENCIAL TEÓRICO

2.1 Segurança Cibernética no Governo Brasileiro

A segurança cibernética pode ser definida como o conjunto de práticas, tecnologias e processos destinados a proteger sistemas digitais, redes e dados contra acessos não autorizados, danos ou interrupções. Com a crescente dependência de tecnologias digitais, a segurança tornou-se um tema central em diversas organizações, pois envolve a proteção de dados sensíveis e a garantia da privacidade e integridade dessas informações (Bittencourt *et al*., 2024). A gestão eficaz de riscos envolve a identificação, avaliação e mitigação de ameaças, utilizando estratégias como a implementação de políticas claras, treinamento de pessoal e adoção de padrões internacionais de segurança (Cheng; Wang, 2022).

No âmbito do Governo Federal do Brasil, a segurança da informação e privacidade e a segurança, bem como a segurança cibernética, são regulamentadas por várias leis e decretos que visam proteger dados sensíveis e garantir a integridade dos sistemas de informação. Alguns destas leis e regulamentos são citados a seguir em ordem cronológica de publicação.

No contexto da privacidade, a Lei Geral de Proteção de Dados (LGPD), instituída pela Lei nº 13.709 de 2018, tem como principal objetivo proteger os direitos fundamentais de liberdade e privacidade, garantindo a segurança jurídica no tratamento de dados pessoais (BRASIL, 2018). A LGPD estabelece diretrizes para o tratamento de dados pessoais, incluindo a necessidade de consentimento e a criação de um encarregado para lidar com os titulares dos dados.

A Política Nacional de Segurança da Informação (PNSI) (BRASIL-PNSI, 2018) instituída pelo Decreto nº 9.637, de 26 de dezembro de 2018, tem como objetivo assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação em âmbito nacional, abrangendo segurança cibernética, defesa cibernética, segurança física e proteção de dados organizacionais. A PNSI é implementada por meio da Estratégia Nacional de Segurança da Informação (ENSI) e dos planos nacionais. A Estratégia Nacional de Segurança Cibernética (E-Ciber) é um módulo da ENSI, estabelecido pelo Decreto nº 10.222 de 2020, que visa proteger o governo e as infraestruturas críticas contra ataques cibernéticos. A estratégia tem como objetivos preencher lacunas sobre segurança cibernética, proteger o governo e realizar a proteção cibernética das empresas responsáveis por infraestruturas críticas (BRASIL, 2020).

Em 2023 foi instituído pela Portaria SGD/MGI nº 852 de 2023, o Programa de Privacidade e Segurança da Informação (PPSI) com o objetivo de elevar a maturidade e resiliência dos órgãos e entidades em privacidade e segurança da informação no âmbito do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) (Brasil, 2023). O programa é estruturado em cinco áreas: Governança, Maturidade, Metodologia, Pessoas e Tecnologia (Brasil, 2025).

Ainda no âmbito das instituições governamentais, o Tribunal de Contas da União incluiu os temas segurança da informação e segurança cibernética na Lista de Alto Risco (LAR) (BRASIL-TCU, 2024), ferramenta estratégica que consolida a avaliação do TCU sobre 29 áreas críticas da administração pública, que apresentam riscos significativos, capazes de comprometer a qualidade dos serviços prestados ao cidadão e a efetividade das políticas públicas. O órgão realiza várias ações para identificar problemas, avaliar riscos e sugerir melhorias para tornar os sistemas e dados do país mais seguros, ajudando a fortalecer a proteção digital e a criar um ambiente tecnológico mais confiável para todos os brasileiros. Nos últimos anos realizou várias fiscalizações para aferir a adequação dos órgãos às políticas e leis vigentes bom como a aplicação de controles sugeridos em programas como o PPSI. Os resultados e recomendações resultantes destas fiscalizações estão disponíveis em acórdãos publicados no site da instituição (BRASIL-TCU, 2025).

2.2 Segurança da Informação e Gestão de Riscos em Instituições Acadêmicas Federais

Pertencendo ao rol dos orgãos da administração pública federal, sujeitas portanto às regulações pertinentes, as universidades federais enfrentam desafios significativos de segurança cibernética devido à sua natureza descentralizada e à cultura de abertura, tornando-as alvos atraentes

para ataques cibernéticos (Hobbs, 2023). Essas instituições armazenam grandes volumes de dados sensíveis, incluindo registros de dados pessoais de toda a comunidade acadêmica, informações financeiras e pesquisas acadêmicas valiosas, o que as torna vulneráveis a ataques como *phishing*, *malwares*, *DoS*, ameaças internas e *ransomware* dentre outros (Karafiloski, 2021; ELLUCIAN, 2024).

Uma revisão sistemática da literatura realizada por Bittencourt *et al*. analisou artigos publicados entre 2012 e 2022 sobre a gestão da segurança da informação no contexto da Universidades, revelando escassez de pesquisas empíricas sobre riscos cibernéticos específicos nestas instituições. Apesar dessa lacuna, os estudos revisados demonstraram convergência quanto à relevância do tema, reforçando a percepção que as universidades são alvos frequentes de ataques devido à grande quantidade de dados sensíveis que armazenam e à sua natureza (Bittencourt *et al*., 2024; Karafiloski, 2021; ELLUCIAN, 2024). Também foi constatado um aumento expressivo na produção acadêmica sobre o assunto nos últimos anos, indicando o reconhecimento crescente da relevância do tema. Aponta-se, no entanto, a escassez de pesquisas como uma janela importante a ser preenchida por futuros estudos (Bittencourt *et al*., 2024).

Iniciativas como a adoção da LGPD (BRASIL, 2018) e a criação do Programa de Privacidade e Segurança da Informação (PPSI) (Brasil, 2025) atuam no sentido de enfatizar a importância da adoção de estruturas formais e controles relacionados ao tema em órgãos e entidades da administração pública federal, sendo um passo importante para uma melhoria na segurança da informação no âmbito governamental e consequentemente nas Instituições de ensino superior públicas (Maia Arruda; Linhares Lima, 2024).

Essas políticas, programas e fiscalizações trabalham em conjunto para garantir que as instituições públicas brasileiras adotem práticas robustas de segurança da informação e cibernética, protegendo dados sensíveis e mitigando riscos cibernéticos.

2.3 Gestão de Ativos e Priorização

Um dos componentes essenciais na segurança da informação é a gestão de ativos. Contemplada pelo framework do PPSI e referenciada em diversos frameworks como as famílias de normas ISO/IEC 19770 e 27000 e o COBIT 5, esta gestão permite que as organizações identifiquem, monitorem e protejam todo o ecossistema de TIC, como hardware, software, redes e seus dispositivos e dados (CIS, 2021). Ela envolve o rastreamento, a classificação e o gerenciamento contínuo de todos os ativos tecnológicos utilizados pela instituição. Este processo inclui a criação de um inventário detalhado, categorização dos ativos com base em sua criticidade e monitoramento constante para identificar vulnerabilidades ou alterações não autorizadas (Libeer, 2024; SCYTALE, 2024). Sem uma visão clara dos ativos existentes, torna-se mais difícil protegê-los adequadamente contra ameaças cibernéticas. Além disso, a falta de rastreamento adequado pode dificultar a resposta a incidentes e aumentar os custos associados a violações de segurança (Shaw, 2019).

Ao abordar a gestão de ativos, é essencial destacar a importância de uma correta classificação do nível de criticidade, permitindo a identificação dos ativos realmente essenciais para o funcionamento da instituição. Essa identificação constitui a base para uma estratégia de segurança eficaz, exigindo a consideração de impactos operacionais, regulatórios e de imagem,

além da adoção de defesas multicamadas e da integração contínua entre a gestão de ativos e as políticas institucionais de segurança (Antoni; Ammad, 2018). É fundamental, portanto, compreender os serviços e funções críticos da organização e associá-los aos ativos e tecnologias dos quais dependem, a fim de priorizá-los com precisão (NCSC, 2024).

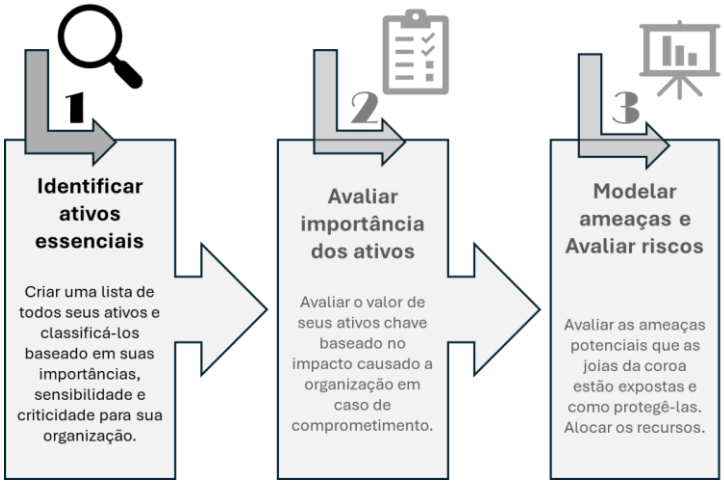
Nesse processo de priorização, a definição de critérios de avaliação torna-se um componente indispensável. Os critérios utilizados para avaliar riscos e impactos podem ser classificados em qualitativos e quantitativos, cada qual com vantagens e limitações específicas. Os critérios qualitativos baseiam-se em julgamentos subjetivos, geralmente estruturados em escalas como "alto", "médio" ou "baixo" para representar a probabilidade e o impacto de riscos. Essa forma de avaliação, embora de rápida aplicação, pode apresentar limitações relacionadas à introdução de vieses e à dificuldade de realizar comparações mais robustas entre diferentes cenários (METRICSTREAM, 2023). Por outro lado, os critérios quantitativos utilizam dados objetivos, modelos matemáticos e análises estatísticas, oferecendo resultados mais mensuráveis e confiáveis. No entanto, exigem maior esforço na coleta e tratamento dos dados, o que pode tornar sua aplicação mais onerosa e demorada (CROWDSTRIKE, 2024).

Neste contexto, metodologias multicritério, como o método *AHP* (*Analytic Hierarchy Process*), o modelo OCTAVE e a Análise de Joias da Coroa (AJC), têm se mostrado eficazes na classificação de ativos com base em múltiplos critérios ponderados, permitindo a identificação e priorização daqueles de maior relevância estratégica (Saaty, 1990; Ishizaka & Labib, 2011). Estudos apontam que o uso de critérios bem definidos e estruturados favorece decisões mais consistentes, promovendo alocação eficiente de recursos e mitigação de riscos (Musman *et al.*, 2011).

A crescente sofisticação das ameaças cibernéticas impõe às organizações a necessidade de adotar abordagens estruturadas para proteger seus ativos mais sensíveis. Nesse cenário, a AJC destaca-se como uma abordagem estratégica, capaz de identificar e priorizar ativos essenciais à missão institucional. Esses ativos incluem desde infraestruturas críticas até dados sensíveis e propriedade intelectual, cujo comprometimento pode impactar diretamente a continuidade operacional e a reputação da organização (Musman *et al.*, 2011; Singh, 2024; Goss, 2024).

Mais do que identificar ativos, a AJC propõe uma análise de seu papel estratégico no alcance dos objetivos institucionais. Essa característica torna o método especialmente adequado a contextos com escassez de dados quantitativos, como o ambiente universitário público. Ao priorizar ativos com base em sua relevância e no impacto potencial de sua indisponibilidade, permite uma alocação mais eficaz de recursos e o direcionamento de medidas de segurança mais precisas (Musman *et al.*, 2011). O processo é estruturado em três etapas principais: (i) identificação dos ativos essenciais segundo sua relevância institucional; (ii) avaliação dos impactos potenciais de sua perda ou comprometimento, considerando aspectos financeiros, operacionais e reputacionais; e (iii) modelagem de ameaças e definição de estratégias de mitigação e proteção, Figura 1 (Goss, 2024).

Figura 1 – Fluxo da Análise de Joias da Coroa



Fonte: Elaboração própria com base em Musman *et al*. (2011) e *Kraven Security* (2024).

Nesse sentido, para dar maior consistência metodológica à definição dos critérios utilizados neste estudo e garantir aderência ao contexto institucional analisado, recorreu-se a modelos existentes na literatura que já foram validados em ambientes semelhantes.

Para estruturar os critérios e subcritérios utilizados neste estudo, foi adotado como base o modelo apresentado no trabalho "Tomada de Decisão em Segurança Cibernética: Modelo para Identificação de Joias da Coroa", que propõe um conjunto de critérios principais validados empiricamente junto a gestores do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) do Poder Executivo Federal (Da Silva *et al*., 2025). Esse modelo multicritério estabelece uma hierarquia composta por critérios como Missão da Organização, Imagem e Reputação, Volume de Usuários Afetados, Impacto Financeiro e Impacto Legal/Regulatório, associados a subcritérios específicos definidos em colaboração com especialistas do setor público.

A escolha de utilizar esse modelo como referência justifica-se pela similaridade entre o ambiente estudado no artigo — o setor público federal brasileiro — e o contexto das Universidades Federais analisadas. Dessa forma, foi possível realizar uma análise comparativa entre os resultados obtidos naquele estudo e os impactos documentados nos PDTICs das universidades, identificando convergências e especificidades do contexto acadêmico. Essa abordagem contribui para validar empiricamente os critérios utilizados e reforça a aderência do modelo proposto às necessidades reais das instituições de ensino superior, fortalecendo a fundamentação teórica e prática deste trabalho.

2.4. Planejamento de TIC e Planos Diretores de Tecnologia da Informação e Comunicação (PDTICs)

O Planejamento de Tecnologia da Informação e Comunicação (TIC) atua como um guia estratégico para orientar a implementação de iniciativas e projetos de TIC na organização, definindo diretrizes claras para a área e estabelecendo planos de ação detalhados que viabilizam o alinhamento de esforços e a alocação eficiente de recursos rumo ao alcance de metas estabelecidas. Em essência, esse processo administrativo e gerencial envolve

a identificação e a organização de equipes, aplicações e ferramentas de TIC, garantindo suporte à entidade na realização de seu planejamento institucional e no cumprimento de seus objetivos organizacionais (Calder, 2008).

Este planejamento deve ser formalizado em um documento oficial, tornado público e amplamente difundido dentro da organização, contemplando tanto o ambiente interno quanto o externo relacionado às atividades de TIC. Sua elaboração exige a colaboração ativa de todas as unidades responsáveis por TIC e das demais áreas finalísticas, garantindo o alinhamento das diretrizes tecnológicas com os objetivos institucionais. Além disso, é essencial que esse documento seja objeto de monitoramento contínuo e de avaliações periódicas, de modo a ajustar estratégias, metas e recursos conforme as necessidades evolutivas da organização (BRASIL-SISP, 2021).

No caso dos órgãos do SISP, o planejamento da TIC é consolidado no PDTIC, sendo que a Instrução Normativa SGD/ME nº 1 de 4 de abril de 2019 define o PDTIC como sendo um "instrumento de diagnóstico, planejamento e gestão dos recursos e processos de TIC, com o objetivo de atender às necessidades finalísticas e de informação de um órgão ou entidade para um determinado período" (BRASIL-SISP, 2021). Constitui-se, ainda, em um importante complemento ao planejamento estratégico institucional, compreendendo diretrizes e ações transversais que suportam objetivos de negócio de todas as áreas da instituição, bem como objetivos estruturais e regimentais dos Órgãos da APF. Conforme orientações do SISP, o PDTIC deve ser elaborado pela unidade competente dos órgãos e das entidades da administração pública federal, aprovado pelo respectivo Comitê de Governança Digital e publicado em seu portal institucional, visando dar maior transparência às informações e decisões tomadas, à exceção das informações classificadas como não públicas, nos termos da legislação aplicável (BRASIL-SISP, 2025).

3 METODOLOGIA

Trata-se de uma pesquisa qualitativa, de natureza exploratória e descritiva, alinhando-se à classificação proposta por Minayo (1994), Gil *et al.* (2002) e Marconi e Lakatos (2004). O caráter exploratório justifica-se pela intenção de investigar um campo ainda pouco sistematizado no contexto universitário, especialmente no que se refere à identificação e classificação de ativos críticos. Já o caráter descritivo decorre da análise de documentos institucionais — especificamente, os Planos Diretores de Tecnologia da Informação e Comunicação (PDTICs) de universidades federais — com o objetivo de caracterizar padrões e critérios utilizados na definição da criticidade dos ativos. A adoção de uma abordagem qualitativa fundamenta-se na natureza dos dados analisados e na ênfase na interpretação dos significados atribuídos aos impactos documentados, conforme argumentam Creswell (2014) e Godoy (1995).

O procedimento técnico adotado foi a pesquisa documental, mediante seleção de PDTICs publicados por Universidades Federais brasileiras que atendessem a dois critérios: (i) validade até, pelo menos, o ano de 2022; e (ii) menção explícita a impactos ou consequências decorrentes de incidentes relacionados à segurança da informação. A coleta de informações foi realizada entre maio e junho de 2025.

Os dados foram analisados utilizando a técnica de análise de conteúdo, que possibilitou agrupar qualitativamente as consequências descritas nos PDTICs em cinco dimensões principais de impacto. Essas dimensões foram extraídas e adaptadas da metodologia de Análise de Joias da Coroa (AJC)

(Musman *et al.*, 2011), tomando como referência um modelo previamente validado no setor público federal brasileiro (Da Silva *et al.*, 2025).

A utilização da Análise de Joias da Coroa (AJC) como referencial metodológico nesta pesquisa justifica-se por sua capacidade de identificar ativos críticos com base em sua contribuição direta para o cumprimento da missão institucional, permitindo uma abordagem estratégica da segurança da informação. No entanto, para a etapa de priorização, adotou-se um modelo hierárquico inspirado no método *Analytic Hierarchy Process* (AHP), amplamente reconhecido entre os métodos multicritérios e frequentemente aplicado em conjunto com a AJC para apoiar processos de decisão estruturados. Essa combinação possibilitou uma análise mais sistemática dos critérios, articulando a lógica da AJC com a robustez hierárquica do AHP. A estrutura resultante oferece um conjunto de critérios aderentes à realidade das Universidades Federais brasileiras, contribuindo para decisões mais consistentes e fundamentadas no âmbito da gestão de riscos e da segurança da informação.

A metodologia seguiu um processo estruturado em quatro etapas principais: (1) Análise e revisão do modelo apresentado no artigo "Tomada de Decisão em Segurança Cibernética: Modelo para Identificação de Joias da Coroa" (Da Silva *et al.*, 2025); (2) obtenção das fontes de dados (PDTICs); (3) Análise de conteúdo (Bardin, 1977; Krippendorff, 2018) para definição de critérios, identificação de impactos e consequências e posterior agrupamento; e (4) Desenvolvimento de estrutura aderente a Universidades. A Figura 2 ilustra essas etapas metodológicas.

Figura 2 – Etapas do processo de pesquisa

Fonte: Elaboração própria (2025).

Na fase inicial deste estudo, adotou-se como ponto de partida o modelo proposto no trabalho "Tomada de Decisão em Segurança Cibernética: Modelo para Identificação de Joias da Coroa" (Da Silva *et al.*, 2025). Esse modelo se

destaca por ter sido construído a partir de uma análise estruturada de publicações científicas que abordam impactos organizacionais em diferentes setores. Além disso, foi validado empiricamente junto a gestores do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) do Poder Executivo Federal.

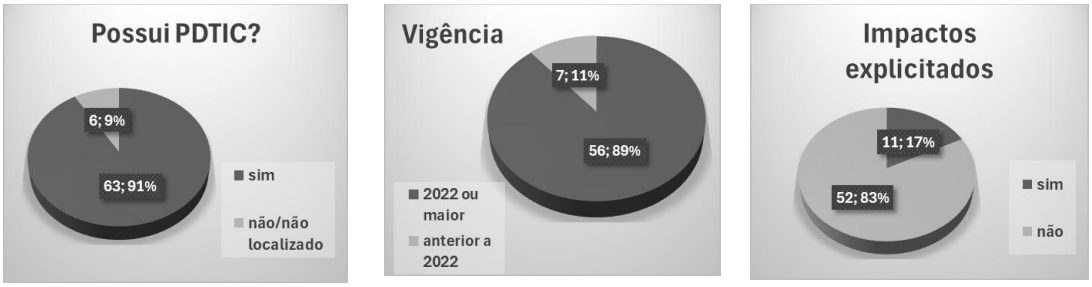
A escolha de utilizar esse modelo como base nesta pesquisa justifica-se por diversos fatores: a aderência metodológica aos objetivos do presente estudo, a similaridade entre o contexto das universidades federais e os órgãos do setor público federal analisados no trabalho original, e a robustez conceitual proporcionada pelo levantamento prévio de literatura aliado à validação prática. Dessa forma, foi possível alinhar os critérios e subcritérios utilizados aqui com aqueles previamente identificados e testados, aumentando a consistência, a comparabilidade dos resultados e a relevância do modelo proposto para a realidade das instituições de ensino superior.

Em seguida, com base nesse modelo de referência, procedeu-se à coleta dos Planos Diretores de Tecnologia da Informação e Comunicação (PDTICs) publicados pelas Universidades Federais.

Para orientar a análise dos Planos Diretores de Tecnologia da Informação e Comunicação (PDTICs) selecionados, este estudo utilizou a técnica de análise de conteúdo por permitir identificar padrões e categorias a partir de documentos oficiais, conforme Bardin (1977) e Krippendorff (2018), baseada em três etapas principais: pré-análise, exploração do material e tratamento dos resultados.

Na fase de pré-análise, foram definidos os critérios de inclusão dos documentos (validade mínima até 2022 e menção explícita a impactos ou consequências). Foram selecionados documentos de 11 instituições que satisfaziam os critérios de inclusão, sendo a amostra representativa de cerca de 16% das universidades federais em funcionamento no país. Considera-se que o fator preponderante para a não inclusão da maioria dos planos foi a falta de menções diretas a impactos ou consequências dos possíveis incidentes. A Figura 3 mostra o número e percentual de instituições com planos publicados e os percentuais de aderência aos critérios estabelecidos.

Figura 3 – Painel com números da pesquisa



Fonte: Elaboração própria com base em dados da amostra das 69 Universidades Federais (2025).

Em seguida, realizou-se uma leitura minuciosa dos PDTICs na etapa de exploração, destacando-se trechos que descreviam diretamente consequências ou impactos de falhas, indisponibilidades ou incidentes de segurança. Por fim, na etapa de tratamento dos resultados, essas consequências foram

agrupadas em categorias de impacto previamente definidas, visando permitir uma avaliação estruturada e comparável entre as universidades analisadas.

Essa categorização dos impactos foi inspirada no modelo hierárquico desenvolvido no artigo "Tomada de Decisão em Segurança Cibernética: Modelo para Identificação de Joias da Coroa" (Da Silva *et al.*, 2025) e permitiu a construção de uma estrutura de avaliação alinhada à realidade das Universidades. Esse modelo, construído a partir de revisão de literatura, questionários aplicados a gestores do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) e sessões colaborativas, apresenta cinco critérios principais validados empiricamente e mostrados na Tabela 1: Missão da Organização, Imagem e Reputação, Volume de Usuários Afetados, Impacto Financeiro e Impacto Legal/Regulatório. A adoção desse modelo neste estudo se justifica pela sua aderência ao contexto do setor público federal — semelhante ao ambiente das universidades federais — e pela possibilidade de alinhar empiricamente os dados obtidos nos PDTICs com critérios reconhecidos, aumentando a consistência e a relevância prática da análise realizada.

Tabela 1 – Critérios potenciais para identificação de ativos críticos

Critério	Descrição	Referências
Missão da organização	afeta diretamente os objetivos institucionais ou o funcionamento essencial da universidade	(Fekete, 2011), (Hinchey & Margaria, 2014), (Martin *et al.*, 2012)
Imagem e reputação	causa danos à credibilidade institucional, à confiança dos usuários ou à percepção pública	(Bennett *et al.*, 1994), (Tervo & Wiander, 2010), (Pang, 2017)
Usuários	quantidade e criticidade dos usuários afetados e efeitos sobre a capacidade da comunidade acadêmica ou administrativa realizar suas funções	(Walls & Harley, 2022), (Shoniregun, 2004)
Financeiro	perdas econômicas diretas ou indiretas, custos de recuperação ou perda de recursos	(Walls & Harley, 2022), (Bisogni & Cavallini, 2010), (Jonkeren *et al.*, 2012), (Hyatt & Santos, 2022), (Lis & Mendel, 2019)
Legais e Regulatórios	riscos de não conformidade com legislações vigentes, como a LGPD, ou com contratos e normativas públicas	(Fekete, 2011), (Rao & Krishna, 2015), (Davis, 1995), (Burnett, 1996)

Fonte: Silva *et al.* (2025).

4 RESULTADOS E DISCUSSÕES

4.1. Pesquisa e critérios para o modelo

Com base na análise dos PDTICs de 11 Universidades Federais e na pesquisa apresentada em "Tomada de Decisão em Segurança Cibernética: Modelo para Identificação de Joias da Coroa" foram priorizados cinco critérios principais de impactos: à missão da organização, à imagem e reputação da instituição, impacto aos usuários, financeiros e impactos legais e regulatórios. A tabela 2 mostra a distribuição dos principais impactos citados, bem como exemplos de impactos.

Tabela 2 – Critérios de Impacto mais citados nos PDTICs analisados

Critério de Impacto	**N° de Citações**	**% do Total**	**Exemplos de Impactos Identificados**
Missão da Organização	89	31,8%	Interrupção de atividades essenciais; paralisação de processos; indisponibilidade de sistemas; prejuízo a projetos.
Usuários	67	23,9%	Insatisfação da comunidade; sobrecarga; demora em atendimentos; redução da produtividade.
Financeiro	52	18,6%	Aumento de despesas; multas; desperdício de recursos; altos custos de manutenção.
Legal e Regulatório	38	13,6%	Não conformidade com LGPD; sanções legais; exposição de dados; penalizações por órgãos reguladores.
Imagem/Reputação	34	12,1%	Danos à imagem institucional; perda de credibilidade; impacto em avaliações externas.

Fonte: Elaboração própria com base na análise dos PDTICs de 11 Universidades Federais (2025).

Com base nesta definição de critérios primários, foi desenvolvida uma estrutura hierárquica que organiza os critérios a subcritérios associados. A estrutura é apresentada na figura 4 e representa de forma estruturada as dimensões a serem avaliadas no contexto da Universidades, tendo sido os subcritérios definidos e refinados através de análise crítica sobre as informações encontradas nos PDTICs.

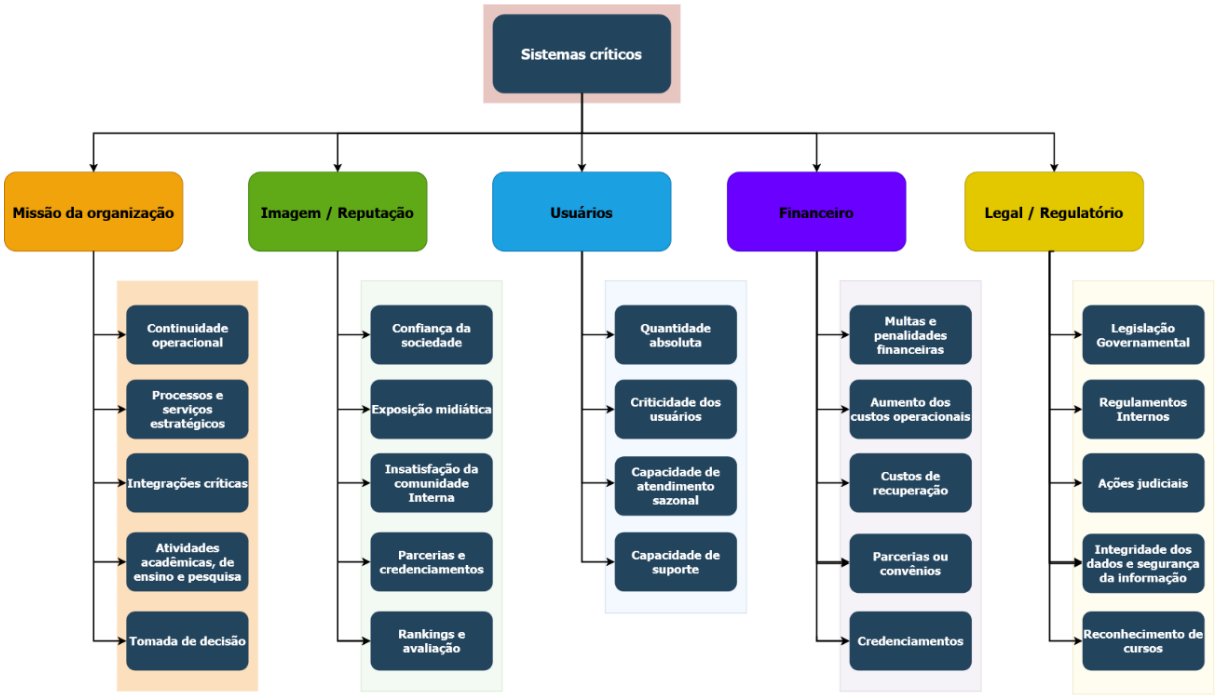
No critério "Missão da Organização", foram estabelecidos subcritérios como impacto na continuidade operacional da instituição, impacto em processos, planos e serviços estratégicos, dependência do ativo para outros sistemas ou processos internos, dependência para funcionamento de atividades de ensino e pesquisa e impacto do ativo para a tomada de decisões estratégicas. O detalhamento do critério "Imagem e Reputação" foi realizado com base em fatores como a perda de confiança da sociedade, insatisfação da comunidade interna gerando um ambiente menos produtivo, impacto em parcerias estratégicas prejudicando o credenciamento da instituição para participação em atividades e representações estratégicas e o prejuízo causado ao

posicionamento da instituição em rankings e avaliações de órgãos avaliadores. Já o critério "Usuários" foi estruturado considerando a quantidade absoluta de usuários impactados diretamente, bem como a criticidade desses usuários, como cidadãos, servidores públicos ou gestores estratégicos. Neste critério foi ainda contemplada a capacidade de atendimento a eventos sazonais, que podem gerar demandas atípicas em períodos específicos e a capacidade da instituição de fornecer suporte aos usuários de seus serviços.

Os subcritérios definidos para impactos "Financeiros" incluem possíveis custos multas ou penalidades financeiras decorrentes do descumprimento regulatório, o aumento de custos operacionais causados pela indisponibilidade do ativo, custos diretos de recuperação após incidentes ou associados à interrupção das operações, perda de receita por interrupção de parcerias ou convênios e perdas causadas por descredenciamento da instituição para prestação de diversos tipos de serviços à comunidade interna e externa. No critério "Legal/Regulatório", foram incluídos aspectos como conformidade com legislações específicas, como a LGPD, o decreto da PNSI e a portaria do PPSI, o não atendimento a regulações internas que possibilitam o correto funcionamento da organização, a exposição a contestações judiciais de atos e ações oficializadas pela Universidade e implicações jurídicas associadas a integridade, confidencialidade e disponibilidade de dados estratégicos ou protegidos pela legislação vigente.

A estrutura hierárquica (Figura 4) resultante desta pesquisa organiza de forma visual e estruturada os critérios e subcritérios identificados, o que facilita sua aplicação prática no contexto organizacional das universidades federais. Além disso, constitui uma base metodológica sólida para a avaliação dos ativos como críticos, apoiando processos decisórios fundamentados em métodos multicritério.

Figura 4 - Estrutura hierárquica para identificação de ativos críticos em Universidades Federais brasileiras



Fonte: Elaboração própria com base nos PDTICs de Universidades

4.2. Interpretação dos resultados

A análise dos PDTICs revelou que a maioria dos impactos citados pelas Universidades Federais está concentrada em dimensões diretamente associadas à missão institucional, especialmente aquelas relacionadas à continuidade das atividades de ensino, pesquisa e extensão. O critério "Missão da Organização" foi citado em 89 ocorrências, representando o núcleo de maior criticidade entre os ativos identificados. Esse dado evidencia que a paralisação ou comprometimento de sistemas associados à missão institucional tem potencial para afetar significativamente a operação das universidades, interrompendo fluxos acadêmicos e administrativos essenciais.

Os demais critérios também apresentaram alta incidência de citações, demonstrando que os impactos de falhas ou ataques cibernéticos transcendem a dimensão operacional e afetam aspectos estratégicos e reputacionais. O critério "Usuários" (67 citações), por exemplo, evidencia preocupações com a qualidade do atendimento à comunidade acadêmica, enquanto o critério "Financeiro" (52 citações) indica a presença de riscos orçamentários e custos indiretos significativos associados a incidentes de segurança. Já os critérios "Legal/Regulatório" e "Imagem/Reputação" (com 38 e 34 citações, respectivamente) reforçam o papel da conformidade normativa e da percepção pública como elementos críticos para a sustentabilidade institucional.

Ao comparar os achados com a literatura, observa-se coerência com estudos prévios (Bittencourt *et al*, 2024; Ulven; Wangen, 2021) que apontam para a vulnerabilidade das universidades a ataques cibernéticos, especialmente devido à complexidade de seus sistemas e à elevada sensibilidade dos dados tratados (Musman *et al*., 2011). Além disso, a ausência de uma estrutura centralizada de governança de TIC nas universidades, conforme indicado por Georg *et al*. (2023), contribui para o aumento do risco organizacional e dificulta a implementação de políticas unificadas de segurança.

A estrutura hierárquica desenvolvida com base nesses critérios e subcritérios, associada a modelos multicritério como o apresentado em Silva (2025) fornece uma estrutura adaptável às especificidades das instituições de ensino superior, permitindo não apenas a avaliação da criticidade de ativos, mas também o direcionamento de esforços de segurança de forma proporcional ao risco. A natureza multidimensional do modelo possibilita uma abordagem mais holística, alinhando a gestão de riscos com os objetivos institucionais e fortalecendo a resiliência organizacional frente a ameaças cibernéticas.

4.3. Aplicabilidade do modelo

A estrutura hierárquica desenvolvida neste estudo apresenta elevado potencial de aplicação prática no contexto das Universidades Federais brasileiras, especialmente no apoio a processos decisórios relacionados à gestão de riscos e à segurança da informação. Construída a partir de critérios e subcritérios extraídos de evidências documentais e alinhados à metodologia de Análise de Joias da Coroa (AJC), a proposta oferece uma ferramenta objetiva e adaptável para identificação de ativos críticos. Para além dessa identificação inicial, a etapa de priorização pode ser fortalecida pelo uso do método Analytic Hierarchy Process (AHP), que organiza os critérios em uma hierarquia e permite comparações pareadas entre eles, atribuindo pesos

relativos a cada dimensão de impacto. Dessa forma, além de mapear os ativos críticos, o modelo fornece subsídios quantitativos para ordená-los segundo sua relevância para a missão institucional.

No âmbito institucional, a estrutura associada a modelos multicritérios pode ser incorporada como instrumento auxiliar durante o ciclo de planejamento de TIC, contribuindo para a priorização de ativos cuja proteção é essencial para a continuidade das atividades-fim da universidade. A incorporação do AHP nessa etapa de priorização viabiliza, por exemplo, que gestores avaliem com maior rigor se impactos na missão devem ter mais peso que os de ordem financeira ou de imagem, resultando em decisões mais transparentes e justificáveis. O modelo também pode ser utilizado por equipes de segurança da informação, comitês de governança digital e setores de conformidade e auditoria, ao proporcionar uma avaliação estruturada e mensurável do impacto potencial da indisponibilidade ou comprometimento de sistemas críticos.

Além disso, a categorização proposta facilita a integração da estrutura com metodologias de gestão de riscos já consolidadas, como a Análise de Impacto nos Negócios (BIA), frameworks como o COBIT 5 e a ISO/IEC 27001, bem como estratégias de continuidade de serviços. Nessa integração, o AHP atua como elo de apoio quantitativo, oferecendo escalabilidade e maior precisão às análises, sem substituir práticas já institucionalizadas.

Outra vantagem significativa do modelo é sua capacidade de adaptar-se ao grau de maturidade institucional. Em universidades com baixa maturidade em governança de TIC, a estrutura hierárquica pode servir como ponto de partida para a definição de políticas mais robustas, fornecendo inclusive um mecanismo simples de priorização via AHP. Já em instituições com práticas consolidadas, o modelo pode funcionar como mecanismo de refinamento e validação de estratégias de proteção, contribuindo para ajustes finos nos critérios de criticidade e confirmando decisões previamente estabelecidas.

Por fim, a estrutura hierárquica favorece a comunicação entre áreas técnicas e a alta gestão, ao traduzir a criticidade de ativos de TIC em impactos organizacionais tangíveis e alinhados à missão institucional. O uso do AHP nesse processo, ao fornecer resultados numéricos claros de priorização, facilita ainda mais a compreensão por parte dos gestores e pode apoiar a obtenção de recursos para investimentos em segurança cibernética. Nesse sentido, o modelo torna-se não apenas uma ferramenta de análise, mas também um catalisador para a construção de ambientes universitários mais resilientes.

5 CONCLUSÃO

Este artigo identificou critérios e os organizou de forma hierárquica, de modo a apoiar a identificação de ativos críticos de instituições federais de ensino superior, a partir da análise de Planos Diretores de Tecnologia da Informação e Comunicação (PDTICs) das Universidades.

A predominância de impactos associados à missão institucional, evidenciada nos documentos analisados, destaca a vulnerabilidade das universidades diante da indisponibilidade ou comprometimento de seus ativos críticos de TIC. Esses achados reforçam a importância de adotar abordagens estruturadas para orientar a priorização de ativos conforme sua relevância estratégica.

A estrutura hierárquica proposta oferece uma ferramenta útil para avaliação e gestão de ativos críticos, sendo aplicável tanto em instituições com baixa maturidade em governança de TIC quanto naquelas com práticas mais

consolidadas. A estrutura representa, ainda, uma oportunidade de alinhamento entre os esforços técnicos e estratégicos das universidades, contribuindo para a governança digital e a efetividade das políticas de TIC no setor público.

Além disso, a proposta contribui para o fortalecimento da segurança cibernética institucional, ao subsidiar decisões mais assertivas na alocação de recursos, definição de controles e planejamento de contingências. Sua utilização favorece o diálogo entre áreas técnicas e a alta gestão, promovendo maior conscientização sobre os riscos e ampliando a capacidade de resposta organizacional.

Entre as limitações do estudo, destaca-se a dependência exclusiva de documentos estratégicos oficiais como fonte primária, o que pode limitar a compreensão de aspectos práticos e operacionais da gestão de ativos críticos. A heterogeneidade nos formatos e conteúdo dos PDTICs analisados, também evidencia a necessidade de padronização e de maior maturidade no planejamento de TIC entre as instituições públicas de ensino superior. Uma possível solução para minimizar a disparidade entre os planos seria a adoção do guia elaborado pelo SISP (BRASIL-SISP, 2021) e forte capacitação das equipes de elaboração dos documentos.

Como desdobramentos futuros, recomenda-se a aplicação prática da estrutura apresentada, em modelos multicritério, em ambientes reais, incluindo a realização de estudos de caso, entrevistas com gestores e validação empírica com especialistas. Adicionalmente, o desenvolvimento de ferramentas computacionais baseadas no modelo hierárquico como o proposto em (Da Silva *et al*., 2025), associado à estrutura proposta neste artigo pode ampliar sua aplicabilidade e eficiência em processos decisórios relacionados à segurança da informação especificamente para as universidades.

Em síntese, a estrutura hierárquica representa uma contribuição relevante para o avanço da gestão de ativos críticos no setor educacional público, oferecendo uma base metodológica sólida para orientar estratégias de proteção e fortalecer a resiliência organizacional frente aos desafios emergentes da segurança cibernética no ensino superior.

REFERÊNCIAS

ANDIFES. Universidades federais patrimônio da sociedade brasileira. 2017. Disponível em: https://ufpr.br/wp-content/uploads/2017/11/livreto-Andifes-FINAL-para-Universidades-v24112017_baixa2.pdf

ANTONI, Marc; AMMAD, Nadia. 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»**. 2018.

BARDIN, Lawrence. Análise de conteúdo. **Lisboa: edições**, v. 70, p. 225, 1977.

BENNETT III, Robert H.; FADIL, Paul A.; GREENWOOD, Robin T. Cultural alignment in response to strategic organizational change: New considerations for a change framework. **Journal of Managerial Issues**, p. 474-490, 1994.

BISOGNI, Fabio; CAVALLINI, Simona. Assessing the economic loss and social impact of information system breakdowns. *In:* **International Conference on Critical Infrastructure Protection**. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010. p. 185-198.

BITTENCOURT, Olivia Tozzi *et al*. Segurança cibernética nas universidades: uma revisão sistemática da literatura sobre a gestão de segurança da informação no ensino superior. **InterSciencePlace**, v. 19, 2024.

BRASIL. **Lei nº 13.709 de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 03 ago. 2025.

BRASIL. **Decreto nº 10.222, de 5 de fevereiro de 2020**. Aprova a Estratégia Nacional de Segurança Cibernética (E-Ciber). 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm. Acesso em: 03 ago. 2025.

BRASIL. **Portaria SGD/MGI nº 852, de 28 de março de 2023.** Institui o Programa de Privacidade e Segurança da Informação. 2023. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908. Acesso em: 03 ago. 2025.

BRASIL. **Portal do Programa de Privacidade e Segurança da Informação (PPSI).** 2025. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca. Acesso em: 03 ago. 2025.

BRASIL-PNSI. **Decreto nº 9.637, de 26 de dezembro de 2018**. Institui a Política Nacional de Segurança da Informação. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9637.htm. Acesso em: 03 ago. 2025.

BRASIL-SISP. **Guia de PDTIC do SISP - Versão 2.1**. 2021. Disponível em: https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/sisp/guia-do-gestor/documentos/guia-de-pdtic-do-sisp-2-1/view. Acesso em: 03 ago. 2025.

BRASIL-SISP. **Guia do gestor**. 2025. Disponível em: https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/sisp/guia-do-gestor/pdtic. Acesso em: 03 ago. 2025.

BRASIL-TCU. **Lista de alto risco da administração pública Federal 2ª edição.** 2024. Disponível em: https://sites.tcu.gov.br/listadealtorisco/seguranca_da_informacao_e_seguranca_cibernetica.html. Acesso em: 03 ago. 2025.

BRASIL-TCU. **Portal de Fiscalização de Segurança da Informação e Cibersegurança**. 2025. Disponível em: https://portal.tcu.gov.br/tecnologia-da-informacao/fiscalizacao-de-seguranca-da-informacao-e-ciberseguranca#fiscalizacoes. Acesso em: 03 ago. 2025.

BURNETT, Rachel. Anticipate and Prevent—Managing the Legal Risks in Safety Critical Systems. *In:* **Safety-Critical Systems: The Convergence of High Tech and Human Factors: Proceedings of the Fourth Safety-critical Systems Symposium**. London: Springer London, 1996. p. 139-152.

CALDER, Alan. **ISO/IEC 38500: the IT governance standard**. IT Governance Ltd, 2008.

Center for Internet Security. **Controles CIS versão 8**. 2021. Disponível em https://learn.cisecurity.org/cis-controls-download-v8. Acesso em: 03 ago. 2025.

CHENG, Eric CK; WANG, Tianchong. Institutional strategies for cybersecurity in higher education institutions. **Information**, v. 13, n. 4, p. 192, 2022.

COSTA, Paulo *et al*. The security challenges emerging from the technological developments: A practical case study of organizational awareness to the security risks. **Mobile networks and applications**, v. 24, n. 6, p. 2032-2037, 2019.

CRESWELL, John W. **Investigação Qualitativa e Projeto de Pesquisa-: Escolhendo entre Cinco Abordagens**. Penso Editora, 2014.

CrowdStrike. **How To Perform a Cybersecurity Risk Assessment.** 2024. Disponível em: https://www.crowdstrike.com. Acesso em: 03 ago. 2025.

DA SILVA, Edvan Gomes *et al*. (2025). Tomada de Decisão em Segurança Cibernética: Modelo para Identificação de Joias da Coroa. **Revista Ibérica de Sistemas e Tecnologias de Informação (RISTI)**. 2025. DOI: 10.5281/zenodo.15364727.

DA SILVA, Roberta Morais. A educação superior e seu papel de relevância no desenvolvimento econômico e social das nações. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 10, n. 9, p. 2157-2171, 2024.

DA VEIGA, Adele *et al*. Defining organisational information security culture—Perspectives from academia and industry. **Computers & Security**, v. 92, p. 101713, 2020.

DAVIS, Dai. 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**. London: Springer London, 1995. p. 156-170.

DE ASSIS, Leandro Duarte; DA COSTA FILHO, Custódio Genésio. Fatores críticos de sucesso na implantação do sistema eletrônico de informações em Universidades Federais. **Revista Gestão Universitária na América Latina-GUAL**, p. 180-202, 2022.

DE SOUZA, Eduardo André Araujo; DE ALMEIDA, Nival Nunes. A questão da segurança e defesa do espaço cibernético brasileiro, e o esforço políticoadministrativo do Estado. **Revista da EGN**, v. 22, n. 2, p. 381-410, 2016.

ELLUCIAN. **Information security for higher education.** 2024. Disponível em: https://www.ellucian.com/assets/en/ebook/information-security-higher-education.pdf. Acesso em: 03 ago. 2025.

FEDATO, Geovana Alves de Lima; PIRES, Vanessa Martins; BRESCIANI, Sirlene Aparecida Takeda. *Impacto social y misión de las universidades públicas brasileñas¿ Hay convergencia?*. **Revista de Administração de Empresas**, v. 65, p. e2024-0202, 2025.

FEKETE, Alexander. Common criteria for the assessment of critical infrastructures. **International Journal of Disaster Risk Science**, v. 2, n. 1, p. 15-24, 2011.

GEORG, Marcus Aurélio Carvalho *et al*. Os desafios da Segurança Cibernética no setor público federal do Brasil: estudo sob a ótica de gestores de tecnologia da informação. **E54**, p. 602-616, 2023.

GIL, Antonio Carlos *et al*. **Como elaborar projetos de pesquisa**. São Paulo: Atlas, 2002.

GODOY, Arlida Schmidt. Introdução à pesquisa qualitativa e suas possibilidades. **Revista de administração de empresas**, v. 35, p. 57-63, 1995.

GOSS, Adam. ***Crown Jewel Analysis: How To Figure Out What To Protect.*** 2024. Disponível em: https://kravensecurity.com/crown-jewel-analysis/. Acesso em: 03 ago. 2025.

HINCHEY, Mike; MARGARIA, Tiziana. Evolving Critical Systems-Track Introduction. *In*: **International Symposium On Leveraging Applications of Formal Methods, Verification and Validation**. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014. p. 1-3.

HOBBS, Jonathan. **Cybersecurity awareness in higher education: a comparative analysis of faculty and staff**. 2023. Tese de Doutorado. Middle Georgia State University.

HYATT, David; SANTOS, Joost. An input-output model to determine the operability and economic impacts of IT on interdependent industries. *In:* **2022 Systems and Information Engineering Design Symposium (SIEDS)**. IEEE, 2022. p. 37-42.

ISHIZAKA, Alessio; LABIB, Ashraf. Review of the main developments in the analytic hierarchy process. **Expert systems with applications**, v. 38, n. 11, p. 14336-14345, 2011.

JONKEREN, Olaf *et al*. Regional economic assessment of Critical Infrastructure failure in the EU: A combined systems engineering and economic model. 2012.

KARAFILOSKI, Davor. ***Emerging issues in cybersecurity for higher education institutions***. 2021. Disponível em: https://www.sumologic.com/blog/emerging-issues-in-cyber-security-for-higher-education-institutions/. Acesso em: 03 ago. 2025.

KRIPPENDORFF, Klaus. **Content analysis: An introduction to its methodology**. Sage publications, 2018.

LIBEER, Laura. **How Cybersecurity Asset Management Enhances Your IT Security**. 2024. Disponível em: https://www.lansweeper.com/blog/cybersecurity/how-cybersecurity-asset-management-enhances-your-it-security/. Acesso em: 03 ago. 2025.

LIS, Piotr; MENDEL, Jacob. Cyberattacks on critical infrastructure: An economic perspective. **Economics & Business Review**, v. 5, n. 2, 2019.

MAIA ARRUDA, Constança Maria; LINHARES LIMA, Pedro Arthur. PROTEÇÃO DE DADOS: EXPERIÊNCIA INTERNACIONAL E O CASO BRASILEIRO-RELAÇÃO COM A SEGURANÇA DA INFORMAÇÃO E A GOVERNANÇA CIBERNÉTICA. **Relações Internacionais**, n. 82, 2024.

MARCONI, M. de A.; LAKATOS, Eva Maria. **Metodologia científica**. São Paulo: Atlas, 2004.

MARTIN, Andreas *et al*. Discussion group: Mission critical systems influence of component reliability on design decisions wrt performance & robustness. *In:* **2012 IEEE International Integrated Reliability Workshop Final Report**. IEEE, 2012. p. 217-219.

Metricstream. **Qualitative or Quantitative Risk Assessment? A Practical Guide to Assessing Non-Financial Risks**. 2023. Disponível em: https://www.metricstream.com/learn/practical-guide-to-assessing-non-financial-risks.html. Acesso em: 03 ago. 2025.

MINAYO, Maria Cecília de Souza. Pesquisa social: teoria, método e criatividade. *In:* **Pesquisa social: teoria, método e criatividade**. 1994. p. 80-80.

MUSMAN, Scott *et al*. A systems engineering approach for crown jewels estimation and mission assurance decision making. *In*: **2011 IEEE Symposium on Computational Intelligence in Cyber Security (CICS)**. IEEE, 2011. p. 210-216

National Cyber Security Centre. **10 Steps to Cyber Security - Asset management**. 2024. https://www.ncsc.gov.uk/collection/10-steps/asset-management. Acesso em: 03 ago. 2025.

NOVAES, Cristina Verônica Santos; FONSECA, Josefa Sônia Pereira. A universidade brasileira e sua função social no percurso constitucional. *In*: **VII Congresso Nacional de Educação**. 2020.

PANG, Augustine. Product safety failure and restoring reputation across markets: Fonterra's management of the 2013 bacterial contamination crisis. **Journal of Marketing Channels**, v. 24, n. 3-4, p. 136-152, 2017.

RAO, G. Venkat; KRISHNA, D. Jayarama. Alignment of HR practices with organizational strategies. **The Indian Journal of Industrial Relations**, p. 666-679, 2015.

SAATY, Thomas L. How to make a decision: the analytic hierarchy process. **European journal of operational research**, v. 48, n. 1, p. 9-26, 1990.

SCHMIDT, Sarah. Computadores vulneráveis: Ataques cibernéticos a universidades e instituições científicas crescem no país. **Revista Pesquisa FAPESP** ed. 352, p. 32-35, jun. 2025.

SCYTALE. **What is Cybersecurity Asset Management? Best Practices**. 2024. Disponível em: https://scytale.ai/glossary/cybersecurity-asset-management/. Acesso em: 03 ago. 2025.

SHAW, Marcel. **10 Reasons Why IT Asset Management is Key to Cybersecurity**. 2019. Disponível em: https://www.ivanti.com/blog/10-reasons-why-it-asset-management-is-key-to-cybersecurity. Acesso em: 03 ago. 2025.

SHONIREGUN, Charles Adetokunbo. An investigation of information systems project failure and its implication on organisations. **International Journal of Services Technology and Management**, v. 5, n. 1, p. 25-41, 2004.

SINGH, Sandeep. **From NIST to Risk Model to Crown Jewels: The Evolution of Cybersecurity Models**. 2024. Disponível em: https://www.linkedin.com/pulse/from-nist-risk-model-crown-jewels-evolution-models-sandeep-singh. Acesso em: 03 ago. 2025.

SINGH, Umesh Kumar; JOSHI, Chanchala. Information Security Risk Management Framework for University Computing Environment. **Int. J. Netw. Secur.**, v. 19, n. 5, p. 742-751, 2017.

TERVO, Heli; WIANDER, Timo. Failures and Image. **European Conference on Information Systems**, 2010.

ULVEN, Joachim Bjørge; WANGEN, Gaute. A systematic review of cybersecurity risks in higher education. **Future Internet**, v. 13, n. 2, p. 39, 2021.

WALLS, Judith; HARLEY, Bill. Call for papers: Special issue of strategic organization: Impact driven strategy research for grand challenges. **Strategic Organization**, v. 20, n. 1, p. 225-227, 2022.