Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Modelo de Gestão de Riscos de TI aplicado ao Consórcio Nacional em Educação, Ciência, Tecnologia e Inovação (ConectiBR)

José Fábio de Oliveira

Dissertação apresentada como requisito parcial para qualificação do
Mestrado Profissional em Computação Aplicada

Orientador
Prof.a Dr.a Ana Carla Bittencourt Reis

Brasília
2022

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

de Oliveira, José Fábio
dm Modelo de Gestão de Riscos de TI aplicado ao Consórcio Nacional em Educação, Ciência, Tecnologia e Inovação (ConectiBR) / José Fábio de Oliveira; orientador Ana Carla Bittencourt Reis. -- Brasília, 2022.
141 p.

Dissertação (Mestrado - Mestrado Profissional em Computação Aplicada) -- Universidade de Brasília, 2022.

1. Gestão de Risco. 2. Consórcio. 3. Plataforma Digital. 4. Análise Multicritério . I. Reis, Ana Carla Bittencourt , orient. II. Título.

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Modelo de Gestão de Riscos de TI aplicado ao Consórcio Nacional em Educação, Ciência, Tecnologia e Inovação (ConectiBR)

José Fábio de Oliveira

Dissertação apresentada como requisito parcial para qualificação do
Mestrado Profissional em Computação Aplicada

Prof.a Dr.a Ana Carla Bittencourt Reis (Orientador)
PPCA/UnB

Prof. Dr. Ari Melo Mariano
Universidad de Sevilla

Prof.a Dr.a Renata Maciel
Universidade Federal de Pernambuco

Prof. Dr. Marcelo Ladeira
Coordenador do Programa de Pós-graduação em Computação Aplicada

Brasília, 25 de fevereiro de 2022

Dedicatória

A Deus por toda benignidade ao conceder saúde, foco e perseverança. Aos meus pais pelo carinho, conselhos e cuidados ao longo da vida. Minha esposa Solange e meu filho Gabriel por suportarem toda ausência durante essa jornada acadêmica, meus firmamentos.

Agradecimentos

A Deus pela vida, foco, fé e força.

Aos meus pais que, apesar de toda dificuldade, sempre buscaram o melhor para mim.

A minha esposa Solange pelo apoio, compreensão, ajuda, sugestões técnicas, carinho, atenção e cuidado dispensados, sempre.

A Universidade de Brasília por proporcionar uma experiência ímpar ao viabilizar essa jornada acadêmica sem precedentes. As palavras não são suficientes para exteriorizar minha gratidão.

Aos ilustres professores verdadeiras "minas de ouro", repletos de conhecimentos e constantemente ávidos por compartilharem essa imensidão de saber.

A minha ilustre orientadora, Profa. Dra. Ana Carla Bittencourt Reis, pelo voto de confiança, assistência, sugestões, correções, dicas, ensinamentos e dinamismo.

Ao meu mentor e amigo doutorando Alexandre Prestes Uchoa, pelas dicas, orientações e cooperação.

Ao meu grande amigo Cláudio Fabrício pela assistência, confiança e inspiração.

Ao meu grande amigo Harrysson Gilgamesh por todo apoio junto ao Conecti Brasil, orquestrando diversas imersões junto aos especialistas.

Ao Conecti Brasil pela oportunidade de desenvolver o trabalho de pesquisa.

A RNP pela oportunidade de fazer parte do Projeto da Plataforma Nacional de Integração de Dados.

Aos amigos Cleber Mitchell, Johnny Hatzinakis, Newton Franklin e Paulo Evelton por fazerem parte dessa caminhada de conhecimento. Foram muitas madrugadas, contribuições, trocas de conhecimento, publicações e gentilezas.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES), por meio do Acesso ao Portal de Periódicos.

Resumo

No Brasil é mais frequente que organizações públicas e privadas, em consequência de objetivos em comum, formem associações (consórcios), e apartir disso, dentre outros aspectos, é possível compartilhar os riscos entre as instituições. Com o intuito de desenvolver a Plataforma Nacional de Integração de Dados, foi formado o Consórcio Nacional em Educação, Ciência, Tecnologia e Inovação entre os principais agentes promotores da ciência no Brasil (entes públicos, privados e uma organização social sem fins lucrativos - OS), Consórcio Multi-Institucional (CMI). Entretanto, a tomada de decisão pode ser prejudicada devido a visões, estratégias, cultura e disponibilidade de recursos humanos e financeiros. Dessa forma, este trabalho de pesquisa propõe a hierarquização de ações relacionadas a alternativas para Governança de TI, no contexto do consórcio, com apoio de Análise Multicritério. Foi proposto, similarmente, um modelo de gestão de riscos relacionado ao principal ativo de TI identificado, base de dados, o qual possa viabilizar o gerenciamento dos riscos. A principal contribuição do estudo relaciona-se à utilização de ferramentas de apoio à gestão de riscos, desde a identificação até o tratamento dos riscos, relacionados ao ativo de banco de dados, o qual possui um alto grau de sensibilidade para o fomento do ensino, pesquisa, compartilhamento e tratamento de dados pessoais, os quais formam o principal negócio do CMI. A base de dados da plataforma consolida as informações coletadas, processadas, desambiguadas, semanticamente adequadas e compartilhadas em forma de serviços ou por consulta em ferramentas próprias com todos os membros consorciados. Os resultados apresentados reforçam a necessidade e importância de controles, monitoramento e gestão eficaz dos riscos, além de propiciar que o modelo seja utilizado em órgãos públicos ou empresas privadas, os quais compartilhem a necessidade de tratamento de dados pessoais.

Palavras-chave: Gestão de Riscos; Consórcio; Plataforma Digital; Análise Multicritério

Abstract

In Brazil, it is more common for public and private organizations, as a result of common objectives, to form associations (consortia), and from this, among other aspects, it is possible to share risks between institutions. In order to develop the National Data Integration Platform, the National Consortium in Education, Science, Technology and Innovation was formed among the main agents promoting science in Brazil (public and private entities and a non-profit social organization - OS) , Multi-Institutional Consortium (CMI). However, decision making can be hampered due to visions, strategies, culture and availability of human and financial resources. Thus, this research work proposes the hierarchy of actions related to alternatives for IT Governance, in the context of the consortium, with the support of Multicriteria Analysis. It was similarly proposed a risk management model related to the main identified IT asset, database, which can enable risk management. The main contribution of the study is related to the use of tools to support risk management, from the identification to the treatment of risks, related to the database asset, which has a high degree of sensitivity for the promotion of education, research, sharing and processing of personal data, which form the core business of CMI. The platform's database consolidates the information collected, processed, disambiguated, semantically adequate and shared in form of services or by consulting all the consortium members using their own tools. The results presented reinforce the need and importance of controls, monitoring and effective risk management, in addition to allowing the model to be used in public bodies or private companies, which share the need for processing personal data.

Keywords: Risk Management; Consortium; Digital Platform; Multicriteria Analysis

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Quadros

Lista de Abreviaturas e Siglas

AD Administrador de Dados.

AHP *Analytic Hierarchy Process*.

AI Administrador de Infraestrutura.

API Interface de Programação de Aplicações.

ASI Analista de Segurança da Informação.

BD Banco de Dados.

CAPES Coordenação de Aperfeiçoamento de Pessoal de Nível Superior.

CCPA *California Consumer Privacy Act*.

CGU Controladoria Geral da União.

CIO *Chief Information Officer*.

CIS *Center for Internet Security*.

CMI Consórcio Multi-Institucional.

CMMI *Capability Maturity Model Integration*.

CNPq Conselho Nacional de Desenvolvimento Científico e Tecnológico.

ConectiBR Consórcio Nacional em Educação, Ciência, Tecnologia e Inovação.

CONFAP Conselho Nacional das Fundações Estaduais de Amparo à Pesquisa.

CPP Consórcio Público Privado.

CR *Consistency Ratio*.

CRIS *Current Research Information System*.

CTI Ciência, Tecnologia e Inovação.

D Detecção.

DBA *Database Administrator*.

DBMS *Data Base Management System*.

DPA *Data Protection Act*.

EAR Estrutura Analítica dos Riscos.

ECTI Educação, Ciência, Tecnologia e Inovação.

ELECTRE *Elimination et Choice Traduisant La Realite*.

FMEA *Failure Mode and Effects Analysis*.

FTC Federal Trade Commission.

GDM Tomada de decisão em grupo.

GDPR *General Data Protection Regulation*.

GR Gestão de Riscos.

GTI Governança de TI.

IBICT Instituto Brasileiro de Informação em Ciência e Tecnologia.

ID Identificador.

IEEE *Institute of Electrical and Electronic Engineers*.

IES Instituição de Ensino Superior.

IFAC *International Federation of Accountants*.

IoT *Internet of Things*.

ISO *International Organization for Standardization*.

LGPD Lei Geral de Proteção de Dados Pessoais.

MCDA *Multi-Criteria Decision Analysis*.

MCDM *Multi-Criteria Decision Making*.

MFA Múltiplo Fator de Autenticação.

NIS Solução Ideal Negativa.

O Ocorrência.

ORCID *Open Researcher and Contributor ID*.

OS Organização Social.

PD Plataforma Digital.

PII Informações de Identificação Pessoal.

PIS Solução Ideal Positiva.

PMBOK *Project Management Body of Knowledge*.

PNID Plataforma Nacional de Integração de Dados.

PPP Parcerias Público-Privado.

PROMETHEE *Preference Ranking Method for Enrichment Evaluation*.

RI Índice aleatório.

RNP Rede Nacional de Pesquisa.

RPN *Risk Priority Number*.

S Severidade.

SciELO Biblioteca Eletrônica Científica Online.

SGBD Sistemas de Gestão de Banco de Dados.

SNPG Sistema Nacional de Pós-Graduação.

SQL *Structured Query Language*.

TCU Tribunal de Contas da União.

TI Tecnologia da Informação.

TIC Tecnologia da Informação e Comunicação.

TOPSIS *Technique for Order of Preference by Similarity to Ideal Solution.*

VIKOR Otimização multicritério e solução de Compromisso.

WOS *Web of Science.*

Capítulo 1

Introdução

A Rede Nacional de Pesquisa (RNP) (1) constrói seu Ecossistema em alinhamento com as universidades e centros de pesquisa que a compõem. O projeto, a implantação e a operação dessa infraestrutura de serviços para suporte à educação e à pesquisa utilizam o conhecimento, a competência dos pesquisadores, especialistas em computação, os sistemas brasileiros distribuídos e de parceiros internacionais. A RNP promove e desenvolve parcerias públicas e privadas que viabilizam a superação de barreiras de infraestrutura, tecnologia e qualificação, pois ao construir soluções junto à comunidade acadêmica, são partilhados os incentivos e promovido o desenvolvimento da educação, ciência e tecnologia para o benefício dos brasileiros. Para atender a esse grande desafio, a RNP procura sempre tornar seu Ecossistema abrangente, seguro, simples e eficiente (2). Tudo isso é possível graças aos recursos recebidos de seus órgãos financiadores. Em seu portfólio de clientes e parceiros encontra-se a Coordenação de Aperfeiçoamento de Pessoal de Nível Superior CAPES (3), a qual é responsável pela operacionalização da gestão dos programas de pós-graduação nacionais, o que inclui prover os processos de acompanhamento, de fomento, de promoção e de avaliação dos mesmos. A CAPES desenvolve em parceria com a RNP a Plataforma Nacional de Integração de Dados - PNID (4). Ao vislumbrar o potencial de retorno à sociedade, promovido pela PNID, no âmbito acadêmico ou não, a CAPES vivifica a união dos principais agentes promotores da ciência no Brasil para formar o Consórcio Nacional em Educação, Ciência, Tecnologia e Inovação, intitulado de Conecti Brasil ou ConectiBR. Esse Consórcio Multi-institucional (CMI) é formado por entes públicos, privados e organização social sem fins lucrativos (OS), a saber (4):

- Coordenação de Aperfeiçoamento de Pessoal de Nível Superior é responsável pela gestão dos dados dos programas de pós-graduação para fins de divulgação e avaliação, além de fomentar o ensino e a pesquisa brasileira (3).
- Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq tem como principais atribuições fomentar a pesquisa científica, tecnológica e incentivar a formação

de pesquisadores brasileiros (5).

• Conselho Nacional das Fundações Estaduais de Amparo à Pesquisa (CONFAP) tem por finalidade representar, coordenar e articular os interesses comuns das Fundações Estaduais de Amparo à Pesquisa, com base na integração entre os Sistemas Estaduais de Ciência, Tecnologia e Inovação (CTI), a contribuir para o aperfeiçoamento da Política Nacional de CTI (6).

• Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT) tem por atribuições promover a competência, o desenvolvimento de recursos e a infraestrutura de informação em ciência e tecnologia para a produção, socialização e integração do conhecimento científico e tecnológico (7).

• Biblioteca Eletrônica Científica Online (SciELO) é um programa de infraestrutura de pesquisa de apoio à comunidade científica, biblioteca digital e modelo cooperativo de publicação digital de periódicos científicos do Brasil de acesso aberto (8)

• Rede Nacional de Ensino e Pesquisa - RNP tem como objetivos planejar e executar atividades de desenvolvimento tecnológico, inovação, operações de meios e serviços, envolvendo tecnologias de informação e comunicação para a educação, ciência, tecnologia, inovação e suas aplicações em políticas públicas setoriais (1).

O CMI possui como um de seus objetivos desenvolver um conjunto de serviços de dados, a partir da Plataforma Nacional de Integração de Dados como provedora de serviços, o qual forneça às organizações membras e correlatas, como universidades e institutos dados precisos acerca dos diferentes agentes, objetos e produtos relacionados à educação superior, à ciência, à tecnologia e à inovação (autores, teses, bolsas e financiamentos, projetos, artigos científicos, docentes e programas de pós-graduação, entre vários outros). A ambição subjacente à criação da Plataforma Digital (PD) consiste em reduzir ambiguidades e conflitos entre dados usados por diferentes organizações em seus sistemas informáticos para representar as mesmas entidades. Com isso, espera-se um ganho significativo de precisão e eficiência nos serviços providos pelas organizações membras, além de redução nos esforços, custos de desenvolvimento, manutenção de sistemas e bases de dados. Uma fonte única e comum de dados precisos permite a destinação de recursos ao desenvolvimento de novos projetos e serviços ainda não disponíveis. Entre os objetivos mais amplos do CMI, considera-se:

• Promover ferramentas integradoras de conteúdo entre as instituições brasileiras partícipes do consórcio, para os principais sistemas nacionais de informações de Educação, Ciência, Tecnologia e Inovação (ECTI) (Plataforma Sucupira, Plataforma Lattes, Plataforma Oasis, Biblioteca Digital Brasileira de Teses e Dissertações e Plataforma Confap CRIS).

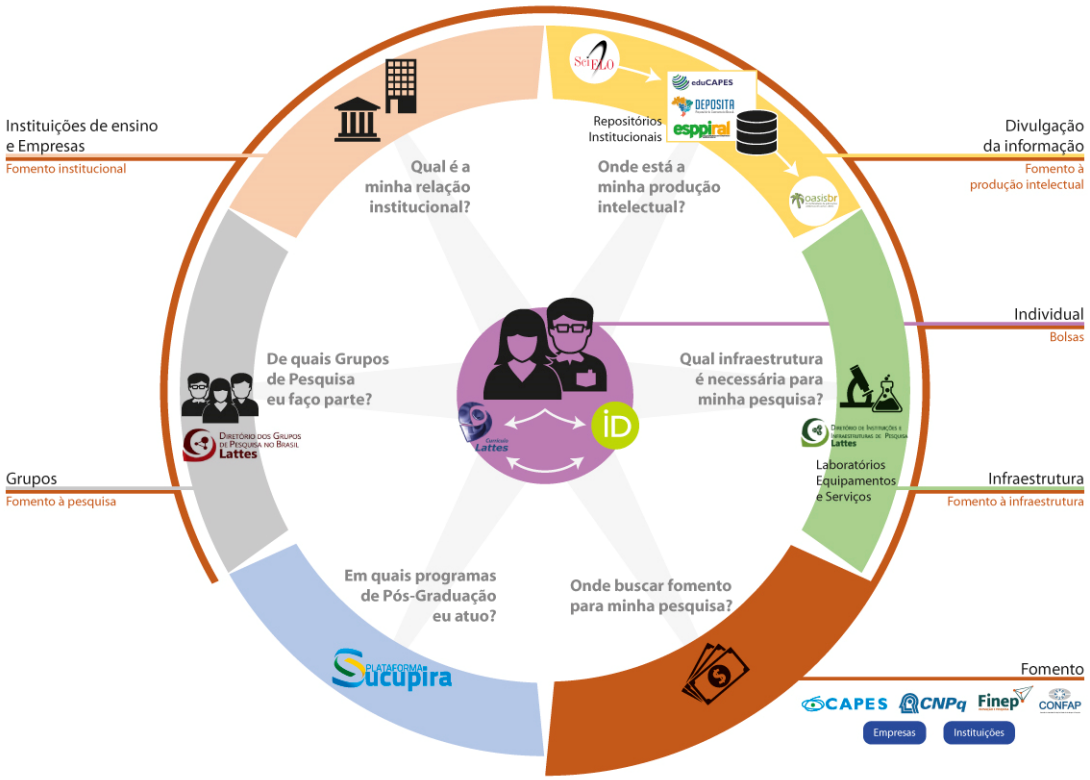
• Coletar, filtrar e disponibilizar conteúdo da ECTI brasileira seguindo padrões nacionais e internacionais.

• Promover programas de geração e disponibilização de dados abertos.

• Viabilizar acordos internacionais na forma de consórcio (por exemplo, assinatura e adoção do ORCID como identificador persistente de pesquisadores).

• Agregar as informações acadêmicas, científicas e de fomento da pesquisa brasileira, ao integrar os sistemas já existentes, como a Plataforma Lattes, a Plataforma Sucupira, o OASIS-BR e os repositórios institucionais, conforme mostra a Figura 1.1, que apresenta a relação de interconectividade entre os membros do CMI ao formar o Ecossistema de ECTI.

Figura 1.1: Interconectividade entre os membros.



Fonte: : Conecti Brasil (4).

Ao consolidar esse conjunto de informações, originárias de diversos sistemas, em um único projeto, uma plataforma digital caracteriza-se o que é denominado de *Current Research Information System* (Sistema Atual de Informações de Pesquisa - CRIS). Porque embora tenham sido desenvolvidos como sistemas claramente diferenciados, com diferentes objetivos e funcionalidades, padrões e modelos de dados, e para diferentes necessidades e grupos de usuários (9), possuem características comuns. Os sistemas CRIS ajudam a

conectar os pontos, funcionalidades dispersas entre vários sistemas, ao apoiar pesquisadores, alunos e equipes de pesquisa com tarefas administrativas ao longo do ciclo de vida da pesquisa (10).Uma das principais iniciativas de projetos CRIS é a adoção de um identificador único e agregador de informações, o qual viabiliza a integração entre os bancos de dados dos consorciados (11). Desta maneira, o Consórcio Multi-institucional optou pela utilização do *Open Researcher and Contributor ID* (ID Aberto de Pesquisador e Contribuidor - ORCID) como identificador único e agregador de informações.O objetivo de utilizar um identificar único é reduzir o tempo que os pesquisadores atualmente dedicam para inserir informações repetidamente em várias fontes, além de proporcionar a melhoria da qualidade de dados disponíveis. A adoção do ORCID como agregador promoverá a geração de conhecimento de forma mais sistêmica ao permitir um melhor acompanhamento e análise, inclusive para a definição de políticas públicas. Os dados que serão integrados e sistematizados tornarão mais fáceis e rápidas não só as consultas aos conteúdos, mas também aos dados atrelados ao setor de pesquisa no Brasil, tais como docentes, discentes, concessão de bolsas e fomento a nível federal e estadual no país e no exterior, produções científicas, projetos de pesquisa e colaborações científicas (4).

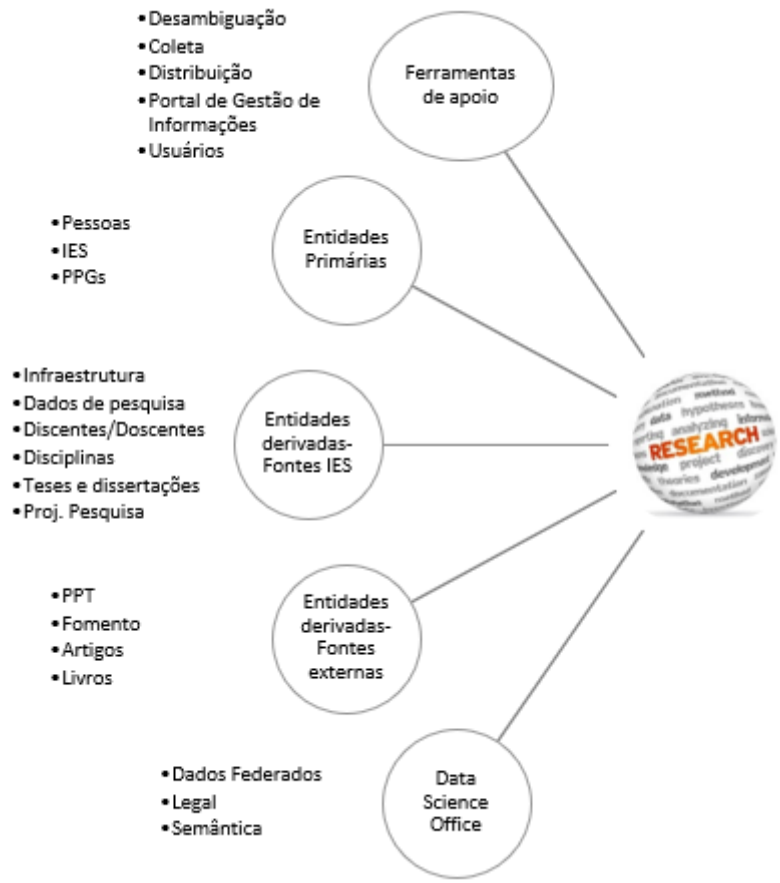
1.1 Contextualização do Problema

No Brasil é comum que organizações públicas e privadas, desde que com objetivos em comum, formem associações (consórcios). A partir de um consórcio, dentre outros aspectos, é possível compartilhar os riscos com as instituições privadas, maximizar a qualidade no fornecimento de serviços, aumentar a capacidade de desenvolver produtos relacionados a inovações, aumentar a competência de realizar projetos, e assim por diante. Contudo, é importante ressaltar a existência de leis e códigos os quais delimitam a criação e atuação de cada instituição partícipe de consórcios. Um bom exemplo é a Lei 11.107, art. 1º, § 1º, que define a possibilidade de constituição de um consórcio público por uma associação pública ou pessoa jurídica de direito privado (12). A referida lei é uma derivação do artigo 241 da CF/88 (13); e a Lei nº 11.079 define as normas gerais quando o consórcio for celebrado entre instituições públicas e pessoa jurídica de direito privado (14). Dessa forma, a criação de parcerias entre entes públicos e privados no Brasil, perante a Administração Pública direta e indireta, segue a aplicação da política de conformidade com normas, leis, regulamentos, políticas públicas, instruções normativas e diretrizes estabelecidas. Além de parcerias público-público uma segunda forma de colaboração entre à Administração Pública e o segmento privado são os consórcios ou Parcerias Público-Privado, as também conhecidas PPP.

Em pesquisa realizada nas bases de dados da Scopus e *Web of Science*, percebe-se que a cooperação público-privada, com foco em financiamento de projetos, aumenta a níveis globais (15). Em diferentes contextos, as parcerias são cada vez mais percebidas como uma abordagem política inovadora capaz de promover uma educação de melhor qualidade e oferecer às populações desfavorecidas novas oportunidades educacionais (16). Elas estão presentes em vários segmentos, como na esfera da educação superior cujas PPP são definidas como um sistema de relações de longo prazo mutuamente benéficas entre o Estado e as empresas, com vistas à distribuição eficiente de papéis entre os parceiros na esfera da Educação Superior para melhorar a competitividade do ensino (17). Porém, o recente aumento das Parcerias Público-Privado, consórcios, convênios e contratos entre governos nacionais e empresas privadas acrescentou uma nova dimensão ao debate relativo à vantajosidade desses acordos, uma vez que essas parcerias requerem o envolvimento colaborativo de diferentes grupos de atores os quais muitas vezes são impulsionados e respondem a sistemas de valores e padrões de comportamento diferentes, às vezes conflitantes (18).

Neste cenário, que envolve as PPP, o Consórcio Multi-institucional é alvo do presente estudo, sendo formado por instituições públicas e privadas. As organizações públicas são responsáveis pelo fomento do ensino, pesquisa e produção científica. Por sua vez, as instituições privadas são responsáveis pela publicação digital de periódicos científicos e redes avançadas em tecnologia da informação. Dessa maneira, as instituições públicas e privadas as quais integram o Consórcio Multi-institucional formam o Ecossistema ConectiBR, conforme Figura 1.2.

Figura 1.2: Ecossistema ConectiBR



Fonte: : Conecti Brasil (4).

Imagem: Direitos autorais: kbuntu - Fotolia.

Ao implantar o Ecossistema de pós-graduação e ciência brasileira, de forma automática, busca-se proporcionar oportunidades de ganho significativo de eficiência e economia através da geração e oferta aberta de informações abrangentes, precisas e atualizadas sobre todas as entidades e agentes que produzem ou fomentam ciência no Brasil. O conhecimento gerado e compartilhado no âmbito do consórcio é sensível e está relacionado à criação de informação, proveniente de pesquisadores, instituições, projetos e seus respectivos produtos científicos. Tais dados auxiliarão agências governamentais, organizações de ensino, fomento e até mesmo o pesquisador individual a melhor gerir e planejar suas atividades e recursos. São exemplos de possíveis benefícios do Ecossistema:

Pesquisadores:

- Melhorar o reconhecimento e a visibilidade de sua pesquisa.
- Dedicar mais tempo para pesquisa e menos tempo administrando-a.
- Controlar e administrar um registro confiável e facilmente compartilhável de suas atividades de pesquisa e afiliações, gratuitamente.

Instituições:

• Poupar tempo e reduzir erros com o compartilhamento automatizado de informações e a interoperabilidade cruzada entre sistemas.

• Administrar o nome de sua organização e as conexões de seus pesquisadores com ela.

• Manter vínculos com seus pesquisadores – passados, atuais e futuros.

Sociedade:

• Conhecimento.

• Prestação de contas.

• Serviços integrados.

• Maior visibilidade internacional.

Gestores:

• Otimizar a aplicação dos recursos para pesquisa.

• Maior qualidade dos dados.

• Serviços integrados.

• Gestão integrada das informações de pesquisa.

Comunidade Científica:

• Menos trabalho operacional; mais tempo para pesquisa.

• Informações úteis a pesquisas em grupo e parcerias.

• Maior divulgação científica.

Com relação à visão estratégica, negocial e holística, alinhadas às expectativas dos *Stakeholders*, o ciclo de vida da PNID é composto por ações de Governança de TI - GTI e por definições de Estratégias e Desenvolvimento de Interface de Programação de Aplicações - API e Infraestrutura de TI. Salienta-se, ainda, que esse trabalho de pesquisa contempla somente as ações de Governança de TI.

1.2 Problema de Pesquisa

Diante de um ecossistema de informações em pesquisa com foco no pesquisador, o qual integra sistemas federais e estaduais, além disso otimiza a gestão do conhecimento, com recursos humanos e financeiros limitados a um problema de pesquisa, emerge a questão: como priorizar ações de Governança de TI e aplicar a Gestão de Riscos no contexto do principal ativo de Tecnologia da Informação vinculado a Governança TI?

Primordialmente, a primeira ação a qual justifica o trabalho de pesquisa envolve ações de Governança de TI voltadas para o Consórcio e requerem que suas atividades sejam priorizadas. Ademais, por diversos motivos, essa ordenação necessita ser materializada e um bom exemplo diz respeito ao Compliance à nova gestão pública. Essa nova gestão tem

se pautado em resultados, além de buscar melhores desempenhos, eficiência no emprego dos recursos públicos e incremento na responsabilidade governamental (19). Assim, o *International Federation of Accountants* (Federação Internacional de Contadores - IFAC) (20) realizou um estudo intitulado de Boa governança no setor público: esboço de consulta para uma estrutura internacional, o qual definiu que a Governança compreende a estrutura (administrativa, política, econômica, social, ambiental, legal, entre outras), essencial para garantir que os resultados pretendidos pelas partes interessadas sejam definidos e alcançados. A mesma Federação Internacional (21) elencou, sob sua ótica, os benefícios proporcionados pela boa governança no setor público, a qual oportuniza, dentre outras:

I. Garantir que a organização seja, e pareça, responsável para com os cidadãos.

II. Ser transparente, mantendo a sociedade informada acerca das decisões tomadas e dos riscos envolvidos.

III. Garantir a existência de um sistema efetivo de gestão de riscos.

IV. Controlar as finanças de forma atenta, robusta e responsável.

V. Possuir e utilizar informações de qualidade e mecanismos robustos de apoio às tomadas de decisão.

Sem dúvida as ações de Governança de TI no âmbito do Consórcio Multi-Institucional necessitam serem priorizadas, pois os recursos financeiros são limitados, dependem de repasse público, e a exemplo do estudo realizado pelo IFAC (21), o CMI necessita estar em conformidade com a boa governança no Setor Público Brasileiro. Em termos de investimento, o Consórcio conta com a participação de instituições privadas, porém a maior fonte de fomento ao projeto é proveniente da União, pois são recursos públicos. Com isso, a administração financeira do CMI necessita de um bom gerenciamento, e em resumo, maiores controles, transparência, Gestão de Riscos e priorizar as ações da Governança de TI podem garantir a execução orçamentaria de acordo com os limites empenhados. Essa priorização é fundamental, porque a Gestão de Riscos será aplicada no contexto do principal ativo de TI que possa, direta ou indiretamente, inviabilizar a continuidade do desenvolvimento dos serviços providos pela PNID.

Assim sendo, a partir da priorização das alternativas, as quais serão conhecidas durante a aplicação da Fase 2 (definição do modelo de apoio a decisão) da Metodologia, é que o principal ativo de TI, vinculado a ações de Governança de TI do Consórcio, pode ser identificado. Para o CMI é fundamental aplicar uma efetiva Gestão de Riscos a esse ativo, pois a Plataforma Nacional de Integração de Dados centraliza e disponibiliza dados sensíveis relacionados a pessoas, Instituições de Ensino Superior, Programas de Pós Graduação, dados de pesquisas, teses e dissertações, dados federados, artigos, dentro outros. Por fim, a proposição de um modelo de GR é fundamental para continuidade do negócio.

1.3 Justificativa do Tema

Segundo o Corpo de Conhecimento em Gestão de Projetos, ou simplesmente PMBOK (22), existem dois tipos de riscos de projeto: o individual e o geral (22). O risco individual é um evento ou condição incerta que, se ocorrer, provocará um efeito positivo ou negativo em um ou mais objetivos do projeto (22). Já o risco geral é o efeito da incerteza do projeto no seu todo, decorrente de todas as fontes de incerteza, incluindo riscos individuais, representando a exposição das partes interessadas às implicações de variações no resultado do projeto, sejam positivas ou negativas (22).

No contexto da Plataforma Nacional de Integração de Dados os riscos podem ser provenientes de ativos relacionados direta ou indiretamente a Governança de TI, além de diversas fontes ou origens, por exemplo, bases de dados, documentos, equipamentos, locais físicos, pessoas, sistemas e unidades organizacionais públicas e privadas. Desta forma, a quantidade de riscos, os quais perpassam o CMI, inegavelmente, são inúmeros, pois cada membro pode suscitar uma série de eventos desconhecidos. Resumidamente, a complexidade das conexões entre riscos e ativos são análogas a quantidade de atores, aos sistemas e às instituições da pós-graduação que se relacionam com o negócio da Plataforma e, respectivamente, com o Consórcio. Uma iniciativa dessa amplitude carece de uma sólida Gestão de Riscos - GR que possa mitigar eventos negativos durante e após a implementação da Plataforma. À vista disso, essa Gestão de Riscos carece de alinhamento ao Compliance (conformidade) alusivo a normas, leis, decretos, frameworks (padrões) e ferramentas computacionais voltadas para projetos com dados integrados, compartilhados e sensíveis. Acrescentando-se que, a PNID agrega informações dos principais entes públicos de fomento à pesquisa e educação no Brasil (CAPES, CNPq e instituições de Ensino Superior), e nesse universo as seguintes ações são justificáveis no âmbito desse trabalho para suporte ao CMI:

a) Apoio na definição de priorização de ações de Governança de TI, pois existem limitações orçamentárias e de recursos humanos para execução do projeto.

b) Adoção da Gestão de Riscos no âmbito da Plataforma Nacional, uma vez que inexiste essa boa prática.

c) Conformidade referente às leis nacionais e internacionais de proteção de dados pessoais e de pessoas jurídicas voltadas para compartilhamento de dados.

d) Redução de impactos negativos inerentes à arquitetura da PNID, a qual é voltada para serviços, com dados coletados (extração, transformação e carga), desambiguados, tratados semanticamente, base de dados centralizada e informações compartilhadas entre vários entes (pessoas físicas e jurídicas).

e) Possibilitar transparência aos Stakeholders quanto a criticidade dos riscos, os quais envolvem a iniciativa do CMI.

A PNID recebe, trata e compartilha dados, os quais estão expostos a riscos relacionados ao acesso, a modificação e a remoção não autorizada, perda, roubo, retenção prolongada de dados sem necessidade, compartilhamento ou distribuição de dados pessoais com terceiros fora da administração pública federal, sem o consentimento do titular dos dados pessoais, entre outros (23). Esses dados requerem proteção e aplicação de boas práticas de segurança, sigilo e governança, pois em contrário, o Consórcio pode, por exemplo, responder legalmente e sofrer sanções administrativas por não estar em conformidade com leis ou decretos relacionados à proteção de dados pessoais De acordo com a Lei nº 13.709 (23), são sanções administrativas aplicáveis pela autoridade nacional: advertência, multa, bloqueio e eliminação dos dados, suspensão do exercício da atividade de tratamento dos dados e proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. Caso esses riscos se concretizem o Consórcio, provavelmente, terá dificuldades para oferecer serviços aos pesquisadores, instituições, sociedade, gestores e comunidade cientifica.

1.4 Objetivos

Esta seção contém os objetivos geral e específicos, os quais guiarão a pesquisa e estabelece os resultados pretendidos, com o consequente limite do escopo, além do alinhamento referente aos passos a serem dados.

1.4.1 Objetivo Geral

O objetivo geral desta pesquisa é apresentar um modelo de Gestão de Riscos de Tecnologia da Informação, que possa viabilizar o gerenciamento dos riscos para ativo crítico de Governança de TI em um Consórcio Multi-institucional de Ensino e Pesquisa.

1.4.2 Objetivos Específicos

1. Descrever o cenário de tomada de decisão que envolve os entes membros do CMI para conceber a Plataforma Nacional de Integração de Dados.
2. Determinar a hierarquização das ações alternativas para Governança de TI para o CMI.
3. Validar a ordenação das ações alternativas, a fim de identificar o ativo crítico para Governança de TI.
4. Identificar metodologias de Gerenciamento de Riscos aplicáveis ao contexto do estudo.

5. Adaptar metodologia de gerenciamento de risco identificada ao contexto.

1.5 Contribuição Esperada

Propor um modelo de Gestão de Riscos que seja aplicável ao Consórcio Multi-institucional, além de mitigar os riscos relacionados a continuidade da PNID. Propõe-se, também, a demonstrar a efetividade da relação entre academia, Administração Pública e mercado privado, maximizando a importância do mestrado profissional ao aplicar o conhecimento científico a práticas e necessidades ágeis requeridas por sociedade, entes públicos e privados.

1.6 Estrutura do trabalho

O presente trabalho de pesquisa está ordenado em cinco capítulos, o qual a Introdução é o primeiro. Os demais capítulos buscam instituir uma ordem cronológica evolutiva da pesquisa, a saber:

Capítulo 2 - Revisão do estado da arte.

Capítulo 3 - Definição da metodologia proposta.

Capítulo 4 - Estudo de caso, o qual envolve o CMI.

Capítulo 5 - Conclusão relacionada aos achados, considerações finais e trabalhos futuros.

Capítulo 2

Revisão do Estado da Arte

2.1 Consórcio, Contratos e Parcerias Público-Privado

Consórcios, contratos e Parcerias Público-Privado são formas de ação do poder público, os quais buscam expandir o financiamento e a prestação de serviços de Educação, Comunicação, Tecnologia e Inovação. São vistos como oportunidades para corrigir a ineficiência na oferta pública de educação e para mobilizar novos recursos, a fim de aumentar o acesso e reduzir o custo da educação (24).

Ainda por cima, essas parcerias são consideradas, também, como um conjunto de formas distintas de organizar as relações econômicas de longo prazo entre instituições educacionais estatais e não estatais, fundadores, empresas privadas e consumidores de serviços educacionais. Essas organizações buscam, identicamente, a alienação conjunta de capital, bem como posse, apropriação e uso de valor agregado mediado pela influência do mercado de trabalho (25).

Apesar disso, as relações que envolvem o setor educacional podem gerar uma série de dúvidas quanto a eficácia e eficiência devido ao ponto de vista largamente difundido da educação como atividade política e social complexa, e que deve permanecer, em grande parte, se não na totalidade, no setor público e a serviço dos interesses públicos (26).

Entretanto, a realidade dos resultados alcançados no setor educacional brasileiro tem demonstrado os benefícios gerados por essas iniciativas. Um exemplo dessa combinação foi identificado no estudo realizado por Chattopadhay e Nogueira (27), cuja parceria firmada entre a Secretaria de Estado da Educação e empresas privadas do segmento de telecomunicações e varejo, com a proposta de criar e aplicar um modelo de sustentabilidade em duas escolas públicas do Estado do Rio de Janeiro, demonstrou notáveis resultados. À vista disso, os autores concluem a geração de excelentes resultados ao apresentar um modelo educacional com potencial para realizar uma reforma a nível nacional no ensino

público. Porquanto, se mostrou inovador, sustentável e ofereceu melhorias na qualidade dos resultados alcançados pelos alunos.

Apesar dos resultados alcançados, como pode ser observado no caso de sucesso (27), a geração de ensino com qualidade encontra alguns obstáculos. Pois, prover educação básica e superior com sinergia, fomentar a interação dos agentes de educação e garantir níveis de qualidade no ensino que sejam capazes de atender as expectativas, em termos de resultados a alunos, pais e educadores, é um desafio para o Brasil empreender recursos e desenvolver políticas educacionais. Em vista do que foi citado, o país necessita de maiores investimentos no sistema educacional, dessa forma, Fontanela, Santos e Da Silva Albino (28) entendem que no Brasil, uma das tendências para fomentar a interação entre os agentes de educação é a combinação de esforços entre as universidades e o setor produtivo. Esse acordo, segundo os autores, pode resultar na formação de parques regionais de pesquisa universitária, os quais além do ensino, são direcionados à comunidade com o propósito de gerar diversas atividades sociais ao longo de várias décadas. Nesse sentido, as conclusões sugerem que as parcerias contribuem para o desenvolvimento das IES e respectivas regiões as quais se situam.

Outra pesquisa importante que envolve não apenas as instituições de ensino superior localizadas nas capitais, mas também outros níveis de escolaridade situados nas diversas partes do país foram desenvolvidos por de Brito e Marins (29). Os autores examinaram a Fundação Lemann, instituição privada, sem fins lucrativos, atuante em programas e projetos para as redes de ensino, municipais e estaduais, em todas as regiões do Brasil com governos estaduais e outras entidades da sociedade civil de forma inclusiva. Após analisarem uma série de índices relacionados aos resultados alcançados pela Fundação, os autores sugerem que a iniciativa publica-privado é um importante componente proporcionado pelo Estado, pois alcança desde a pré-escola até instituições de ensino superior ao fornecer programas de liderança, soluções inovadoras, além de mobilizar ações para prover internet às escolas atendidas por essa parceria.

Outro meio de associação entre IES e Iniciativa Privada, intitulada Coopetição, avança com bons resultados. Essa forma de consórcio preconiza a competição e cooperação mútua entre seus consorciados, ou seja, a pesquisa e a prática de negócios de forma estratégica e dinâmica para impulsionar o desenvolvimento de novos negócios (30). A Coopetição, da mesma forma, foi estudada por Dal-Soto e Monticelli (2017) (31), a partir do Consórcio das Universidades Comunitárias Gaúchas, formado por 15 instituições de ensino superior localizadas na região Sul do Brasil. Consoante aos autores, a pesquisa resultou na identificação e criação de valor a partir de mecanismos de proteção ao mercado, competição entre empresas e transferência de conhecimento por meio da cooperação. Portanto, essas ações em conjunto proporcionam um aumento da base de clientes e maximizam o desempenho

financeiro, desde que os cooperados consigam equilibrar a competição e cooperação.

Certamente, a transferência de conhecimento entre os membros da colaboração pública-privada é fundamental para sustentar a infraestrutura de conhecimento existente na parceria. Assim, Mundim e Silva (2019) (32) apresentaram os resultados parciais de uma pesquisa que relaciona a gestão estadual com a interação público-privada, tendo como foco o sistema educacional do estado do Goiás e o Instituto de Corresponsabilidade na Educação-ICE. O organismo é uma instituição privada, a qual atua desde 2013 em mais de quarenta escolas de ensino médio. Após concluírem essa fase fracionária do estudo, os autores identificaram um produto intitulado Projeto de Vida o qual foi estabelecido pela gestão estadual e o ICE. O Projeto de Vida se configura como um manual de boas práticas, orientações e prescrições cujo objetivo visa guiar o jovem a uma reflexão relativa à sua capacidade de ser autônomo, solidário, competente e capaz de alterar seu destino.

Finalmente os autores inferem que o produto pode introduzir para os alunos a lógica empresarial, de mercado, influenciar no modo de pensar, desenvolver competência, competitividade e aprender a gerenciar a própria vida. Por conseguinte, avaliam que as PPP atuantes no sistema educacional, a partir de estratégias, dispositivos pedagógicos e gerenciais bem definidos, contribuem para formação de novos indivíduos preparados para o mundo globalizado. Certamente é conhecida a necessidade de uma boa formação educacional, pois a globalização de forma ampla está associada à crescente mobilidade de bens, serviços, commodities, informações, pessoas e comunicações através das fronteiras nacionais (33). Por consequência da globalização, uma empresa global de tecnologia localizada no Polo Industrial de Manaus firmou parceria com uma universidade local, a fim de definir e executar um programa de qualificação rápida e dedicada aos estudantes e profissionais de TI na área de automação de testes de *software* (34). Ao término do programa proposto os alunos, os quais participaram da iniciativa, tornaram-se multiplicadores e foram empregados no Polo Industrial. Portanto, os pesquisadores defendem que o sucesso da parceria foi devido ao comprometimento dos envolvidos (alunos, patrocinador, universidade e instrutores), outrossim, o modelo elaborado pode ser replicado em cenários semelhantes, os quais a falta de infraestrutura pode ser compensada com o incentivo profissional e eficiência pedagógica.

Por certo, a capacidade de gerenciar o programa educacional, seja ele na competência federal, estadual ou municipal, certamente exige sinergia e participação entre os envolvidos. Esse foi o desafio assumido por Miranda, Cunha e Pereira (2020) (35), ao estudarem a utilidade e interesse do Estado brasileiro em conjunto ao governo da Bahia. Objetivo dessa parceria foi regulamentar a gestão da educação no espaço territorial por meio de Consórcios Públicos e PPP, como estratégia de colaboração e cooperação no federalismo brasileiro. Nesse ínterim, de acordo com os autores, foi possível identificar a falta de

intenção dos membros consorciados para explorar a potencialidade disponível, ampliar a atuação e aperfeiçoar o suporte aos beneficiários no alcance das metas educacionais. Em contraste à percepção da falta de compromisso de alguns envolvidos, os escritores reconhecem a eficácia e eficiência, típicos do segmento empresarial, nos formatos de arranjos público-privados. Indubitavelmente, a coparticipação no âmbito das Instituições Públicas e Privadas, no Brasil, abrange diversas citações na literatura conforme observam (36), (37) e (38).

Do mesmo modo que no Brasil as parcerias firmadas pela Administração Pública e o Setor Privado são relevantes, no contexto internacional a cooperação entre instituições públicas e privadas, em conformidade com a literatura, representam um importante meio de impulso à educação. Visto que potencializam o desenvolvimento de alunos, profissionais de educação, pesquisadores, IES, estimulam ideias inovadoras e alavancam a criação de novas oportunidades de trabalho (39). Uma amostra dessa colaboração pode ser observada entre a Universidades de Bolonha e a Agência Regional de Prevenção, Meio Ambiente e Energia - ARPAE. Essas organizações investigam o panorama atual do sistema de reciclagem de resíduos plásticos na Itália com o objetivo de descobrir em que medida o desempenho atual vai ao encontro do cenário futuro estabelecido pela Comissão Europeia quanto ao uso de plástico e melhoria maciça de gestão de resíduos (40). Esse estudo resultou em um acervo de recomendações consonante à gestão de resíduos plásticos e visões de cenários futuros, os quais viabilizam estratégias capazes de capturar o valor intrínseco dos materiais plásticos para potencializar a criação de negócios lucrativos.

Análogo ao trabalho desenvolvido pela Universidade de Bolonha e a ARPE (2021) (40), Hogan (2016) (41) realizou uma análise crítica dos negócios educacionais envolvidos com a Autoridade de Currículo, Avaliação e Relatórios da Austrália. Conforme indicação do autor, essas parcerias público-privadas emergentes exemplificam novas estruturas de governança heterárquica na Austrália, pois agentes públicos e privados contribuem para elaborar novos processos da política educacional. O autor dispõe o valor agregado com as mudanças aplicadas na estrutura de governança australiana, assim como destaca a convergência de agentes públicos e privados atuantes na política educacional. É importante ressaltar que os agentes públicos são fundamentais para o sucesso de ações públicas e privadas conforme destacam Osei-Kyei e Chan (2018) (42), ao comparar as visões do setor público em relação as práticas de PPP sucedidas em Gana e Hong Kong. A pesquisa elicitou informações relativas à realização de projetos educacionais com e sem a participação de instituições privadas e proporcionou a criação de uma metodologia baseada em PPP. Após coletarem informações junto à profissionais de instituições públicas e aplicarem a metodologia os resultados demonstram uma melhoria na execução de projetos governamentais com entregas rápidas, no prazo acordado, sem extrapolar o orçamento,

com qualidade, além de garantir a satisfação dos usuários do segmento de educação. Segundo os autores, os resultados do estudo oferecem estratégias úteis para interessados em práticas de PPP na África e na Ásia.

Bem como os trabalhos de pesquisa anteriormente apresentados, educação como estudo de caso, Carpintero e Siemiatycki (2015) (43) investigaram a aquisição de novas escolas subvencionadas na região de Madrid, Espanha, de 2005 a 2012. Essa aquisição foi de 56 escolas, as quais fornecem educação para cerca de 60.000 alunos com um investimento total por volta de 650 milhões de euros. Diante disso, os autores explicam o motivo dessa aquisição ser bem-sucedida, ao contrário de certos projetos de PPP de escolas em outros países e iniciativas de parcerias em determinadas partes do serviço público espanhol não obterem o sucesso esperado. Por outro lado, há outra forma de políticas educacionais raramente estudada, sob o mesmo rito das parcerias, da qual a popularidade aumenta em consideráveis proporções (44). Trata-se de um governo financiar escolas internacionais privadas em outro país. Em virtude desse tipo PPP, os autores examinaram as razões pelas quais os governos firmam esse tipo de contrato, assim como buscaram entender o ganho para o sistema de educação proveniente desse investimento. Eles finalizam a abordagem ao relacionar a ambição dos governos de integrar um currículo internacional a educação pública local sob a forma de ampliação das melhores práticas e inovação na esfera de suas políticas públicas. Outrossim, consideram a possibilidade de estender esses benefícios a todos ao longo do tempo.

Em síntese, as parcerias existentes a partir do uso de Consórcios Públicos e PPP, com ênfase em educação, estão relacionadas a diversos trabalhos presentes na literatura, conforme pode ser observado nos exemplos: Hendre et al.(2019) (45), Graham et al. (2019) (46), Mengal et al. (2018) (47), Capurro et al. (2017) (48), Patel et al. (2021) (49) e Jongbloed e Vossensteyn (2016) (50).

No contexto que envolve os segmentos de Tecnologias, Inovações e suas várias aplicações a literatura evidencia que existe uma forte dinâmica. De certo, a formação de consórcios e suas variantes são bastante exploradas e difundidas como pode ser observado nos exemplos de Milenkovic, Rasic e Vojkovic (2017) (51), Dey (2018) (52), Kassen (2018) (53), Díaz-Díaz e Pérez-González (2016) (54), Weerakkody et al. (2017) (55) e Atmo et al. (2017) (56), dentre outros.

Mediante o exposto, os resultados confirmam a vantajosidade para o setor público e justificam a expansão dos consórcios, contratos e parcerias público-privado. De fato, os resultados justificam o investimento em realizar alianças público privado, entretanto, é importante que essas relações sejam coordenadas a partir de uma boa governança, sejam elas de TI ou corporativa. Uma vez que o setor público dispõe de governança corporativa e relacionamentos de responsabilidade diferentes e potencialmente conflitantes

para administrar em comparação com o relacionamento único de direção, o qual é o foco da governança corporativa do setor privado (57).

2.2 Governança de TI

Produzir o conceito de Governança de TI e tudo a ver com ele para alcançar o alinhamento e integração com a governança corporativa tem sido um grande esforço da academia, empresas de consultoria, parcerias de pesquisa, órgãos reguladores e organizações de normalização (58). Diversas iniciativas podem corroborar com essa produção como, por exemplo, o Gartner (59) que define GTI como os processos os quais garantem o uso eficaz e eficiente de TI para permitir que uma organização alcance seus objetivos.

O *Information Technology Governance Institute* (Instituto de Governança de Tecnologia da Informação - ITGI (60), por sua vez, define como um elemento da governança corporativa, que visa melhorar a gestão geral de TI e obter maior valor do investimento em informação e tecnologia. Com isso, as estruturas de Governança de TI permitem que as organizações gerenciem seus riscos de TI com eficácia e garantem que as atividades associadas à informação e tecnologia estejam alinhadas com seus objetivos gerais de negócios (60). Para o Isaca a GTI é de responsabilidade dos executivos e do conselho de administração e consiste, ainda, na liderança, estruturas organizacionais e processos os quais garantem que a TI da empresa sustenta e estende a estratégia e objetivos (61) corporativos.

Paralelamente aos institutos, existe o padrão internacional relacionado à Governança de TI que é a norma ISO/IEC 38500 (62), a qual é bastante difundida. Essa norma fornece princípios orientadores para os membros de órgãos diretivos de organizações (que podem incluir proprietários, diretores, sócios, gerentes executivos ou semelhantes) sobre o uso eficaz, eficiente e aceitável de TI dentro de suas organizações (62). São exemplos de aplicação do padrão ISO/IEC 38500 de acordo com a literatura: Jairak,Praneetpolgrang e Subsermsri (2015) (39), Quezada-Sarmiento et al. (2017) (63), Oñate-Andino et al. (2018) (64) e Espinoza-Aguirre e Pillo-Guanoluisa (2018) (65). Como se não bastasse, a governança corporativa é um mecanismo de tomada de decisão para controlar, monitorar e gerenciar (66) as decisões dos dirigentes públicos ou privados.

2.3 Modelo de apoio à decisão

A tomada de decisão de um gestor público, por si só, é algo complexo e deve seguir o ditame do regramento legal (leis, portarias, decretos, instruções normativas, dentre outras), além de serem auditados por órgãos de controle - caso do Tribunal de Contas

da União (TCU) e Controladoria Geral da União (CGU). Esses órgãos visam validar a aderência do gestor público quanto a Governança Pública.

Em 2018, o TCU realizou um estudo do qual identificou o baixo nível de maturidade em relação à Governança Pública. Esse estudo foi realizado com 581 órgãos e entidades integrantes da Administração Pública Federal, com o objetivo de obter e sistematizar informações sobre a situação de Governança Pública, Governança de TI, Gestão de Tecnologia da Informação (TI), contratações, pessoas e resultados (67). Para o cálculo dos valores, foi utilizado o Índice Integrado de Governança e Gestão - iGG, composto pelo índice de governança pública, de governança e gestão de pessoas, de governança e gestão de TI, de governança e gestão de contratações e pelo índice de resultados. O resultado do estudo demonstra que 41% das organizações estão no estágio inicial quanto à Governança Pública. Governança e gestão foram contabilizadas 58% das organizações em estágio de capacidade inicial e, por fim, 50% no estágio inicial quanto a Gestão de TI (68). Assim, o órgão de controle aferiu que a maioria das instituições federais não possui capacidade de entregar à sociedade o que se espera, seja por deficiência em liderança, estratégia ou *accountability* (controles), seja por carências na gestão de operações (planejamento, execução e controle) ou Governança de TI (67).

Esse estudo ratifica a necessidade de o gestor público buscar seguir as melhores práticas de mercado, *frameworks* (estruturas) e normas de Gestão Corporativa de TI, conformidade com leis, e aperfeiçoar seus métodos de realização da Gestão da Pública. Em contrapartida, gestores da iniciativa privada ao realizarem a tomada de decisão visam, em muitos casos, o retorno referente ao investimento, seja ele em forma de recursos financeiros, imagem da instituição ou oportunidades de mercado. Assim, tanto para o gestor público quanto para o gestor da iniciativa privada a tomada de decisão caracteriza-se por ser uma deliberação sensível.

Na ocasião em que a tomada de decisão envolve instituições públicas e privadas coordenando um mesmo projeto, a relação entre eles pode ser problemática devido ao conflito de interesses entre às coisas públicas e ao interesse dos sujeitos privados (69). Assim, percebe-se a existência de uma notória intervenção da esfera pública, por intermédio do financiamento estatal convergente com políticas públicas, ao referir-se as suas relações com colaboradores privados (70). Outro fator a ser considerado é o falso pensamento de subordinação do ente público em relação ao privado, pois ambos podem financiar o mesmo projeto.

Diante desse complexo cenário, o qual envolve a tomada de decisão, a Análise de Decisão Multicritério - MCDA, um campo pertencente à Pesquisa Operacional, apresenta uma boa alternativa para mitigar o hermético processo decisório e reúne uma série de métodos aplicados a problemas de decisão (71). Os problemas MCDA (também conhecidos como

tomada de decisão multicritério ou MCDM), envolvem a classificação de um conjunto finito de alternativas em termos de um número finito de critérios de decisão (72). Além do mais, em pesquisa realizada nas bases de dados Scopus (Elsevier) foram apresentados 965 artigos os quais referenciam *Multiple Criteria Decision Analysis* e 3.438 com o critério MCDA. Na base da *Web of Sciences* foram apresentados 1.292 artigos e 2.723 com o critério MCDA. Nesta análise identificou-se a utilização de vários métodos em inúmeras aplicações, dentre eles (73):

- AHP – *Analytic Hierarchy Process* (Processo de Hierarquia Analítica).
- Métodos da família ELECTRE - *Elimination et Choice Traduisant la Realite* (Eliminação e Escolha como Expressão da Realidade).
- Métodos da família PROMETHEE - *Preference Ranking Method for Enrichment Evaluation* (Método de Organização de Classificação de Preferência para Avaliação de Enriquecimento).
- TOPSIS - *Technique for Order Preference by Similarity to Ideal Solution* (Técnica para Ordem de Preferência por Similaridade à Solução Ideal).
- VIKOR - *ViseKriterijumskaOptimizacija i KompromisnoResenje* (Otimização Multicritério e Solução de Compromisso).

Em suma, o apoio à decisão embasado na Análise de Decisão Multicritério possuí uma boa quantidade de métodos aplicáveis a diversos segmentos, a saber: Administração Pública para seleção de fornecedores, decisões públicas e corporativas, Tecnologia da Informação para priorizar investimentos no desenvolvimento de algum serviço ou produto, dentre outros (74). Os métodos MCDA permitem a consideração simultânea dos interesses das partes interessadas e avaliações técnicas, utilizando métodos científicos rigorosos para processar informações técnicas, e é especialmente importante em situações de incerteza significativa e escassez de dados (75), como na Gestão de Riscos em projetos de desenvolvimento de .

2.4 Gestão de Riscos em projetos de desenvolvimento

Os riscos são em geral denominados como ameaças ou incertezas que influenciam o desempenho do projeto e seus resultados em maior ou menor intensidade (76) e podem prejudicar o desempenho do projeto e até mesmo causar o seu fracasso (77). Por isso, planejar respostas aos riscos de um projeto é um componente importante da GR, na busca por garantir o sucesso do projeto (78). Em pesquisa realizada na base de metadados *Web of Science* e ao considerar a palavra chave "Gestão de Riscos", e limitar a busca pela área de “Ciência da Computação” e “Engenharia de Software”, o artigo mais citado é o de Boehm (1991) (79), 614 vezes. Ele sugere que os riscos identificados e gerenciados

no início do desenvolvimento podem reduzir os custos de longo prazo, além de ajudar a prevenir desastres. Ao considerar a base de metadados Scopus (Elsevier), o artigo mais citado é o de Buyya et al.(2009) (80), 3.858 vezes, o qual aborda a computação em nuvem e plataformas de TI emergentes. A prática da GR é uma disciplina abrangente, por buscar maximizar o alcance dos objetivos planejados. Sua aplicação pode ser observada no trabalho de Reed e Angolia (2018) (81), pois considera uma amostra de 557 gerentes de projetos virtuais para avaliar o uso de práticas de gerenciamento de riscos e sua associação com resultados bem-sucedidos ou não. A pesquisa indicou, dentre outros resultados, que os processos mais conhecidos e fáceis são comumente usados. Por outro lado, a utilização de um plano avançado e detalhado de como os riscos são monitorados e gerenciados é menos comumente desenvolvido.

Os dados dos autores (81) são corroborados ao longo do relatório concebido pelo *Standish Group International*, intitulado de Relatório CHAOS (2018) (82), o qual busca consolidar dados relativos a projetos de desenvolvimento de *software*. O relatório considera o alcance das metas no prazo estipulado, cumprimento do orçamento e alcance do escopo definido. Ele agrupa os dados nas categorias sucesso, desafio ou falha. Para o ano de 2018, os dados apresentados foram: sucesso 36%, desafio 45% e falha 19%. Ao considerar a combinação de satisfação do cliente com o retorno sobre o valor para organização, os números diferem: sucesso 14%, desafio 67%, falha 19%. Para o ano de 2020, os dados demonstram sucesso 31%, desafio 50% e falha 19% (83).

Deste modo, o sucesso na GR pode ser observado com práticas das quais sugerem que uma análise de risco bem sucedida inclui elementos como definição e formulação do problema, além da coleta de dados (84). Nesse contexto, o autor propõe o uso de um modelo Tropos, que proporciona a geração de evidências para satisfação e negação. Com isso, o modelo mostrou-se eficaz na análise e na identificação de riscos os quais envolvem requisitos de *software*. Já na abordagem que envolve uma avaliação de custos e complexidade de projetos, os autores Lebedeva e Guseva (2019) (85) desenvolveram um mapa cognitivo de Gestão de Riscos, que evidenciou bons resultados no contexto do desenvolvimento de documentações e relatórios. No quesito de criação e gestão de planos de riscos, a ferramenta desenvolvida por Castro-Rivera, Herrera-Acuña e Villalobos-Abarca (2020) (86) apresentou resultados eficientes, os quais podem apoiar na criação de planos de GR.

À vista disso, a literatura nos apresenta diversos desafios e casos de sucesso os quais envolvem boas práticas de Gestão de Riscos. Por exemplo, no trabalho desenvolvido por García et al. (2018) (87), que estudaram a GR voltada para pequenas e médias empresas e suas dificuldades para implementar as melhores práticas preconizadas por padrões e modelos internacionalmente aceitos em conformidade com o CMMI , ISO, PMBOK, dentre outros. Os autores identificaram eventuais elementos como a falta de recursos econômicos,

humanos, competências, ferramentas e técnicas voltadas para a implementação das práticas recomendadas como potencializadores de eventos negativos no contexto das pequenas e médias empresas. Além disso, para os autores Chadli e Idri (2017) (88), o maior desafio relacionado a GR compreende gerenciar a dispersão das partes interessadas em projetos de *software*. Com isso, a falta da Gestão de Riscos em determinadas situações pode levar a falhas, como é possível observar na literatura.

Todavia, não é apenas a gestão das partes interessadas que pode influenciar no resultado final dos planejamentos. No caso estudado por Mousaei e Gandomani (2018) (89) e Sadia, Abbas e Faisal (2019) (90), o fracasso de projetos de *software* envolve as metodologias adotadas, além de uma insatisfatória engenharia de requisitos como padrão de desenvolvimento. Para Menezes, Gusmão e Moura (2019) (91) as falhas são inerentes aos fatores de mapeamento dos riscos em ambientes de programas de desenvolvimento de projetos. Como contribuição a pesquisa dos autores listou onze dos principais riscos identificados, a saber:

1. A equipe não possui as habilidades necessárias.
2. Ambiguidade de requisitos.
3. Mau comprometimento do usuário/cliente.
4. Mudanças de requisitos.
5. Introdução de nova tecnologia.
6. Ambiente organizacional instável.
7. Fornecimento, externo ao projeto, de componentes e interfaces com baixa qualidade.
8. Complexidade técnica.
9. Nenhum planejamento ou planejamento inadequado.
10. Requisitos incompletos.
11. Baixa qualidade das especificações/documentação.

Com toda a certeza, a Gestão de Riscos realiza um importante papel no sucesso da Gestão de Projetos de desenvolvimento de *software*, dado que todas as fases do ciclo de vida do desenvolvimento são potenciais fontes de riscos, pois envolvem *hardware*, *software*, tecnologia, pessoas, custos e cronograma (92). Isto posto, a GR tornou-se uma das principais atividades em programas de desenvolvimento (93). E além disso, a GR possui uma padronização, a partir de normas internacionais (94) e (95), a qual uniformiza a abordagem relacionada a gestão de riscos.

2.5 Normas sobre Gestão de Riscos

2.5.1 ABNT NBR ISO/IEC 31000

A norma ABNT NBR ISO/IEC 31000 (94) fornece uma abordagem comum para gerenciar qualquer tipo de risco e não é específica para uma determinada indústria ou setor. A norma ISO 31000 (94) é um verdadeiro guia para a implantação eficaz da Gestão de Riscos. Conforme sua própria definição é possível implantar a GR em várias áreas internas sem restrições, a fim de apoiar a tomada de decisão em todos os níveis.

Sem embargo, ressalta-se que deve ser analisada para refletir a necessidade negocial, capacidade e granularidade de seu uso, ou seja, é premissa definir o contexto de sua aplicação. Por meio da implantação e manutenção do processo de GR, com o princípio de seguir o rito da norma ISO 31000 (94), as metas a serem alçadas tornam-se mais fáceis de serem auferidas. Como também viabiliza uma gestão proativa, a qual envolve eventos de riscos, melhora a confiança dos Stakeholders (Partes Interessadas), reduz perdas, entre outras. Assim, o padrão ISO 31000, conforme a própria norma sinaliza, possui diversas aplicações (94). O Quadro 1 demonstra a relação entre as áreas de aplicações, referências bibliográficas e aplicações práticas relacionadas a norma.

Quadro 1: Relação entre áreas, referências e aplicações.

Área de aplicação	Referências bibliográficas	**Aplicações práticas**
Engenharia	Poveda-Orjuela et al. (2020) (96), Chemweno et al. (2020) (97), Spross et al. (2020) (98), Asgari, Kibala e Beauregard (2020) (99) e Dippenaar e Bezuidenhout (2019) (100).	ISO 31000 aplicada a: oportunidades e recursos de energia e água; robôs colaborativos; projeto de engenharia voltado para geologia; transporte e armazenamento de materiais residuais perigosos e GR com ênfase em abastecimento de água.
Economia	Panić et al. (2019) (101), Benetti (2019) (102), Ishaque (2019) (103), McShane (2018) (104) e Paulus (2017) (105).	ISO 31000 aplicada a: GR empresarial no desempenho de empresas ante países em transição; GR corporativo, após a crise financeira global; conflito de interesses em firmas profissionais de contabilidade; risco empresarial e riscos no processo de gestão de segurança.
Ciências Ambientais	Parviainen et al.(2021)[106], Rodríguez-Rosales et. al (2021) (107), Igras e Creed (2020) (108), Bilska, Tomaszewska e Kołożyn-Krajewska (2020) (109) e Creed et al. (2019) (110).	ISO 31000 aplicada a: risco marítimo de derramamento de óleo; riscos e vulnerabilidades em ambientes costeiros aplicados a edifícios históricos; redução da carga de fósforo nas águas superficiais; risco de desperdício de alimentos em estabelecimentos de serviços alimentícios e gestão de riscos para a zona boreal do Canadá.
Tecnologia da Informação	Barafort, Mesquida e Mas (2017) (111), Ni et al. (2016) (112), Großmann e Seehusen (2015) (113), Chemweno et al. (2015) (114), Matheu-García et al. (2019) (115) e Aven e Ylönen (2016) (116).	ISO 31000 aplicada a: integração de atividades baseadas em processos, implementando mecanismos para vincular entidades de TI e não-TI; método de avaliação de risco para sistemas embarcados; segurança cibernética que abrange tanto a avaliação de risco de segurança quanto os testes de segurança; metodologia de seleção de avaliação de risco para tomada de decisão de manutenção de ativos; metodologia de certificação de segurança projetada para IoT e implicações das perspectivas de risco sobre a regulamentação de segurança, usando as indústrias de petróleo, gás e nuclear como case.

Fonte: Autoria própria.

A partir do Quadro 1 é possível reiterar a diversidade de aplicações práticas relacionadas a norma ABNT NBR ISO/IEC 31000 para prover a Gestão de Riscos.

2.5.2 ABNT NBR ISO/IEC 31010

A Norma ISO/IEC 31010 (95) é uma estrutura de apoio à ISO/IEC 31000 (94), da qual fornece orientações relativas à seleção e aplicação de técnicas para o processo de avaliação de riscos. A Norma não é impositiva ou taxativa quanto a aplicação de técnicas ou ferramentas inerentes a análise de riscos, assim como não especifica quais ferramentas e técnicas são adequadas para determinados segmentos de mercado, problema ou negócios. Ressalta-se o cuidado, referenciado pela Norma, alusivo a não invalidação de outras técnicas existentes para suprir a Gestão de Riscos. A Norma lista uma série de benefícios

atinentes ao seu uso, os quais compreendem: entender os riscos e seu potencial impacto; comunicar riscos e incertezas; auxiliar no estabelecimento de prioridades; satisfazer as conformidades regulatórias; dentre outros. A ISO/IEC 31010 é composta pelo Anexo A, o qual apresenta uma série de técnicas para suportar o processo de avaliação de riscos. No Anexo B as técnicas são minuciosamente detalhadas e para um melhor entendimento encontram-se informações relativas à sua visão geral, utilização, entradas, processo, saídas, pontos fortes e limitações (95). Consequentemente então, as normas ISO/IEC 31000 e ISO/IEC 31010 podem ser utilizadas como apoio a Gestão de Riscos de diversas áreas, conforme Quadro 1. Por exemplo, a Engenharia aplicada a exploração de robôs colaborativos ou Tecnologia da Informação na avaliação de risco no desenvolvimento de Plataformas Digitais.

2.5.3 Plataformas Digitais – CRIS

A transição gradual para uma economia digital exige que todas as entidades empresariais ou não se adaptem às novas condições ambientais, as quais ocorrem por meio de sua transformação digital (117).

Essa transformação é suportada por infraestruturas digitais, as quais transformam a inovação e o empreendedorismo (118) em novas estruturas de trabalho que redefinem as fronteiras da indústria setorial e moldam a saúde econômica local e regional (119) e (120). Esse pensamento em torno dessa nova visão traz consigo uma noção de inovação disruptiva, a qual na perspectiva de Gawer (2021) (121) pode ser construída a partir de uma visão econômica, gestão estratégica e pesquisa de sistemas de informação.

Ao mesmo tempo que as organizações tradicionais criam valor dentro dos limites de sua empresa ou cadeia de suprimentos, as Plataformas Digitais - PD alavancam e orquestram um conjunto de funcionalidades criadas a partir da integração de metadados de outros sistemas (122). Destarte, com o amadurecimento na utilização desse tipo de solução foi possível observar o crescimento do seu uso para diversos segmentos de mercado, como economia (123), técnica (124), negócios (125) e social (126).

Essa nova forma de centralização e de compartilhamento de informações requerem uma mudança de mentalidade, logo, Hein et al.(2019) (127) sugerem uma evolução do pensamento, comportamento e atitudes. Desse jeito, as PD são modelos de negócio que operam por intermédio de tecnologias, bem como modificam a forma como são consumidos e fornecidos produtos e serviços. Por isso, as Plataformas Digitais agregam valor ao permitir que gestores coordenem sua relação de dependência por meio de um conjunto de funções e regras semelhantes, a evitar a necessidade de celebração de acordos contratuais customizados com cada parceiro (128). Além do que, com a visão de que as PD são modelos integradores de negócio a literatura apresenta inúmeras aplicações práticas relativas

a esse conceito, como no estudo versado por Gutierrez (2018) (129), o qual retrata uma solução que descreve serviços integradores urbanos. Nesse trabalho as infraestruturas, as quais se relacionam com a *Internet of things* (Internet das coisas - IoT), aparecem como facilitadores para a gestão sustentável de cidades inteligentes por meio de uma plataforma urbana. O resultado do estudo sugere a adoção progressiva de tecnologias IoT em serviços urbanos, os quais permitem a criação de soluções em blocos com o intuito de configurar o paradigma da cidade inteligente. Tal abordagem pode se tornar um dos facilitadores na consolidação de políticas de governo aberto ou na reconfiguração das perspectivas de Ecossistemas de interação de negócios, por exemplo, transporte público ou gestão de resíduos.

Acresce que o emprego de soluções de TI baseadas em Plataformas Digitais relacionam-se, também, ao seu uso. Dessa forma, ao empregar as PD como meio de integração e compartilhamento de informações científicas de pesquisa, elas são conceitualmente chamadas de CRIS, *Current research information system* (Sistema Atual de Informações de Pesquisa), que é um banco de dados ou outro sistema de informação para armazenar, gerenciar e trocar metadados contextuais de pesquisa. Eles podem ser mantidos por um financiador de pesquisa ou sustentados em uma organização executora de pesquisa (ou agregação desta) (130). A seguir serão elencadas amostras de implantações bem sucedidas de Plataformas CRIS:

- **USDA**: a instituição realiza pesquisas contínuas em agricultura, alimentação, nutrição e silvicultura. O sistema contém mais de 30.000 descrições de projetos de pesquisa e com apoio público são conduzidos por agências do USDA, estações experimentais estaduais e agrícolas (em todo o mundo), faculdades e universidades estaduais de concessão de terras, escolas estaduais de silvicultura, escolas cooperativas de medicina veterinária e beneficiários de bolsas do USDA (131).
- **euroCRIS**: fornece um fluxo de informação entre uma ampla variedade de partes interessadas, as quais destacam-se pesquisadores, gestores e administradores de pesquisa, conselhos de pesquisa, financiadores de pesquisa, empresários e organizações de transferência de tecnologia (130).
- **PTCRIS**: a iniciativa busca otimizar o processo de financiamento, facilitar o acesso, a gestão e o reporte da atividade de pesquisa, a medição, a análise e a comparação da atividade científica, a descoberta de tecnologias, as ideias inovadoras, a identificação de concorrentes e os colaboradores, o acesso à informação fidedigna, a completa e a atualizada sobre a atividade científica (132).
- **ICPSR**: consórcio internacional com mais de 750 instituições acadêmicas e organizações de pesquisa. O *Inter-university Consortium for Political and Social Research* (Consórcio Interuniversitário de Pesquisa Política e Social) oferece liderança e treina-

mento em acesso a dados, curadoria e métodos de análise para a comunidade de pesquisa em ciências sociais (133).

• ***CANARIE Research Software***: *Software* de Pesquisa, permite que pesquisadores e desenvolvedores de *software* de pesquisa identifiquem e aprendam sobre eles. Esses sistemas são fornecidos por participantes do programa e por membros da comunidade de pesquisa em geral. Todo o software registrado no portal é de uso gratuito desde que seja para fins de pesquisa. O portal oferece suporte à plataformas e a serviços de software de pesquisa em registros separados. Projetos de pesquisa financiados pela CANARIE retornam à plataforma sob a forma de serviços de *software* de pesquisa (134).

Por fim, é possível, a partir dos diversos exemplos, verificar a evolução das Plataformas Digitais e como são úteis em diversos segmentos e iniciativas distintas. A etapa seguinte do estudo consiste na definição da metodologia utilizada.

Capítulo 3

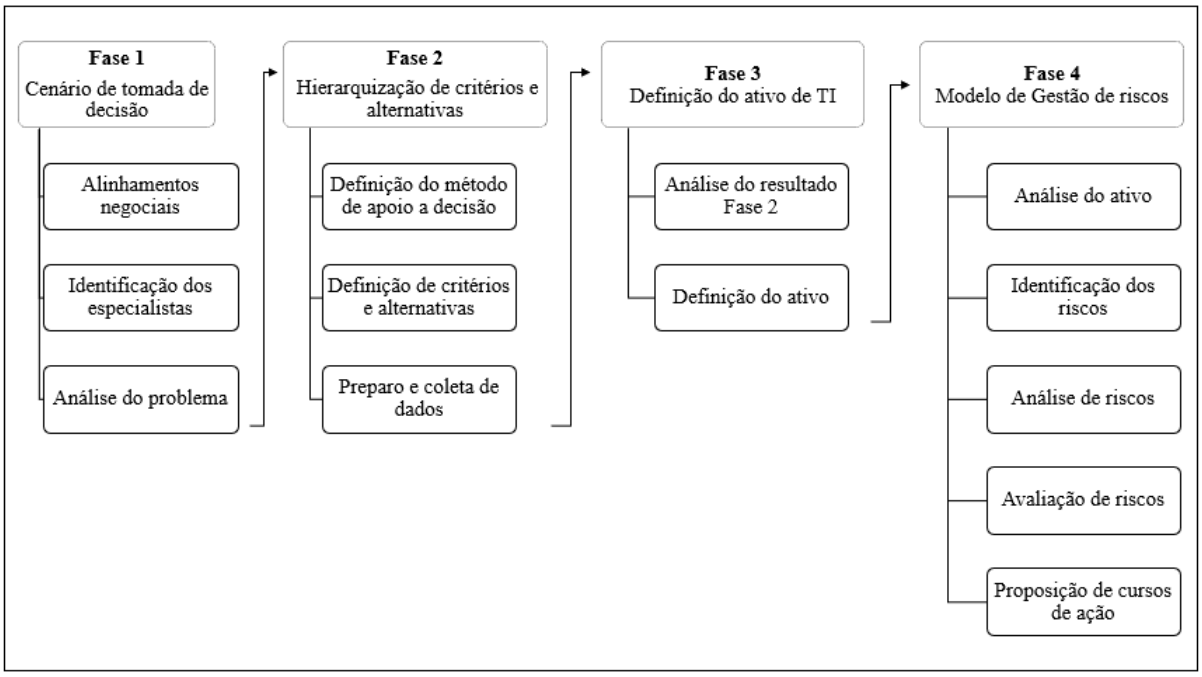
Metodologia da Pesquisa

3.1 Método da pesquisa

A pesquisa em curso é moderada por uma metodologia aplicada ao estudo de caso da PNID. É do tipo exploratória com abordagem qualitativa e em seu contexto possui o Consórcio Multi-Institucional. Para a coleta de dados utiliza um questionário online, a fim de obter a sensibilidade dos especialistas (vide Quadro 2 - Funções dos especialistas), o qual é uma adaptação de Saaty (1980) (135). Visto que a topologia da composição do grupo de especialistas/decisores que forma o CMI é multidisciplinar, dessa maneira, a literatura sugere uma abordagem de decisão em grupo. Os autores (136) abordaram a tomada de decisão em grupo (GDM) com comparações pareadas no Processo de Hierarquia Analítica - AHP, para chegar a uma solução significativa e confiável ao considerar a consistência individual e o consenso do grupo no processo de decisão. Por isso, o método de análise baseia-se na aplicação do MCDA na composição da Plataforma Nacional de Integração de Dados.

A Plataforma possui como principal negócio a integração de dados e informações de diversas instituições, assim, caracterizando-a como um sistema CRIS. Outro fator preponderante, o qual envolve o estudo de caso, refere-se ao Consórcio Multi-Institucional, responsável pelo desenvolvimento da PNID, que é resultante de um CPP. Ele envolve entidades públicas, privadas e uma organização social sem fins lucrativos. Nesse âmbito, a metodologia proposta busca absorver as diversidades culturais, políticas, financeiras e tecnológicas existentes entre os tomadores de decisão que representam a iniciativa do consórcio. À vista disso, a Metodologia proposta é composta por quatro fases, conforme a Figura 3.1, que apresenta a Metodologia em formato de Estrutura Analítica, a qual é composta por quatro fases com as respectivas atividades.

Figura 3.1: Metodologia proposta, visão geral.



Fonte: Belton e Stewart (2002) (137) (adaptado).

Posto isso, seguida uma breve descrição de cada fase.

• **Fase 1**: cenário de tomada de decisão. Essa fase busca identificar o cenário que envolve os tomadores de decisão no contexto do Ecossistema do Consórcio Multi-Institucional.

• **Fase 2**: determinar a hierarquização das alternativas. Responsável por determinar a hierarquização dos critérios e alternativas relacionadas às ações de Governança de TI do CMI.

• **Fase 3**: definição do ativo de TI. Responsável pela indicação do principal ativo de TI identificado a partir validação da categorização das alternativas resultado da Fase 2. Ressalta-se que para a definição do ativo o cenário (político, econômico, legal, contratual, internacional, entre outros) será considerado na tomada de decisão por parte dos *Stakeholders*.

• **Fase 4**: modelo de GR. O Modelo será uma customização aderente às necessidades identificadas junto das partes interessadas com o objetivo de prover a GR para o principal ativo de TI identificado. Em suma, as próximas etapas detalham as atividades por cada fase da metodologia.

3.2 Detalhamento das fases

Com o fim de evidenciar as informações, as quais compõem a pesquisa, a seguir serão detalhadas as atividades que integram as quatro fases.

3.2.1 Fase 1

A primeira fase é composta pelas tarefas: alinhamentos negociais (a), identificação dos especialistas (b) e análise do problema (c).

Alinhamentos negociais (a):

De acordo com Gartner, até 2022, 50% das organizações terão maior colaboração entre suas equipes de negócios e de TI, logo, as unidades de negócios e times de TI não podem mais funcionar em silos, pois equipes distantes podem causar o caos (138). Em vista disso, a tarefa (a) busca entender as necessidades e expectativas negociais dos patrocinadores e *Stakeholders* relacionadas a TI e as áreas negocias do consórcio. Esse entendimento será alcançado a partir da realização de entrevista semiestruturadas, cujos principais objetivos envolvem: entender o propósito e principais metas do CMI, identificar a cadeia de valor, principais processos e entender como a TI pode dar suporte e agregar valor ao negócio, dentre outros.

Identificação dos especialistas (b):

Segundo Fleury (2002) (139), competência é saber agir de maneira responsável e reconhecida, que implica em mobilizar, integrar, transferir conhecimentos, recursos, habilidades que agreguem valor econômico à organização e valor social ao indivíduo. Portanto, a tarefa de identificar os especialistas encarregou-se em determinar dentre os vários componentes técnicos do consórcio, a partir da realização de entrevista semiestruturada, aqueles detentores de conhecimentos diferenciados (técnicos, legais, culturais, estratégicos, gerenciais, políticas públicas, orçamentários, entre outras) os quais agregam valor ao projeto. A entrevista foi realizada durante a 1º reunião do Grupo de Trabalho de Estratégia, que contou com a participação de 24 membros, os quais fazem parte do consórcio Multi-Institucional.

O Quadro 2 consolida as funções dos entrevistados, que compreende a designação do cargo dos especialistas identificados e sugeridos pelo CMI. Esses especialistas são os responsáveis pela definição dos critérios e alternativas de decisão relacionados às ações de Governança de TI do CMI, além da condução e apoio na realização das demais fases e atividades necessárias para consolidação da PNID. Os critérios com as respectivas alter-

nativas são identificados pelos especialistas durante a execução da tarefa: definição de critérios e alternativas (e) - Fase 2.

Quadro 2: Funções dos especialistas.

Funções dos especialistas
Coordenação de Projetos
Coordenação de Projetos da Tecnologia da Informação
Coordenação-Geral de Tecnologia da Informação
Coordenadores de Divisão
Gerente de Projetos
Arquitetos de soluções
Diretor de Programa
Doutor em Engenharia de Produção
Gerente de Soluções
Coordenação Geral de Avaliação
Especialista em Sistemas

Fonte: Autoria própria.

A partir deste quadro, é possível visualizar a diversidade de perfis e funções, as quais compõem o corpo técnico de especialistas do Consórcio Multi-Institucional.

Análise do problema (c):

A análise do problema busca entender os fatores motivacionais (político, cultural, orçamentário, legal, internacional), os quais envolvem a priorização de atividades de Governança de TI, uma vez que para construção da PNID existem limitações orçamentárias e de recursos humanos. De forma assegurada, para alcançar o objetivo da tarefa (c) os especialistas, decerto, devem ser imparciais, pois percebe-se que, na área da educação, existe uma notória intervenção da esfera pública, por intermédio do financiamento estatal convergente com políticas públicas, ao referir-se às suas relações com colaboradores privados (70). Outro ponto de atenção a ser considerado durante a análise é o falso pensamento de subordinação do ente público em relação ao privado, pois ambos financiam a Plataforma Nacional de Integração de Dados (70) a partir de um Consórcio Público-Privado.

3.2.2 Fase 2

A Fase 2 é composta pelas atividades: definição do método de apoio a decisão (d), definição de critérios e alternativas (e) e preparo e coleta de dados (f).

Definição do método de apoio a decisão (d):

Com o cenário difuso apresentado na Análise do problema, tarefa (c), uma tomada de decisão quanto a priorização das ações de Governança de TI, torna-se conflitante e

difícil de ser realizada, pois cada decisor pode priorizar a ação que melhor se adeque a sua realidade e proporcione uma vantagem individual para sua organização. Inopinadamente, essa foi a percepção a partir das práticas e dinâmicas realizadas em grupo com os 11 exímios conhecedores do negócio, os quais são apresentados na Tabela 2. Acrescente-se que, conforme definição do PMBOK (22), Capítulo 10 - Gerenciamento das Comunicações do Projeto, a quantidade de canais de comunicação é calculada pela fórmula: n(n-1)/2, em que n é igual a quantidade de canais de comunicação. Assim, para um universo de 11 especialistas, existem 55 canais de comunicação, os quais representam a dificuldade de decidir nas circunstâncias em que o problema foi exposto.

Por isso, a tomada de decisão a qual envolve múltiplas partes interessadas pode ser melhor conduzida se aplicada em conjunto uma técnica de apoio a decisão. No caso da pesquisa em curso a Análise de Decisão Multi-Critérios - MCDA foi o método adotado, apesar de ser um termo genérico para uma coleção de abordagens sistemáticas desenvolvidas especificamente com o intuito de apoiar a avaliação de alternativas em termos de objetivos múltiplos e frequentemente conflitantes (137), foi o método adotado. O MCDA é composto por vários métodos, dentre eles: *Analytic Hierarchy Process* (Processo de Hierarquia Analítica - AHP); *Elimination and Choice Expressing Reality* (Eliminação e Escolha Expressando a Realidade - ELECTRE) ; *Preference Ranking Organisation Method for Enrichment Evaluation* (Método de Organização de Classificação de Preferência para Avaliação de Enriquecimento - PROMETHEE); *Technique for Order Preference by Similarity to Ideal Solution* (Técnica para Preferência de Pedido por Semelhança com a Solução Ideal - TOPSIS), entre outros (74). Para esse trabalho de pesquisa, dentre os vários métodos da família MCDA, foi escolhido o AHP pela racionalidade compensatória do problema de decisão. O método realiza um procedimento de comparação de pares baseado em escala linguística, a fim de comparar o grau de importância dos critérios e a conformidade de alternativas em relação aos critérios (135). O Processo de Hierarquia Analítica é um método para apoio a decisão no contexto MCDM. O método apoia a estruturação, medição e síntese e tem sido aplicado a situações-problema, por exemplo: seleção entre alternativas concorrentes em um ambiente multiobjetivo, alocação de recursos escassos e previsão (140). Essas características do AHP são congruentes às necessidade identificadas no ecossistema do CMI: ambiente com vários tomadores de decisão, atores e interlocutores distintos e recursos financeiros e humanos insuficientes para realização de ações. Com isso, a priorização de atividades são fundamentais para sustentabilidade do Consórcio e o método AHP, 28.201 citações na *Scopus* em pesquisa realizada sem filtros adicionais no dia 15/03/2022, demonstra ser o método adequado para aplicação no cenário do CMI.

Definição de critérios e alternativas (e):

O Consórcio utiliza a norma ISO/IEC 38500 (2015) (62) como guia de Governança de TI, pois essa norma tem como finalidade a promoção eficaz da Tecnologia da Informação nas organizações. A norma possui seis princípios para uma boa governança de TI, os quais são: Responsabilidade, Estratégia, Aquisição, Desempenho, Conformidade e Comportamento Humano. Após a realização de duas reuniões, os especialistas convergiram em cinco (5) critérios ao utilizar a norma (62) como base, são eles: Responsabilidade, Estratégia, Desempenho, Conformidade e Comportamento Humano. O princípio da Aquisição não foi considerado um critério válido no contexto do CMI, pois o consórcio não realizará a aquisição de ativos de TI. É importante destacar que os critérios são elementos fundamentais para o processo decisório, os quais avaliam o desempenho das alternativas. Decorrente dos critérios, as alternativas de decisão são compostas por Papéis e Responsabilidades, Sustentabilidade, Processos, Legislação e Plano de Comunicação, as quais formam o conjunto viável de opções para tomada de decisão com o objetivo final de priorizar os ativos críticos de TI.

Preparo e coleta de dados (f):

A atividade (f) é composta pelas tarefas de preparo e coleta de dados relativos à avaliação dos especialistas acerca dos critérios e alternativas, os quais serão utilizados para realizar a avaliação pareada de comparação entre os critérios e alternativas (135). A preparação encarrega-se da modelagem e aplicação do questionário e envolve prover os meios físicos, *hardware*, periféricos e *software*. O questionário é a ferramenta utilizada para coleta da sensibilidade dos especialistas em relação a magnitude de cada critério e alternativa. A tarefa de preparo propõe-se a definir os pesos, conforme Quadro 3, a serem utilizados na relação entre os critérios (C1 e C2, C1 e C3...Cn e Cn) e alternativas (A1 e A2, A1 e A3...An e An) ao aplicar à avaliação pareada de comparação entre os critérios e alternativas, adaptada de Saaty (1980) (135).

Quadro 3: Escala de preferência relativa baseada em Saaty (1980).

Intensidade da preferência (Valor Numérico)	**Definição (Escala Verbal)**	**Observações**
1	Igualdade de preferência	Elementos que contribuem igualmente para um mesmo objetivo.
2	1º Valor intermediário	Elemento intermediário entre a intensidade de preferência 1 e 3.
3	Fraca preferência de um dos elementos	Um elemento é levemente mais importante que o outro.
4	2º Valor intermediário	Elemento intermediário entre a intensidade de preferência 3 e 5.
5	Forte preferência de um dos elementos	Um elemento é fortemente mais importante que o outro.
6	3º Valor Intermediário	Elemento intermediário entre a intensidade de preferência 5 e 7.
7	Muito forte preferência de um dos elementos	Um elemento é muito mais importante que o outro.
8	4º Valor intermediário	Elemento intermediário entre a intensidade de preferência 7 e 9.
9	Preferência absoluta de um dos elementos	Um elemento é extremamente mais importante.
Valores recíprocos (não negativos)	Elemento i que obtiver um dos valores apresentados acima quando comparado com o elemento j, então j possuirá o valor recíproco quando comparado com i	

Fonte: Saaty (1980) (135) e Abdullah e Najib (2014) (141) (adaptado).

O principal parâmetro utilizado para se chegar aos pesos dos critérios é a escala fundamental desenvolvida por Saaty (135), que consiste de uma série de valores, a contar de "igual importância" a "extrema importância", conforme Quadro 3. A coleta, por sua vez,

encarrega-se de armazenar e gerar o resultado final da aplicação dos questionários, além de realizar a aplicação do método MCDA.

O instrumento de coleta de dados foi desenvolvido para avaliação da comparação para a par entre os critérios e posteriormente entre as alternativas de ação. E foi respondida pelos especialistas elencados na tarefa de identificação dos especialistas (b), definida na fase 2. O questionário foi estruturado em 10 perguntas para os critérios e em 50, aplicadas posteriormente, para as alternativas.

3.2.3 Fase 3

A terceira fase compreende as atividades de análise do resultado (Fase 2) (g) e definição do ativo (h).

Análise do resultado (g):

A etapa de análise do resultado (g) assimila o entendimento das conclusões relativas à compilação dos questionários aplicados para ordenação dos critérios/alternativas. Visa, também, a identificação da existência de imprecisões e ambiguidades, possivelmente causados pela confiança na experiência ou intuição, no resultado dessas ordenações. Salvo se essas eventualidades citadas anteriormente forem identificadas será pesquisada uma técnica complementar ao AHP, a fim de corrigir a potencial imprecisão dos resultados.

Para consideração final, quanto ao desenvolvimento das alternativas de decisão, serão avaliados os cenários políticos, culturais, orçamentários, legal, internacional, riscos que inviabilizam o negócio, dentre outros. Portanto, a orientação para realização da alternativa, a qual será desenvolvida, ocorrerá a partir da tomada de decisão dos principais interlocutores do CMI ao considerarem o resultado final da aplicação do método e análise de cenários. É importante ressaltar que os resultados apresentados pela aplicação do método AHP constituem uma recomendação que pode ser ratificada pelos tomadores de decisão do Consórcio Multi-Institucional.

Definição do ativo de TI (h):

Priorizadas as alternativas pelos tomadores de decisão do CMI, resultado da análise do resultado (g), o principal ativo de TI que compõem a PNID será identificado na tarefa (h). A identificação desse ativo, sob o prisma do CMI, deverá levar em consideração o ambiente da Plataforma Nacional de Integração de Dados, porque envolve uma análise relativa aos riscos técnicos, legais, culturais, estratégicos, gerenciais, políticas públicas, orçamentários, entre outras, alinhados ao Ecossistema de Educação, Ciência, Tecnologia e Inovação, além das normas ISO 27002 (2013) (142) e ISO 55000 (2014) (143).

A norma ISO/IEC 27002 (2013) (142) define que ativos são objeto de ameaças, tanto acidentais como deliberadas, enquanto que os processos, sistemas, redes e pessoas têm vulnerabilidades inerentes. Os ativos são qualquer coisa que tenha valor para a organização (142) e podem variar em ativos de informação, *software*, físicos, serviços, pessoas e intangíveis.

A norma NBR ISO 55000 (143) define ativo como um item, algo ou entidade que tem valor real ou potencial para uma organização. Este valor pode ser tangível ou intangível, financeiro ou não financeiro, e inclui a consideração de riscos e passivos; pode ser positivo ou negativo, em diferentes estágios da vida do ativo. Conforme Crespo Márquez et al. (2017) (144) os fatores-chave que influenciam uma organização a atingir seus objetivos, quanto a definição de ativos de TI, são: a natureza e propósito da organização, seu contexto operacional, suas restrições financeiras e requisitos regulatórios e as necessidades e expectativas da organização e das partes interessadas. A partir da definição do ativo, tarefa (h), a próxima etapa será desenvolver o Modelo de Gestão de riscos voltado para esse ativo de TI.

3.2.4 Fase 4

A quarta fase, Modelo de Gestão de riscos, é composta pelas atividades: análise do ativo (i), identificação dos riscos (j), análise de riscos (k), avaliação de riscos (l) e tratamento de riscos (m). Para realização dessa fase, a Norma ISO 31000 (2018) (94) foi adequada ao quadro que envolve o ativo de TI (i). A Figura 3.2 apresenta o Processo de Gestão de Riscos contemplado pela Norma.

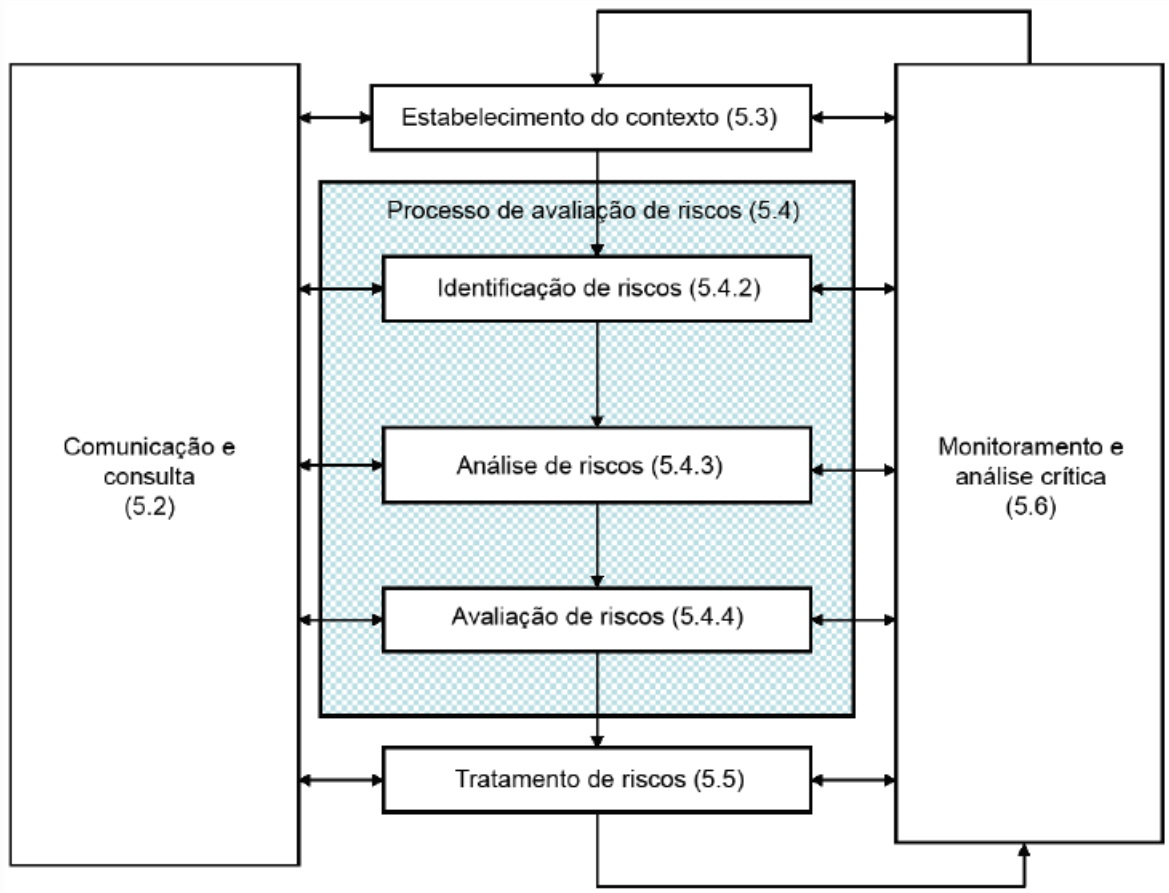
No contexto interno, proposto nesta pesquisa, foi considerada a construção de um Modelo de Gestão de Riscos, metodologia, que atenda ao momento e necessidades da PNID.

Análise do ativo (i):

O CMI é o idealizador e o responsável pelo desenvolvimento da plataforma, que terá os riscos identificados, analisados, validados, tratados, monitorados e comunicados para o ativo de TI identificado na tarefa (i), de acordo com a Norma ISO 31000 (2018) (94). O Processo de Avaliação de Riscos será apoiado pela Norma ISO 31010 (2012) (95), norma de apoio à ABNT NBR ISO 31000 (2018) (94), da qual fornece orientações sobre a seleção e aplicação de técnicas sistemáticas para o processo de avaliação de riscos (95). Além das considerações da norma ISO 31000 (2018) (94), serão realizadas pesquisas, a fim de identificar, a partir da literatura, os principais eventos que podem causar impacto negativo ao negócio, caso o ativo esteja vulnerável.

Identificação dos riscos (j):

Figura 3.2: Interconectividade entre os membros.



Fonte: ISO 31000 (2018) (94) (adaptado).

A tarefa de identificação dos riscos (j) será realizada a partir da concretização de entrevistas semi-estruturadas, as quais devem utilizar técnicas de elicitação de riscos apoiadas na norma ISO 31010 (2012) (95), além de métodos baseados em evidências elencadas na literatura.

Análise de riscos (k):

A Análise de riscos (k) diz respeito ao entendimento do risco e consiste em determinar a probabilidade vs. impacto para ocorrência de eventos de riscos identificados para o ativo de TI determinado na tarefa (h). Para essa atividade, será realizada a análise qualitativa dos riscos.

Avaliação de riscos (l):

A avaliação de riscos (l) consiste na classificação dos riscos quanto ao impacto se alto, médio ou baixo. Tal classificação depende da técnica utilizada para realizar o Processo de Avaliação de Riscos. A técnica utilizada será apoiada na Norma ISO 31010 (2012) (95).

Tratamento de riscos (m):

Por fim, o tratamento de riscos (m) viabilizará as respostas aos riscos mapeados na tarefa (I). Para finalizar o Modelo de GR, é proposto a construção de um modelo para responder aos riscos, que pode conter relatórios de comunicação, tratamento dos riscos, além de indicadores para monitoramento de incidência dos riscos. A próxima etapa consiste no desenvolvimento do estudo de caso.

Capítulo 4

Estudo de Caso

4.1 Fase 1 - Cenário de tomada de decisão

4.1.1 Alinhamentos negociais

Para o ITGI (2003) (145) e ISACA (2012) (146), o alinhamento estratégico negocial, o qual inclui a TI, refere-se aos procedimentos de governança de TI que devem resultar no alinhamento das atividades de TI com os objetivos estratégicos do negócio, nomeadamente por intermédio de sólidas propostas de valor de negócio de TI e excelência operacional de Tecnologia da Informação. Por essa razão, para alcançar o sucesso no negócio e ser sustentável, as empresas devem aumentar seu foco no alinhamento do negócio de forma estratégica com Tecnologia da Informação e governança TI (147). Não só com essas proposições em mente, mas ainda cientes da importância do alinhamento negocial para o sucesso da jornada de implementação da Plataforma Nacional de Integração de Dados, em agosto de 2019 foi oficialmente lançado o CMI. O evento recebeu os dirigentes das instituições, que formam o Consórcio Multi-Institucional de Ensino e Pesquisa e foram transcritas, conforme segue, as expectativas em torno da iniciativa:

CAPES(presidente) - "Há benefícios em tempo e divulgação das pesquisas. Para a sociedade em geral, o consórcio representa acesso a mais conhecimento, melhor transparência na prestação de contas e maior visibilidade internacional para o País" (148).

IBICT(diretor) - "A expectativa é de que tenhamos um sistema de informação de financiamento de pesquisa que integre dados das agências de fomento" (148).

CNPq(presidente) - "O consórcio é uma excelente oportunidade para uma atuação mais inteligente das agências de fomento brasileiras, com mais racionalidade e economicidade" (148).

CONFAP(presidente) - "Esperamos que a integração de conteúdo das instituições que participam do consócio promova uma racionalização de recursos e esforços, dando

mais agilidade e qualidade aos processos de seleção e avaliação das políticas de fomento" (148).

SciELO(diretor) - "Contribuirá para o melhoramento das capacidades e infraestruturas em gestão de informação e comunicação científica que se traduzirá em maior reconhecimento e visibilidade da pesquisa do Brasil" (148).

RNP(diretor) - "A maior transparência das informações é outro resultado que poderá trazer grande impacto na forma como se faz gestão do sistema de ciência, tecnologia e inovação, não apenas por demonstrar onde o recurso está sendo aplicado, mas também pelos benefícios que trará para a comunidade científica, uma vez que tornará mais claro o que está sendo desenvolvido por outros pesquisadores e qual a estrutura disponível para realização das pesquisas" (148).

Em vista, as considerações dos dirigentes reforçam a meta do CMI em oferecer oportunidades de ganhos significativos de eficiência e economia de esforços à comunidade científica. Com isso, também, viabiliza que as instituições disponham de informações abrangentes, das quais possibilitem uma melhor gestão de suas atividades, além de recursos de ensino e pesquisa. Visa, idem, permitir o compartilhamento de boas práticas e estratégias. Com o fim de promover informações abrangentes à comunidade científica, a TI desempenha um papel fundamental no suporte ao consórcio, concebido a partir do fornecimento de serviços propiciados pela PNID, tais como:

- **Análise da Qualidade de Dados e Fontes**: análise de dados indicará as fontes mais adequadas dos dados de cada entidade de informação.
- **Vocabulários abertos e comuns**: todos os dados trocados entre membros usarão um vocabulário aberto e publicados na *Web*.
- **Mapa entre IDs e classificações**: correspondência entre os diferentes identificadores e classificações adotados por membros para uma mesma entidade.
- **Controle de Acesso**: os membros decidirão acerca do público e controle de acesso correspondente de cada dado.
- **Biblioteca de Código Aberto**: as funções de consulta e recuperação de dados da PNID terão seu código aberto e residirão numa biblioteca para reaproveitamento pelos membros.
- **Hospedagens e diretórios**: hospedagem de arquivos e BD compartilhados para troca de dados recorrentes entre serviços e membros.
- **Desambiguação de nomes e títulos**: algoritmos de desambiguação de nomes para se determinar a relação correta entre entidades.
- **Apoio à Governança e Sustentabilidade**: gerenciamento de programas e projetos de implementação, assessorial e consultorias diversas, apoio administrativo.

Os serviços fornecidos pela plataforma ocasionam agregação de valor ao negócio dos consorciados fundados na promoção das seguintes ações:

• **Economia de esforço de tempo**: os pesquisadores não precisarão preencher dados repetidos em sistemas variados, pois os dados serão automaticamente atualizados nos sistemas integrados.

• **Qualificação dos dados**: ao realizar a desambiguação, padronização, validação e certificação dos dados, eles se tornam mais precisos, seguros e confiáveis.

• **Monitoramento de resultados**: Transparência na Prestação de Contas evidenciando os resultados obtidos a partir de pesquisas financiadas com recursos públicos.

• **Disseminação da informação**: gerar mais oportunidades por meio do fácil acesso às informações dos pesquisadores e de suas pesquisas, promovendo a construção colaborativa, compartilhamento de infraestrutura e a internacionalização.

Por fim, a coexistência da iniciativa é alicerçada com suporte do alinhamento e entendimento dos objetivos, comuns, os quais envolvem as principais instituições de fomento à pesquisa científica no Brasil. É fundamental citar que o sucesso do consórcio e evolução da plataforma estão relacionados a participação de especialistas negociais e técnicos, os quais foram indicados pelas instituições formadoras do CMI.

4.1.2 Identificação dos especialistas

A identificação dos especialistas foi baseada nas habilidades técnicas, visão holística e experiências relacionadas ao negócio de cada instituição, uma vez que a PNID se propõe a ser um grande concentrador de informações, centralizando e compartilhando dados entre as várias aplicações, as quais compõem o Ecossistema do ConectiBR. Assim, os especialistas necessariamente devem conhecer as nuances, que envolvem os sistemas que integram esse bojo de informações. Em agosto de 2020 foi realizada a 1º reunião do Grupo de Trabalho de Estratégia e os especialistas foram definidos durante o encontro. O Quadro 4 relaciona os especialistas, enumerados de 1 até 11, com os respectivos conhecimentos, em termos negociais ou técnicos, para compor o grupo de especialistas.

Quadro 4: Especialistas e conhecimento.

Especialistas	Conhecimentos
Especialista 1	Conhecimento negocial e tecnológico que envolve o Portal brasileiro de publicações científicas em acesso aberto - mecanismo de busca multidisciplinar que permite o acesso gratuito à produção científica de autores vinculados a universidades e a institutos de pesquisa brasileiros. Por meio da ferramenta é possível também realizar buscas em fontes de informação portuguesas (149).
Especialista 2	Conhecimento negocial e tecnológico o qual envolve a Plataforma Sucupira, que fornece para toda a comunidade acadêmica, em tempo real e com transparência, as informações, processos e procedimentos que a Capes realiza no SNPG. Igualmente, a ferramenta propiciará a parte gerencial-operacional de todos os processos e permitirá maior participação das pró-reitorias e coordenadores de programas de pós-graduação (150).
Especialista 3	Conhecimento negocial e tecnológico que envolve A Plataforma Lattes representante da integração de bases de dados de currículos, de grupos de pesquisa e de instituições em um único sistema de informações (151).
Especialista 4	Conhecimento negocial relacionado ao Programa Confap-CRIS. A aplicação objetiva, promover avanços em parcerias, apoiar as ações de internacionalização das bases de dados científicos e ampliar a visibilidade das iniciativas estaduais de Ciência, Tecnologia e Inovação promovidas pelas Fundações Estaduais de Amparo à Pesquisa - FAPs (152).
Especialista 5	Conhecimento negocial o qual envolve a SciELO, cujo objetivo é a promoção do acesso internacional às revistas científicas latino-americanas em Ciências Sociais. Sua principal característica é disponibilizar gratuitamente ao público textos completos em inglês, a fim de aumentar a visibilidade e acessibilidade das Ciências Sociais da América Latina (153).
Especialista 6	Especialista em Sistemas Semânticos (*web* semântica).
Especialista 7	Conhecimentos negociais e tecnológicos, os quais envolvem projetos de inovação como a integração com o ORCID, desambiguação de dados, semântica, experiência do usuário e interoperabilidade de sistemas.
Especialista 8	Conhecimentos relacionados ao gerenciamento de projetos de desenvolvimento e implementação de serviços e soluções para parceiros governamentais.
Especialista 9	Conhecimentos técnicos relacionados a diversas tecnologias, linguagens de programação, SGBD, soluções arquiteturais distribuídas, dentre outros.
Especialista 10	Especialista em gestão de projetos ágeis, padrões de projetos, melhores práticas de serviços, governança corporativa de TI, segurança da informação, métricas de *software*, dentre outros.
Especialista 11	Conhecimentos relacionados a planejamento, coordenação, controles, gestão de TIC, normas e padrões técnicos para pesquisar, entre outros.

Fonte: Autoria própria.

Levando em conta o Quadro 4 é razoável ratificar que o grupo, os especialistas, é multidisciplinar com conhecimentos técnicos e negociais nas respectivas ferramentas CRIS, as quais agregam informações de pesquisa, repositórios institucionais, repositórios de dados e bibliotecas digitais. À face do exposto, os especialistas possuem as credenciais necessárias para apoiar a definição do problema da pesquisa.

4.1.3 Análise do problema

O alinhamento entre a TI e negócios é consistentemente classificado como o principal dos problemas para os CIOs de todos os tipos e tamanhos de empresas (154), quando o foco é desenvolver políticas de atuação. De maneira idêntica, a capacidade de detectar problemas e emergências, identificar riscos e reduzir incertezas sobre os possíveis impactos das políticas estão entre os principais desafios do processo de formulação de políticas (155). Com a intenção de realizar uma política de impacto robusta e relevante que implemente o princípio do desenvolvimento sustentável, é necessário determinar as implicações sociais, econômicas, ambientais, jurídicas e organizacionais de uma nova política (156). Além disso, existem certos aspectos-chave dos quais devem estar presentes para definir o escopo da análise da política, incluindo (157):

- Objetivo (s) da análise de política.
- Área geográfica: global, regional, nacional, subnacional e local.
- Aspecto temporal (curto, médio e longo prazo).
- Setores das atividades governamentais relacionadas.
- Participação dos atores.

Dessa forma, a partir do entendimento das necessidades, as quais envolvem aspectos, por exemplo, políticos, culturais, orçamentários, legais, internacionais, foi realizada pelos especialistas a análise do problema que envolve a Plataforma Nacional de Integração de Dados. Desse modo, o problema identificado no contexto do CMI envolve priorizar ações de Governança de TI para suportar a construção da PNID, pois existem limitações orçamentárias, de recursos humanos, de sensibilidade de dados pessoais (autores, pesquisadores e professores) e institucionais. Dessarte, com a ação de GTI priorizada, a partir da hierarquização de critérios e alternativas, é possível identificar o Ativo crítico de TI e apresentar um modelo de Gestão de Riscos de Tecnologia da Informação.

4.2 Fase 2 - Hierarquização de critérios e alternativas

4.2.1 Definição do método de apoio a decisão

A definição do método de apoio à decisão, de acordo com o cenário difuso apresentado na análise do problema, é guiada pela dificuldade em priorizar ações de Governança de TI no ambiente do CMI. Dentre os vários métodos os quais compõem à abordagem MCDA o AHP (135) da Escola America (158), cuja aplicação é apropriada a problemas decisórios de problemáticas de ordenação, nos quais a racionalidade é compensatória o que vai ao encontro do contexto do CMI.

O método AHP é amplamente utilizado com a finalidade de apoiar a seleção e ordenação de critérios e alternativas, como pode ser observado em (159), (160), (161), (162), (163), (164), (165) e (166). Quanto aos critérios e alternativas, que compõem o problema de priorização de ações de Governança de TI, eles são determinados com base na ABNT NBR ISO/IEC 38.500 (2015) (62).

4.2.2 Definição de critérios e alternativas

O Consórcio Multi-institucional emprega a ABNT NBR ISO/IEC 38.500 (2015) (62) como padrão de Governança de TI para o CMI. A norma utiliza a nomenclatura de princípios para definir a boa governança corporativa de TI, ao passo que o consórcio denomina os princípios de critérios. O Quadro 5 apresenta a relação entre os princípios definidos pela ISO/IEC 38.500 (2015) (62) e os critérios extraídos da norma ISO sob a óptica dos especialistas.

Quadro 5: Critérios e alternativas (adaptado).

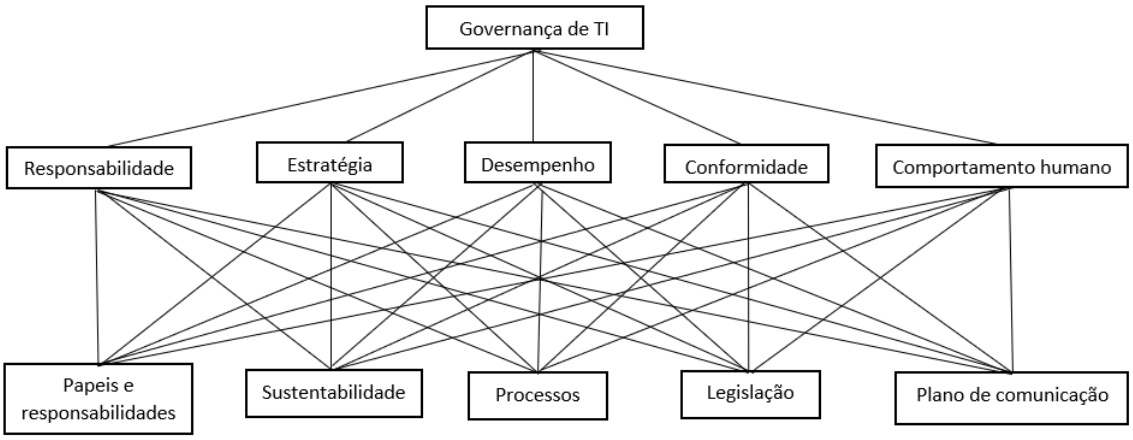
Princípios	**Descrição**	**Critério**	**Descrição**
Responsabilidade	Os indivíduos e grupos dentro da organização compreendem e aceitam suas responsabilidades com respeito ao fornecimento e demanda de TI. Aqueles responsáveis pelas ações também têm autoridade para desempenharem tais ações.	C1-Responsabilidade	Atribui obrigações aos indivíduos e grupos dentro do consórcio. Para esse critério, é importante que indivíduos possuam os conhecimentos e habilidades adequadas, a fim de gerarem melhores resultados em relação às atividades, pelas quais são responsáveis.
Estratégia	A estratégia de negócios da organização leva em conta as capacidades atuais e futuras de TI, e os planos estratégicos para TI satisfazem as necessidades atuais e contínuas da estratégia de negócio da organização.	C2-Estratégia	Relaciona-se ao alinhamento negocial da organização e leva em conta as capacidades atuais e futuras de tecnologia da informação, considera, também, que os planos estratégicos para TI satisfazem as necessidades atuais e contínuas da estratégia de negócio do CMI. Para esse critério, o fator preponderante situa-se na visão holística entre a TI e as áreas de negócio de cada membro do consórcio, pois, dessa forma, é possível abranger os diferentes aspectos organizacionais, políticos, legais, culturais, modelos de negócio e formas de cooperação.
Desempenho	A TI é adequada ao propósito de apoiar a organização, fornecendo serviços, com níveis e qualidade, necessários para atender aos requisitos atuais e futuros do negócio.	C3-Desempenho	Correlaciona-se à capacidade da TI em apoiar a organização ao fornecer serviços que suportem o negócio, além de fornecer transparência no alcance dos objetivos estratégicos.
Conformidade	A TI cumpre com toda a legislação e regulamentos obrigatórios. As políticas e práticas são claramente definidas, implementadas e fiscalizadas.	C4- Conformidade	Versa sobre o cumprimento obrigatório das leis e regulamentos aplicáveis, além das políticas e práticas que devem ser claramente definidas, implementadas e auditadas, interna ou externamente aos membros do consórcio.
Comp. Humano	As políticas, práticas e decisões de TI demonstram respeito pelo Comportamento Humano, incluindo as necessidades atuais e futuras de todas as "pessoas" no processo.	C5- Comp. Humano	Valoriza o respeito pelo comportamento humano em relação as políticas, práticas e decisões de TI. Possibilita a aplicação das habilidades e o exercício dos papéis corretos para gerar melhores resultados, aumentar a sinergia e uso eficiente dos talentos, os quais fomentam um relacionamento produtivo com os stakeholders da associação.

Fonte: Autoria própria.

A relação de hierarquização entre critérios e alternativas pode ser observada na Figura 4.1.

Sendo assim, ao determinar a hierarquização das alternativas, com base no cálculo dos pesos dos critérios e das alternativas, será possível identificar o Ativo de TI relacionado

Figura 4.1: Hierarquização entre critérios e alternativas.



Fonte: Autoria própria.

diretamente às ações de Governança de TI do CMI. A hierarquização será conhecida com a aplicação do método AHP.

4.2.3 Preparo, coleta de dados e aplicação do método AHP

Preparo

A preparação encarregou-se da modelagem e aplicação do questionário,em que utilizou o Formulários do Google como ferramenta de coleta de sensibilidade dos especialistas quanto aos critérios e alternativas (166). Conforme indicado nesta pesquisa, os pesos, de acordo com o Quadro 3, são uma adaptação de Saaty (1980) (135) para aplicação da avaliação pareada de comparação entre critérios e alternativas. Ao todo, a pesquisa realizou a coleta da percepção inerente a 60 perguntas, das quais 10 para os critérios e 50 para as alternativas.

Coleta

A coleta encarregou-se de armazenar e gerar o resultado final da aplicação dos questionários aplicados para os critérios e alternativas, que representa uma amostra da coleta das respostas relativas aos critérios.

Aplicação do método AHP

O método AHP aplicado é uma adaptação de (135), (167), (168) e (169), no qual as fases de construção, análise de prioridades e verificação de consistência são distribuídas das atividades 1 até 6.

Atividade 1 - avaliação e organização dos critérios e das alternativas em matrizes para comparação par a par conforme julgamentos emitidos pelos especialistas (item 4.1.1).

As entradas são originadas dos dados julgados pelos especialistas (item 4.1.1).

Atividade 2 - realização da normalização das avaliações par a par e cálculo do vetor prioridade. Nesse caso o total, somatório, do vetor de cada critério deve ser igual a 1 (100%).

Atividade 3 - calcular o *Lambda* (168), Índice de Consistência (*Consistency Index* - CI) e a Razão de Consistência (*Consistency Ratio* - CR). O CR consiste na comparação entre os julgamentos realizados pelos avaliadores, indicados pelo índice de consistência CI e julgamentos aleatórios, calculados para matrizes de diferentes tamanhos, indicados por RI (*Random Index*) ou por índices aleatórios. O RI varia de acordo com o número de critérios avaliados (n), quando da avaliação dos critérios. Para as alternativas varia de acordo com o número de alternativas avaliadas.

O CR deve ser abaixo de 10%, de acordo com Saaty (135), o qual afirma que um conjunto de decisões pode ser considerado "consistente" se a Razão de Consistência permanecer abaixo de 0,1, ou 10%. Na visão do autor, taxas muito acima deste parâmetro aproximam-se demasiadamente de resultados aleatórios, e isso pode indicar que os julgamentos iniciais necessitam de revisões.

Formulas para aplicação do método AHP

Lambda $\lambda_{Máx}$

Para o cálculo de $\lambda_{Máx}$, é realizada a multiplicação da matriz de comparação pelo seu Vetor Limite. Para o cálculo de

$\lambda_{Máx}$, utiliza-se a fórmula:

$$\lambda_{Máx} = médiadovetorlimite. \tag{4.1}$$

Índice de consistência - CI

$$IC = \frac{\lambda_{Máx}\text{-}n}{n\text{-}1} \tag{4.2}$$

Em que n é o número de linhas e colunas, das quais compõem a dimensão da matriz de decisão.

Taxa de consistência - CR

$$CR = \frac{CI}{RI} \tag{4.3}$$

Atividade 4 – comparação par a par das alternativas a luz de cada critério. Esse procedimento é realizado da mesma forma que foi aplicado para os critérios, conforme atividades 1 e 2.

Atividade 5 - agregação das avaliações. Nessa atividade é realizada a agregação das avaliações das alternativas a luz de cada critério, considerando-se os pesos dos critérios para obtenção do ranque final, ou seja, da avaliação global de cada alternativa ao considerar todos os critérios.

Aplicação

A realização das atividades de 1 a 5 foram apoiadas pela ferramenta *Super Decision* (170), *software* educacional gratuito que implementa o AHP e que *Super Decision* foi desenvolvido pela equipe do idealizador do método, Thomas Saaty (1980) (135). A Figura 4.2 apresenta as classes, as quais representam a ação de Governança de TI, critérios e alternativas.

Figura 4.2: Hierarquização entre critérios e alternativas.

Fonte: *Super Decision* (170).

A Tabela 4.4 representa as entradas originadas dos dados julgados pelos especialistas de acordo com os pesos.

Tabela 4.1: Comparação par a par dos critérios.

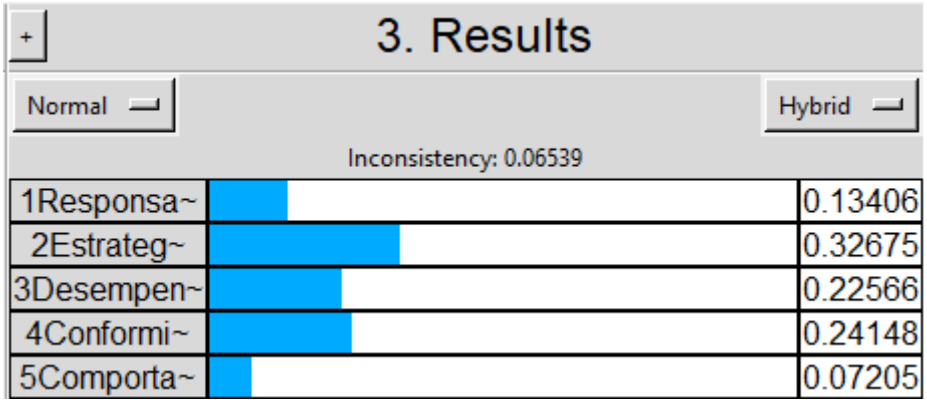
CRITÉRIOS	C1	C2	C3	C4	C4
C1	**1,000**	0,500	0,333	0,500	3,000
C2	2,000	**1,000**	3,000	1,000	3,000
C3	3,000	0,333	**1,000**	1,000	3,000
C4	2,000	1,000	1,000	**1,000**	3,000
C5	0,333	0,333	0,333	0,333	**1,000**

Fonte: Saaty (1980) (135) (adaptado).

Razão de consistência - CR

Ao aplicar os cálculos a *CR* identificada, de acordo com a Figura 4.3, obteve-se o valor de **0,06539**, o qual respeita os 10% para avaliação de consistência recomendados por Saaty (1980) (135).

Figura 4.3: Razão de consistência.



Fonte: Cálculo realizado com apoio da ferramenta *Super Decision* (170).

Resultado final da aplicação do AHP

A partir do resultado final da aplicação do AHP, as alternativas hierarquizadas seguem a seguinte ordenação:

1º Legislação com 28,875% de preferência.

2º Processos com 25,892% de preferência.

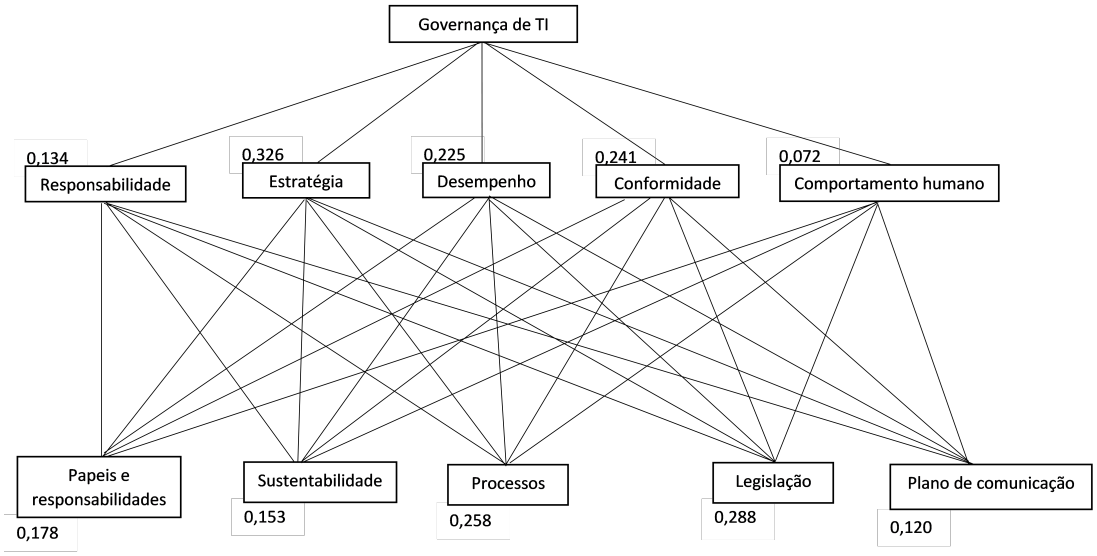
3º Papéis e responsabilidades com 17,841% de preferência.

4º Sustentabilidade com 15,367% de preferência.

5º Plano de comunicação com 12,025% de preferência.

A Figura 4.4 apresenta o resultado da aplicação do método AHP em formato hierárquico.

Figura 4.4: Resultado hierárquico de critérios e alternativas – AHP.



Fonte: Autoria própria e aplicação da ferramenta *Super Decision* (170).

Determinar a hierarquização das alternativas, a partir do cálculo dos pesos dos critérios e das alternativas, relacionadas às ações de Governança de TI do CMI, faz parte dos objetivos específicos da pesquisa. Dessa forma, o resultado alcançado viabiliza opções para tomada de decisão.

4.3 Fase 3 - Definição do ativo de TI

4.3.1 Análise do resultado Fase 2

Ao concluir a aplicação dos pesos, decorrência da análise AHP representada pela Figura 4.4, chegou-se a ordenação final das alternativas, as quais representam as ações inerentes à Governança de TI, critérios e respectivas alternativas no cenário do CMI. Esse é o segundo objetivo específico proposto para essa pesquisa e meta da Fase 2, que alicerçado na hierarquização, fruto da aplicação do método MCDA, foi possível notar que os critérios Estratégia (C2), Conformidade (C4) e Desempenho (C3) destacaram-se em relação aos demais. A ponderação dos critérios viabilizou alcançar os resultados para cada alternativa.

Como resultado, a Figura (4.4) nos revela que o percentual de preferência das alternativas ficou estabelecido na seguinte ordem decrescente: Legislação (28,875%), Processos (25,892%), Papéis e Responsabilidades (17,841%), Sustentabilidade (15,367%) e Plano de Comunicação (12,025%).

Com o término da hierarquização foi possível apresentar à alta gestão do Consórcio uma proposição de alternativas ranqueadas, das quais visam otimizar a execução dos recursos financeiros voltados para ações de Governança de TI.

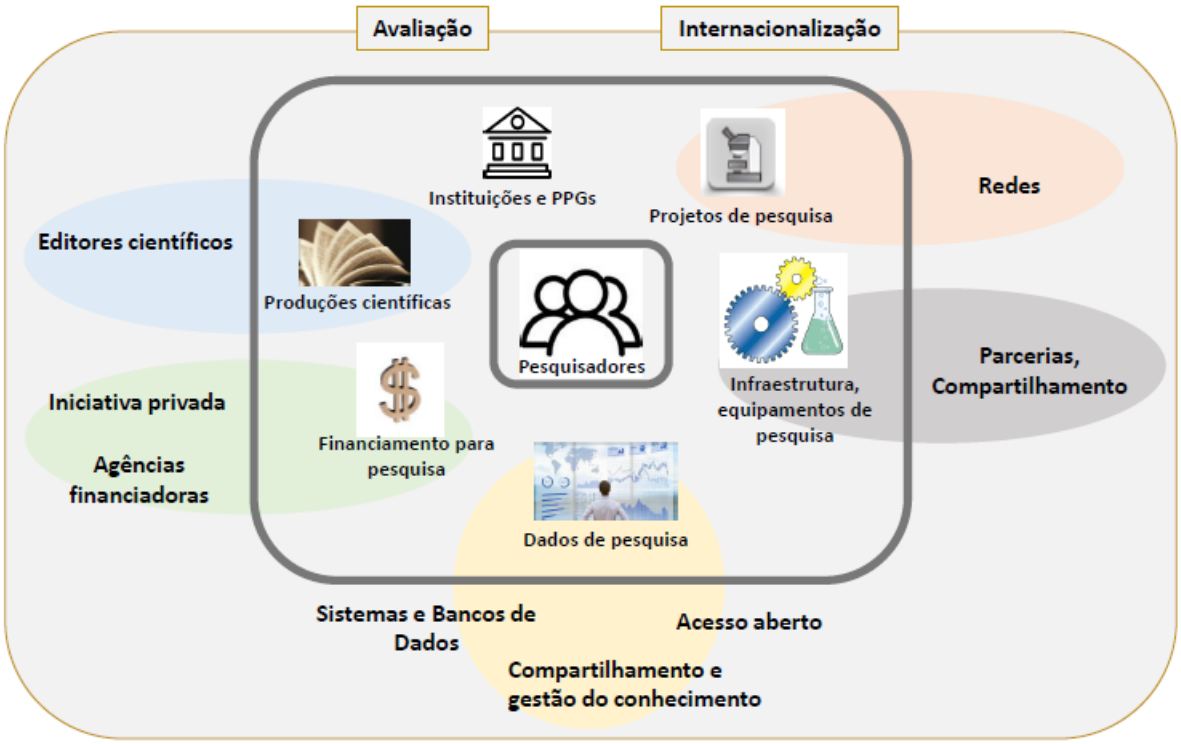
O resultado da aplicação do método AHP no Consórcio Multi-institucional forneceu subsídios concretos e sem vieses políticos, culturais ou organizacionais à tomada de decisão estratégica com foco na melhor alternativa. Dessa forma, os riscos de uma tomada de decisão baseada apenas em empirismo foram mitigados. O propósito alcançado possibilitou aos tomadores de decisão avaliarem, dentre as alternativas pontuadas, em conjunto a um cenário com marcos regulatórios, os quais visam a privacidade de dados pessoais ou corporativos, o que ofereça maior sustentabilidade ao CMI. Portanto, o consórcio entende que implantar ações vinculadas a alternativa "Legislação" pode evitar sanções administrativas por órgãos de auditoria e regulatórios, as quais podem inviabilizar a continuidade do Projeto da PNID e, dessa forma, os tomadores de decisão do consórcio validaram a hierarquização apresentada na Figura 4.4. Assim, de posse da informação que a alternativa Legislação, com 28,875% de preferência, foi preponderante quanto as demais alternativas, o CMI decidiu investir em uma consultoria especializada em conformidade com os princípios legais exigidos pela Lei Geral de Proteção ao Dado Pessoal. No enredo da alternativa com maior peso é importante destacar que Legislação se refere ao conjunto de leis, sendo a Constituição Federal a principal, existindo, ainda, códigos, leis odinárias, dDelegadas, complementares, decretos, etc .

4.3.2 Definição do ativo

Com o término da Fase 2 e validação da hierarquização das alternativas, vide Figura 4.4, por parte dos principais tomadores de decisão do consórcio a próxima etapa busca a definição do ativo de TI relacionado a alternativa Legislação. Esse Ativo preponderantemente deverá considerar o ambiente negocial e tecnológico da PNID, pois a plataforma proporcionará ao Ecossistema de pós-graduação e ciência brasileiro oportunidades de ganho significativo de eficiência e economia por intermédio da geração e oferta aberta de informações abrangentes, precisas e atualizadas sobre todas as entidades e agentes que produzem ou fomentam ciência no Brasil. São dados relativos à pesquisadores, instituições, projetos e seus respectivos produtos científicos, conforme pode ser observado na Figura 4.5.

Tais dados auxiliarão agências governamentais, organizações de ensino, fomento e até o pesquisador individual a melhor gerir e planejar suas atividades e recursos.

Figura 4.5: Ecossistema da informação na pesquisa.



Fonte: Conecti Brasil (4).

No contexto da plataforma, os principais ativos, alinhados ao compliance do negócio, estão correlacionados às informações, as quais envolvem: bases de dados, documentos, equipamentos, locais físicos, pessoas, sistemas e unidades organizacionais.

Os Ativos, os quais compõem o universo do CMI e PNID, possuem direta ou indiretamente relação com autores, pesquisadores, instituições de ensino superior, órgãos de fomento à educação, patrocinadores, empresas particulares dentre outras, os quais podem ser observados na Figura 4.5.

Para consolidar as informações na PNID, o CMI exerce as funções primordiais de coleta, integração e compartilhamento de dados (pessoas físicas e jurídicas), que geram um alto fluxo exponencial de dados entre as instituições e seus titulares.

A partir da hierarquização e aprovação, por parte dos tomadores de decisão do Consórcio, da alternativa Legislação, a qual versa sobre o cumprimento obrigatório das leis e regulamentos aplicáveis, além das políticas e práticas que devem ser claramente definidas, implementadas e auditadas, interna ou externamente aos membros do consórcio, é possível identificar leis, regulamentos, normas, decretos e *frameworks* os quais estão conectados a conformidade de prover proteção de dados. Os dados gerados pela PNID estão relacionados aos artigos, autores, livros, órgãos de fomento, IES, dentre outros. Essas informações compõem o principal negócio do Ecossistema da Plataforma Nacional de Integração de

Dados.

A plataforma possui informações geradas em bases de dados e metadados mantidas em outros países como é caso da *Scopus*, *Web of Sciences*, IEEE e ORCID. Dessa forma, é primordial manter-se em consonância com as leis de proteção de dados pessoais dos países, os quais a PNID transaciona relação de troca de informações. Os dados gerados em outros países imprescindivelmente devem ser protegidos no território brasileiro. Com isso, é possível destacar as principais leis (nacionais e internacionais), decretos e normas, das quais a congruência se faz necessária:

1. ***General Data Protection Regulation*(Regulamento Geral de Proteção de Dados – GDPR) (171).**

   Estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. O presente regulamento defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais.

   Aplicações da GDPR

   • O regulamento aplica-se ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União Europeia, independentemente de o tratamento ocorrer dentro ou fora da União.

   • O regulamento aplica-se ao tratamento de dados pessoais por um responsável pelo tratamento estabelecido não na União, mas num lugar em que se aplique o direito de um Estado-Membro por força do direito internacional público. O tratamento de dados deve observar:

   (a) **Tratamento** - uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registro, a organização, a estruturação, a conservação, a adaptação ou a alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão ou a difusão qualquer.

   (b) **Violação de dados pessoais** - uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizados a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

Princípios relativos ao tratamento de dados pessoais

Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas (integridade e confidencialidade).

Segurança do tratamento

Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado:

(a) A pseudonimização e a cifragem dos dados pessoais.

(b) A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento.

(c) A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico.

(d) Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

Ao avaliar o nível de segurança adequado, devem ser tidos em conta, designadamente, os riscos apresentados pelo tratamento, em particular devido à destruição, perda e alteração acidentais ou ilícitas, e à divulgação ou ao acesso não autorizados, de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento (171).

2. ***Federal Trade Commission*** **(Comissão Federal de Comércio) – FTC**

Os Estados Unidos não possuem uma única autoridade nacional de proteção de dados. A FTC tem jurisdição sobre a maioria das entidades comerciais e tem autoridade para emitir e aplicar regulamentos de privacidade em áreas específicas (por exemplo, para telemarketing, e-mail comercial e privacidade de crianças) e para tomar medidas de execução a fim de proteger os consumidores contra práticas comerciais desleais ou enganosas, incluindo materialmente práticas injustas de privacidade e segurança de dados (172). A missão do FTC é proteger os consumidores

e a concorrência, a evitar práticas comerciais anticompetitivas, enganosas e desleais por meio da aplicação da lei, defesa e educação, sem sobrecarregar, de maneira indevida, as atividades comerciais legítimas (173).

3. ***California Consumer Privacy Act* (Lei de Privacidade do Consumidor da Califórnia) de 2018 CCPA**

   A Lei de Privacidade do Consumidor da Califórnia de 2018 (CCPA) dá aos consumidores mais controle sobre as informações pessoais que as empresas coletam sobre eles e os regulamentos da CCPA fornecem orientação sobre como implementá-la. Tal lei histórica garante novos direitos de privacidade para os consumidores da Califórnia, incluindo:

   • Direito de saber sobre as informações pessoais que uma empresa coleta sobre elas e como elas são usadas e compartilhadas.

   • Direito de excluir informações pessoais coletadas deles (com algumas exceções).

   • Direito de recusar a venda de suas informações pessoais.

   • Direito a não discriminação para o exercício de seus direitos na CCPA.

   As empresas são obrigadas a fornecer aos consumidores certos avisos explicando suas práticas de privacidade, e a CCPA se aplica a muitas empresas, incluindo corretores de dados (174).

4. ***Data Protection Act* 2018 (Lei de Proteção de Dados) DPA**

   O DPA controla como as informações pessoais são usadas por organizações, empresas ou o governo, em razão da implementação do Regulamento Geral de Proteção de Dados (GDPR) no Reino Unido. De acordo com a Lei de Proteção de Dados de 2018, a pessoa tem o direito de descobrir quais informações o governo e outras organizações armazenam sobre você. Isso inclui o direito de:

   • Ser informado sobre como seus dados estão sendo usados.

   • Acessar dados pessoais.

   • Ter dados incorretos atualizados.

   • Ter dados apagados.

   • Parar ou restringir o processamento dos seus dados.

   • Portabilidade de dados (permitindo que você obtenha e reutilize seus dados para diferentes serviços).

- Objetivar como seus dados são processados em certas circunstâncias.
- Processos de tomada de decisão automatizados (sem envolvimento humano) (175).

5. **Lei geral de proteção de dados pessoais (Lei nº 13.709, de 14 de agosto de 2018.) LGPD**

   Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

   A LGPD estabelece também, em seu art. 6º, que o tratamento de dados pessoais deve observar a boa-fé e dez princípios fundamentais específicos, dos quais destacam-se:

   • Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

   • Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

   • Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

   • Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais (23).

   Finalidade

   - Execução de políticas públicas.
   - Cumprimento de obrigação legal ou regulatória pelo controlador.
   - Atender aos interesses legítimos do controlador ou de terceiros.

   Uso compartilhado de dados

   Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de

tratamento permitidas por esses entes públicos, ou entre entes privados (176).

Órgãos de pesquisa

Órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no país, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico. Universidades públicas e entidades de pesquisa pública, como a Fundação Oswaldo Cruz, se enquadram nesta definição (176).

Tratamento de dados pessoais por órgãos de pesquisa (Artigo 13) (23)

Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudoanonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas. A LGPD também trouxe outras regras protetivas para a hipótese:

• Divulgação dos resultados ou excertos do estudo ou pesquisa não poderá revelar dados pessoais.

• O órgão de pesquisa será responsável pela segurança da informação e não poderá – em hipótese alguma – transferir os dados a terceiros.

• O acesso aos dados pessoais pelos órgãos de pesquisa para fins de realização de estudos em saúde pública será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.

6. Decreto nº 10.046, de 9 de outubro de 2019

Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados (177). Sua finalidade está em conformidade com as leis de proteção de dados pessoais, sejam elas de pessoas físicas ou jurídicas.

NORMAS

7. **ABNT NBR ISO/IEC 31000:2018**

   Gestão de riscos - Diretrizes. Fornece uma abordagem comum para gerenciar qualquer tipo de risco e não é específico para qualquer indústria ou setor. Indicar os *frameworks* que realizam o tratamento de base de dados (94).

8. **ABNT NBR ISO/IEC 27001:2013**

   Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão da segurança da informação – Requisitos. Esta Norma foi preparada para prover requisitos para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação (178).

9. **ABNT NBR ISO/IEC 27002:2013**

   Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação. Fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização (142).

10. **ISO/IEC 29100:2011 (2020)**

    Tecnologia da informação — Técnicas de segurança — Estrutura de Privacidade. Fornece uma estrutura de privacidade que especifica uma terminologia de privacidade comum; define os atores e suas funções no processamento de Informações de Identificação Pessoal (PII); descreve as considerações de proteção da privacidade; fornece referências a princípios de privacidade conhecidos para tecnologia da informação. ISO/IEC 29100: 2011 é aplicável a pessoas físicas e organizações envolvidas na especificação, aquisição, arquitetura, projeto, desenvolvimento, teste, manutenção, administração e operação de sistemas ou serviços de tecnologia de informação e comunicação onde controles de privacidade são necessários para o processamento de PII (179).

11. **ISO/IEC 27.701:2019**

Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27001 (2013) (178) e ABNT NBR ISO/IEC 27002 (2013) (142) para gestão da privacidade da informação — Requisitos e diretrizes. Especifica os requisitos e fornece as diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da Informação na forma de uma extensão das ABNT NBR ISO/IEC 27001 (2013) (178) e ABNT NBR ISO/IEC 27002 (2013) (142) para a gestão da privacidade dentro do contexto da organização (180).

12. **ISO/IEC 27005:2018**

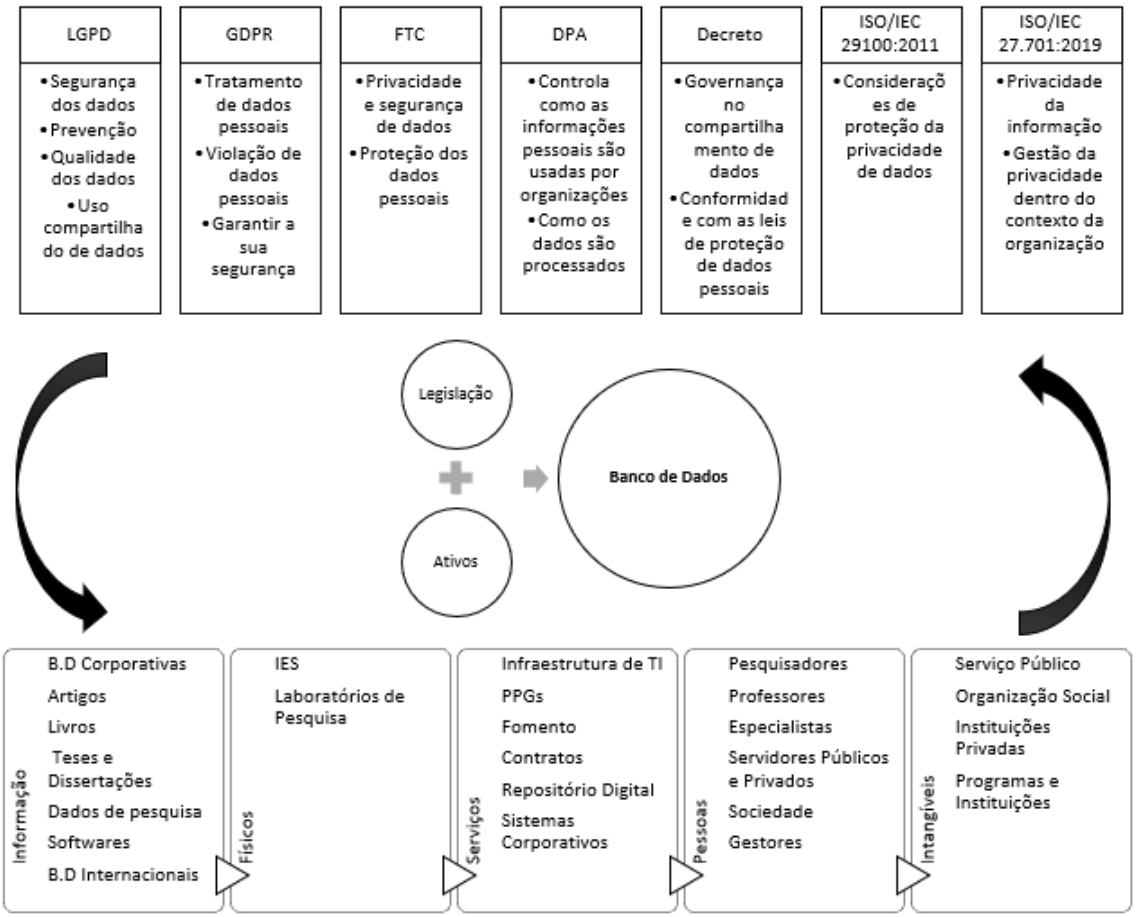
    Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação. Fornece diretrizes para o processo de gestão de riscos de segurança da informação (181).

As leis, decreto e normas supracitadas, estão relacionadas à proteção de dados. Não somente, mas também, sob o ponto de vista da Figura 4.6, que apresenta a relação entre as principais leis, decreto e normas relativas à proteção de dados e aos ativos relacionados à informação, aos físicos, à geração de serviços, às pessoas e aos intangíveis, os quais compõem o negócio do CMI e PNID. Dessa forma, a Figura 4.6 apresenta em seu eixo superior as principais características relacionadas à conformidade da Legislação. Por sua vez, o eixo inferior relaciona os principais Ativos, os quais compõem o Ecossistema de comunicação, educação, pesquisa e informação que fazem parte do CMI.

Ao considerar as principais características negociais e aplicar a técnica *What-If* (95), técnica de análise geral e qualitativa, e ter em conta os potenciais riscos à continuidade do CMI e da PNID sob o rigor da lei, os especialistas consideram que o resultado da relação Legislação + Ativos remete à base de dados como principal Ativo. Uma vez que os dados são um recurso de mérito crítico e, devido à sua importância, a proteção de dados é um componente notável da segurança de banco de dados, a qual refere-se às medidas e ferramentas usadas para proteger um banco de dados de acessos não autorizadas, ameaças e ataques maliciosos (182). A Base de Dados da Plataforma, consolida as informações coletadas, processadas, desambiguadas, semanticamente adequadas e compartilhadas em forma de serviços ou por consulta em ferramentas próprias com todos os membros consorciados. O risco o qual envolve esse ativo está relacionado à alternativa Legislação, pois expor os dados da PNID acarreta ao consórcio, conforme Artigo 52 da LGPD (23), responder a sanções administrativas aplicáveis, pela Autoridade Nacional, aos agentes de tratamento de dados, a saber (23) e (176):

- **Advertência**: com indicação de prazo para adoção de medidas corretivas.

Figura 4.6: Relação entre Legislação e Ativos.



Fonte: Autoria própria.

- **Publicização da infração**: apenas após confirmada a ocorrência.
- **Reputação**: o impacto não são apenas sanções administrativas, também pode afastar outras entidades que busquem parcerias pelo risco de serem impactados.
- **Bloqueio**: até a regularização da situação, os dados pessoais são bloqueados.
- **Eliminação**: confirmada a infração, os dados pessoais a ela relacionados serão eliminados.

Em conclusão, a proteção ao Ativo está em consonância com a alternativa Legislação, da qual contempla a conformidade com as principais leis, decretos e normas nacionais e internacionais de proteção de dados pessoais, requerendo uma análise refinada da Base de Dados da Plataforma Nacional de Integração de Dados. Ressalta-se, ainda, que os ativos físicos como a Infraestrutura de TI, Instituições de Ensino Superior, ativos humanos (pesquisadores, professores, Gestores, entre outros) e ativos intangíveis como serviço público e programas instituições são representativos e impactantes ao negócio do CMI, entretanto, podem ser analisados ao longo da vida útil da PNID não requerendo uma pronta imersão.

4.4 Fase 4 - Modelo de Gestão de riscos

O tema de Gestão Riscos é rico, amplo e bastante difundido na literatura, não havendo consenso em relação qual seria o melhor modelo e sim o mais adequado para cada contexto ou negócio, conforme pode ser observado nos modelos de gestão de riscos conhecidos, a saber:

COSO-IC (COSO I) - em 1992 (183), o Committee of Sponsoring Organizations of the Treadway Commission – COSO publicou o guia Internal Control - integrated framework (COSO-IC ou COSO I), com o objetivo de orientar as organizações quanto a princípios e melhores práticas de controle interno, em especial para assegurar a produção de relatórios financeiros confiáveis e prevenir fraudes. O modelo do COSO-IC é representado por um cubo no qual as três faces visíveis representam os tipos de objetivos, os níveis da estrutura organizacional e os componentes.

Modelo *Boehm* - o modelo de gerenciamento de risco de Boehm concentra-se no conceito de "exposição ao risco". O impacto do risco é determinado pela probabilidade de resultados insatisfatórios e perdas, e Boehm categorizou o processo de gerenciamento de risco em duas etapas principais e cada etapa é dividida em três subetapas principais (79).

Modelo *Riskit* - O modelo fornece informações de projeto precisas e atualizadas para o gerente de projeto, assim, permitindo-lhe reduzir os efeitos adversos e maximizar o potencial do projeto. Este modelo divide o processo de RM em sete processos principais: Definição de Mandato de RM, Revisão de Meta, Identificação de Risco, Análise de Risco, Planejamento de Controle de Risco, Controle de Risco e Monitoramento de Risco (184).

Software Engineering Institute - Software Risk Evaluation (SEI-SRE) originalmente desenvolvido para o domínio de gerenciamento de projetos e integrado aos elementos de gerenciamento de riscos em uma fase posterior. SEI-SRE descreve o processo de identificação de risco com mais detalhes em comparação com outros métodos. Este método também usa uma ferramenta de gerenciamento de risco que foi testada e comumente usada por profissionais. O SEI-SRE é composto por cinco processos principais, a saber, Identificação, Análise, Planejamento, Controle e Comunicação de Riscos (185).

Project Management Body of Knowledge (PMBOK) - conjunto de conhecimentos em gerenciamento de projetos (PMBOK) que descreve o processo de gestão de riscos em seis etapas: planejamento de gerenciamento de riscos, identificação de riscos, análise quantitativa de riscos, análise qualitativa de riscos, planejamento de respostas a riscos e controle de riscos. Os riscos são analisados por meio de análises qualitativas e quantitativas de

riscos, sendo que Análise Qualitativa de Risco prioriza os riscos com base na probabilidade de ocorrência do risco e seu impacto, enquanto a Análise Quantitativa de Risco examina a possibilidade de atingir os objetivos de custo e tempo em relação ao impacto e aos possíveis riscos (22).

ISO 31000 (2018), Gestão de riscos – Diretrizes (94). Por certo o emprego do padrão da norma ISO 31000 (2018) (94), para essa pesquisa de mestrado, assim como demonstrado pela literatura quanto a utilização das ferramentas e técnicas aplicadas ao processo de Gestão de Riscos, evidencia seu uso nos últimos anos no Brasil e em diversos outros países. No Brasil a norma ISO 31000 (2018) (94) é citada e referenciada por diversos entes da Administração Pública Federal, órgãos de controle, como Tribunal de Contas da União e Controladoria Geral da União, além de instituições privadas relacionadas a Gestão de Riscos.

4.4.1 Análise do ativo

Um sistema gerenciador de banco de dados (SGBD) é uma coleção de programas que permite aos usuários criar e manter um banco de dados. O SGBD é, portanto, um sistema de *software* de propósito geral que facilita os processos de definição, construção, manipulação e compartilhamento de bancos de dados entre vários usuários e aplicações (186). Para Silberschatz e Sudarshan (2006) (187), a coleção de dados, normalmente chamada de banco de dados, contém informações relevantes a uma empresa.

Na opinião do *Center for Internet Security* - CIS (Centro de Segurança da Internet) (188), banco de dados é uma coleção organizada de dados, geralmente armazenados e acessados eletronicamente a partir de um sistema de computador. Os bancos de dados podem residir remotamente ou no local. Sistemas de gestão de banco de dados (SGBDs ou DBMSs) são usados para administrar bancos de dados e não são considerados parte de um banco de dados. Deste modo, o SGBD é um Ativo sensível e fundamental na estrutura de empresas e órgãos governamentais, pois nas últimas duas décadas, a quantidade de dados gerados, coletados e armazenados tem aumentado constantemente. Este crescimento está agora alcançando proporções dramáticas e afetando todos os aspectos de nossa vida, incluindo contextos sociais, políticos, comerciais, científicos, médicos e jurídicos. Com o aumento do tamanho, das aplicações potenciais e da utilidade desses dados, as preocupações com a privacidade tornam-se mais agudas (189).

Os SGBDs fazem parte do negócio de empresas, órgãos governamentais, instituições de ensino, centros de pesquisas, entre outros, e, com isso, manter os dados seguros e garantir a privacidade são premissas estratégicas. Tradicionalmente, a privacidade era realizada por meio de vários métodos de controle de acesso ao banco de dados e dependia

muito do uso de visualizações definidas estaticamente, que são construções essencialmente lógicas impostas às tabelas de banco de dados que podem alterar ou restringir os dados que podem ser visualizados por um usuário (190). Assim, esses requisitos de privacidade frequentemente surgem em cenários de aplicação da lei e do governo, bem como em alguns cenários de negócios (191).

Os princípios de proteção de dados podem ser derivados da estrutura legal e é um direito fundamental conforme pode ser observado com a Declaração dos Direitos Humanos das Nações Unidas de 1948, artigo 12, a qual indica: “ninguém será sujeito a interferência arbitrária em sua privacidade, família, casa ou correspondência, nem a ataques à sua honra e reputação. Toda pessoa tem direito à proteção da lei contra tais interferências ou ataques.”. De acordo com a lei europeia de proteção de dados, o tratamento de dados pessoais é legítimo se: o indivíduo cujos dados pessoais estão sendo processados (o titular dos dados) deu consentimento inequívoco, ou o processamento é necessário para a execução de um contrato, para cumprimento de uma obrigação, a fim de proteger os interesses vitais do titular dos dados, para o desempenho de uma tarefa de interesse público ou para efeitos dos interesses legítimos prosseguidos pelas entidades de tratamento de dados, exceto quando tais interesses sejam anulados pelos direitos e liberdades fundamentais de o titular dos dados (192).

Desse jeito, os sistemas de gerenciamento de banco de dados (DBMSs) são a principal "ferramenta" usada para armazenar e manipular dados pessoais, desse jeito, as empresas devem prestar atenção especial ao design e manipulação de seus bancos de dados e a forma como podem estar em conformidade com a Lei de Proteção de Dados (193).

Por fim, é urgente ter uma estrutura de segurança de banco de dados que possa controlar o acesso, proteger a privacidade dos dados e a exposição de dados confidenciais (194). A partir da definição do Banco de Dados como principal Ativo, foco da pesquisa, são relacionadas as ações necessárias alinhadas às melhores práticas das normas de Segurança da Informação disponíveis, como a norma ABNT NBR ISO/IEC 31000 (2018) (94), norma identificada como adequada para aplicação da GR. A ISO 31000 (2018) (94) é caracterizada como o guia mais aplicado nas últimas décadas, conforme pode ser comprovado durante as pesquisas, a qual se propõem a aplicar o processo de Gestão de Riscos. Dessa forma, pode ser considerada como referência na GR, uma vez que compreende de forma ampla os procedimentos inerentes para implantação de um modelo de Gestão de Riscos. A primeira etapa de aplicação da norma consiste na identificação dos riscos, conforme pode ser observado no item que segue.

4.4.2 Identificação dos riscos

O PMBoK (2017) (22) considera que identificar os riscos é o processo de identificação dos riscos individuais do projeto, bem como fontes de risco geral do projeto, e de documentar suas características. O principal benefício deste processo é a documentação de cada risco de projeto existente e as fontes gerais de riscos do projeto. A ISO 31000 (2018) (94) considera que convém a organização identificar as fontes de risco, áreas de impactos, eventos (incluindo mudanças nas circunstâncias) e suas causas e consequências potenciais. A finalidade desta etapa é gerar uma lista abrangente de riscos baseada nestes eventos que possam criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos. Para norma ISO 31010 (2012) (95) a identificação dos riscos é o processo de encontrar, reconhecer e registrar os riscos. O COSO (2015) (183) considera os riscos como eventos e, nesse caso, entende que são eventos internos e externos que influenciam o cumprimento dos objetivos de uma organização e devem ser identificados e classificados entre riscos e oportunidades.

Outrossim, para realização da coleta de dados, tarefa de identificação de riscos, foram utilizadas ferramentas e técnicas apoiadas pela ISO 31010:2012 (95) e PMBOK (2017) (22), vide Figura 4.7 , as quais são classificadas como aplicáveis, a saber:

Figura 4.7: Ferramentas e técnicas.

Fonte: ISO 31010 (2012) (95) e PMBOK (2017) (22).

• ***Brainstorming*** (técnica). O objetivo é obter uma lista abrangente de cada risco de projeto e as fontes do risco geral. A equipe do projeto normalmente realiza *brainstorming*, frequentemente com um conjunto multidisciplinar de especialistas que não fazem parte da equipe. As ideias são geradas sob a orientação de um facilitador, seja em uma sessão de *brainstorming* de forma livre ou uma que usa técnicas mais estruturadas. As categorias de riscos, como uma estrutura analítica dos riscos, podem ser usadas como um modelo. Atenção especial deve ser dada para assegurar que os riscos identificados na sessão de *brainstorming* estejam claramente descritos, pois a técnica pode resultar em ideias não totalmente formadas (95).

• **Listas de verificação** (método baseado em evidências). Uma lista de verificação é uma lista de itens, ações ou pontos a serem considerados, e com frequência é usada como lembrete. Tais listas se baseiam nas informações históricas e no conhecimento acumulado de projetos semelhantes e outras fontes de informações e são uma forma eficaz de capturar lições aprendidas de projetos semelhantes concluídos, listando riscos individuais de projeto que ocorreram anteriormente e que podem ser relevantes para este projeto. No caso das listas, foram pesquisadas em referências teóricas e órgãos especializados em segurança da informação (188), (195) e (196).

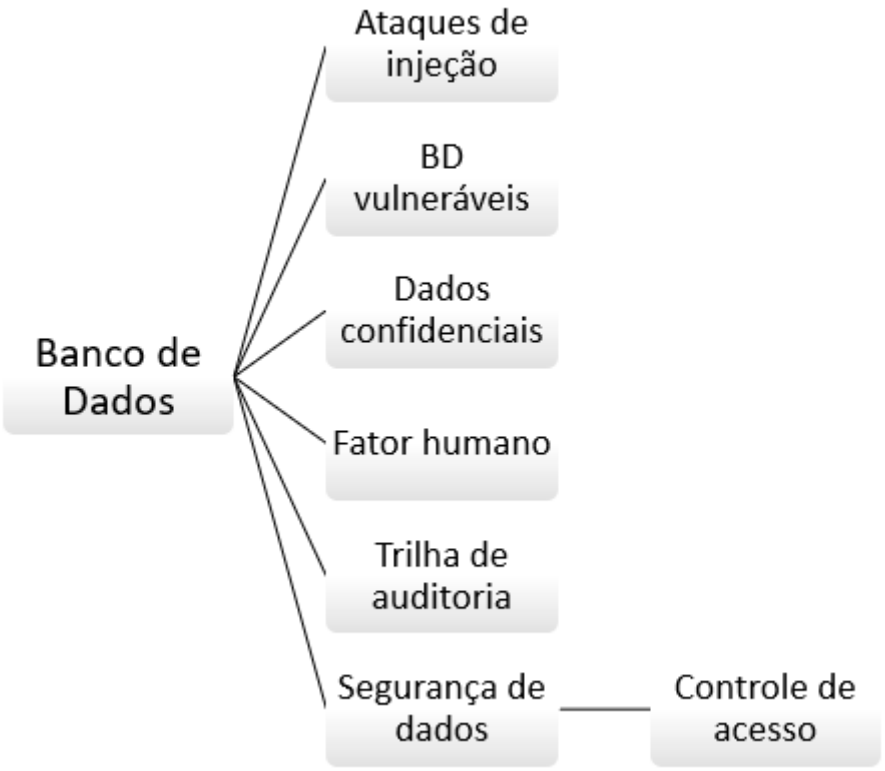
• **Entrevista** (técnica - semiestruturada). Os riscos individuais e as fontes de risco geral podem ser identificados entrevistando participantes com experiência no projeto, partes interessadas e especialistas no assunto. As entrevistas foram realizadas com os especialistas envolvidos no projeto da PNID e técnicos responsáveis pela Infraestrutura e Banco de Dados.

É importante ressaltar as limitações observadas na aplicação da Identificação dos Riscos, pois dados históricos relacionados a potências riscos inerentes ao Ativo Banco de Dados não existem. Os riscos foram identificados com o apoio das ferramentas e técnicas citadas durante reuniões semiestruturadas. Para esse processo de elicitação, participaram os especialistas de negócios relacionados a Plataforma Nacional de Integração de Dados, Administradores de Banco de Dados (DBA), Administradores de Dados (AD), Analistas da infraestrutura (AI) e Analistas de Segurança da informação (ASI), formando, desse jeito, um grupo multidisciplinar de especialistas. Como resultado desse trabalho e melhor forma de visualizar a variedade de fatores, internos e externos, os quais podem dar origem aos riscos relacionados ao ativo Banco de Dados, eles foram organizados em uma Estrutura Analítica dos Riscos - EAR, conforme pode ser observado na Figura 4.8.

Os próximos tópicos buscam, de forma breve, contextualizar cada item, categoria, que compõem a EAR.

• **Ataques de injeção de banco de dados** - os dois principais tipos de ataques de injeção de banco de dados são injeções de SQL que visam sistemas de banco de dados

Figura 4.8: Estrutura Analítica dos Riscos.



Fonte: Autoria própria.

tradicionais e injeções NoSQL que visam plataformas de "big data" (195).

• **Bancos de dados vulneráveis** - geralmente, as organizações levam meses para corrigir os bancos de dados, durante os quais eles permanecem vulneráveis. Os invasores sabem explorar bancos de dados não corrigidos ou bancos de dados que ainda têm contas e parâmetros de configuração padrão. Os problemas típicos incluem altas cargas de trabalho e acúmulos de montagem para os administradores de banco de dados associados, requisitos complexos e demorados para testes de patches e o desafio de encontrar uma janela de manutenção para derrubar e trabalhar no que muitas vezes é classificado como um sistema crítico para os negócios (195).

• **Dados confidenciais não gerenciados** - muitas empresas lutam para manter um inventário preciso de seus bancos de dados e dos objetos de dados críticos contidos neles. Bancos de dados esquecidos podem conter informações confidenciais e novos bancos de dados podem surgir sem visibilidade para a equipe de segurança. Dados confidenciais nesses bancos de dados serão expostos a ameaças se os controles e permissões necessários não forem implementados (195).

• **O fator humano** - a causa raiz de 30% dos incidentes de violação de dados é a

negligência humana, de acordo com o estudo do *Ponemon Institute Cost of Data Breach* (Custo de violação de dados do *Ponemon Institute*) (197).

• **Trilha de auditoria** - em relação aos bancos de dados, é um meio de rastrear todas as atividades que afetam uma informação, como um registro de dados, desde o momento em que entra no banco de dados até o momento em que sai (193).

• **Segurança de dados** - os objetivos de alto nível da segurança de dados estão relacionados ao sigilo, a integridade e a disponibilidade dos dados. O sigilo, ou confidencialidade, está preocupado com a divulgação não autorizada de informações, a integridade com a modificação não autorizada de informações ou processos e a disponibilidade com a negação indevida de acesso à informação. Os meios para atingir esses objetivos e a base para a segurança do banco de dados são fornecidos pela autenticação, controle de acesso e auditoria em conjunto (193).

• **Controle de acesso** - o Controle de Acesso, também conhecido como Autorização, medeia o acesso a recursos com base na identidade e geralmente é orientado por políticas (embora a política possa estar implícita). É o principal serviço de segurança que preocupa a maioria dos *softwares*, com a maioria dos outros serviços de segurança suportando-o (195).

A partir das categorias, os riscos foram identificados e listados, conforme mostra o Quadro 6. Essa lista busca demonstrar as possíveis fontes de fragilidades para cada categoria de riscos elencada na EAR, a saber:

Quadro 6: Lista de Riscos.

Categoria	**Risco**	**Observações**
Ataques de injeção	Uso inadequado de instruções.	Uso de instruções - consiste na injeção de SQL, quando os desenvolvedores de *software.* criam consultas dinâmicas de banco de dados as quais incluem entradas fornecidas pelo usuário.
Ataques de injeção	Procedimentos inadequados armazenados.	Os procedimentos armazenados nem sempre estão protegidos contra injeção, pois as instruções SQL como parâmetros não são parametrizadas automaticamente.
Ataques de injeção	Inadequado uso de escape de entrada.	O SGBD pode confundir a entrada do usuário com o código SQL escrito pelo desenvolvedor, assim causando possíveis vulnerabilidades de injeção de SQL.
Ataques de injeção	Não validar lista de permissões.	Várias partes das consultas SQL podem fazer uso de variáveis de ligação, como nomes de tabelas ou colunas e o indicador de ordem de classificação (ASC ou DESC), facilitando a injeção de SQL.
BD vulneráveis	Inadequado uso de acesso à rede.	BD com acesso à rede (TCP).
BD vulneráveis	Inadequada configuração de acesso.	BD com acesso a *host* não locais, além de *host* comuns com regras frágeis de firewall.
BD vulneráveis	Configuração de Banco de Dados inadequada.	BD permitir conexões que não sejam criptografadas.
BD vulneráveis	Falta de um certificado digital confiável no servidor.	BD sem verificação de confiabilidade de certificado digital.
BD vulneráveis	Inadequado uso de contas e Bancos de Dados padrão.	Falta de contas de usuário e instalações de SGBD configurados como padrão.
Dados confidenciais	Inadequado uso de procedimentos de autenticação.	Falta de procedimentos de autenticação para garantir que a pessoa que faz uma solicitação de acesso ao seu os dados pessoais são, de fato, o titular dos dados.

Categoria	**Risco**	**Observações**
Dados confidenciais	Inadequado uso de identificadores de titulares de dados.	Falta de mecanismos para manter detalhes sobre todos os identificadores de titulares de dados usados nos sistemas da organização.
Dados confidenciais	Permitir localizar todos os dados pessoais.	Falta de mecanismos para localizar todos os dados pessoais mantidos no banco de dados da organização relativos a um único indivíduo.
Dados confidenciais	Inadequado uso de dados que identificam o titular.	Falta de mecanismos para manter detalhes sobre quais dados identificam o titular dos dados e em qual contexto ele se encontra.
Dados confidenciais	Permitir rastreabilidade de dados pessoais.	Falta de mecanismos para exclusão de informações e *links*, os quais permitem que os indivíduos sejam identificados.
Dados confidenciais	Inadequado uso de consentimentos dos titulares dos dados.	Falta de mecanismos para manter detalhes sobre os consentimentos dos titulares dos dados para processar seus dados pessoais, transferir suas informações para outras instituições ou publicar os dados pessoais na *web*.
Dados confidenciais	Não distinguir dados pessoais.	Falta de mecanismos para distinguir dados pessoais entre sensíveis e não sensíveis e quais são processados para fins de pesquisa.
Dados confidenciais	Permitir a rastreabilidade de manipulação de dados.	Falta de rastreabilidade relativa as pessoas autorizadas a manipular os dados pessoais, as funções dos usuários autorizados dentro da organização, as fontes dos dados pessoais e as solicitações de acesso do titular dos dados.
Dados confidenciais	Não ter transparência quanto ao objetivo do uso de dados dos titulares.	Falta de detalhes relativos aos objetivos do processo de armazenamento dos dados dos titulares dos dados.

Categoria	Risco	Observações
Fator humano	Não definir um programa de conscientização de segurança.	Estabelecer e manter um programa de conscientização de segurança.
Fator humano	Inadequada proteção contra ataques de engenharia social.	Falta de treinamentos para os membros da força de trabalho com o intuito de reconhecer ataques de engenharia social.
Fator humano	Não treinar a força de trabalho.	Falta de treinamento dos membros da força de trabalho nas melhores práticas de autenticação, melhores práticas de tratamento de dados, em relação as causas da exposição não intencional de dados, no reconhecimento e comunicação de incidentes de segurança e na identificação e comunicação se o Ativo Banco de Dados corporativos está faltando atualizações de segurança.
Fator humano	Inadequadas competências e conscientização de segurança.	Falta de conduzir treinamento de competências e conscientização de segurança para funções específicas, além de os perigos ao se conectar e transmitir dados corporativos em redes inseguras.
Trilha de auditória	Não auditar os processos de dados pessoais.	Falta de auditar os processos de dados pessoais para garantir que a notificação cobre adequadamente as atividades de processamento.
Trilha de auditória	Uso indevido de dados pessoais.	Falta de implantação de mecanismos para garantir que o uso indevido de dados pessoais dentro da organização pode ser identificado e remediado.
Trilha de auditória	Não restringir o processamento de dados pessoais.	Falta de restrições para realização do processamento de dados pessoais não relacionados com as atividades da organização usando os recursos da organização.

Categoria	**Risco**	**Observações**
Segurança de dados	Não permite divulgações ilegais de dados.	Garantir que o banco de dados não permite divulgações ilegais de dados pessoais.
Segurança de dados	Inadequado uso de solicitação de dados pessoais de outra pessoa.	Garantir que quando alguém solicitar dados pessoais sobre outra pessoa, tais dados devem ser apenas divulgados, e na medida em que requer os dados para o desempenho de suas funções oficiais.
Segurança de dados	Permitir a divulgação de dados pessoais errados.	Garantir que nenhum dado pessoal de outro titular de dados seja divulgado, quando um titular de dados solicitar para acessar seus registros pessoais.
Segurança de dados	Não implantar técnicas de segurança para proteger os dados de ataques.	Garantir a implantação de técnicas de segurança para proteger os dados de ataques eletrônicos internos e externos.
Segurança de dados	Falta de método seguro de transmissão.	Garantir o fornecimento de um método seguro de transmissão, quando os dados pessoais são coletados ou processados on-line.
Segurança de dados	Não exclusão permanentemente os dados.	Garantir a correção e exclusão permanentemente dos dados, além da exclusão automática dos dados pessoais, quando o tempo de retenção expirar.
Segurança de dados	Não mesclar bancos de dados e integrar fontes de informação.	Mesclar bancos de dados e integrar fontes de informação usando correspondências completas de todos os critérios, manter arquivos de papel digitalizados e outros arquivos de computador separados de bancos de dados, que contêm dados pessoais (por exemplo, bancos de dados multimídia).

Categoria	Risco	Observações
Segurança de dados	Não alterar os sistemas de hardware e software da organização.	Alterar os sistemas de hardware e software da organização, evitando perda na precisão dos dados e integridade.
Segurança de dados	Falta de arquivos de backup.	Garantir a realização de arquivos de backup.
Controle de acesso	Não definir processo de concessão de acesso.	Conceder acesso aos ativos corporativos mediante concessão de direitos ou mudança de função de um usuário.
Controle de acesso	Não definir um processo de revogação de acesso.	Revogar o acesso aos ativos corporativos, por meio da desativação de contas imediatamente após o encerramento, revogação de direitos ou mudança de função de um usuário.
Controle de acesso	Não implantar Múltiplo Fator de Autenticação (MFA) para aplicações expostas externamente.	Aplicações corporativas ou de terceiros expostas externamente sem aplicar o MFA.
Controle de acesso	Não inventariar os sistemas de autenticação e autorização.	Inventário dos sistemas de autenticação e autorização da empresa, incluindo aqueles hospedados no site local ou em um provedor de serviços remoto.

Fonte: Autoria própria.

A Atividade de Identificação de Riscos gerou uma lista de potenciais riscos, , conforme tabela acima, a qual é a principal saída da Identificação dos riscos. Nesse processo buscou-se identificar os principais riscos que podem impactar negativamente o Ativo Banco de Dados, entretanto, ressalta-se que a lista não é taxativa ou exauriu os possíveis riscos relacionados ao ativo. Com fundamento na identificação dos riscos, as etapas seguintes são responsáveis por realizar a análise e avaliação dos riscos. Essas etapas são suportadas pela metodologia proposta, conforme Figura 4.10. A seguir um detalhamento quanto à análise e avaliação dos riscos.

4.4.3 Análise de riscos

Segundo a norma ISO 31000 (2018) (94) a Análise de Riscos envolve desenvolver a compreensão dos riscos. A análise de riscos fornece uma entrada para a avaliação de riscos e para as decisões sobre a necessidade de os riscos serem tratados, e sobre as estratégias e métodos mais adequados de tratamento de riscos. A análise de riscos também pode fornecer uma entrada para a tomada de decisões em que escolhas precisam ser feitas e as opções envolvem diferentes tipos e níveis de risco.

A análise de riscos pode ser realizada com diversos graus de detalhe, dependendo do risco, da finalidade da análise e das informações, dados e recursos disponíveis. Dependendo das circunstâncias, a análise pode ser qualitativa, semiquantitativa ou quantitativa, ou uma combinação destas.

O PMBoK (2017) (22) considera a análise de riscos em duas etapas: Análise Qualitativa e Quantitativa. A Análise Qualitativa dos Riscos é o processo de priorização de riscos individuais do projeto para análise ou ação posterior, através da avaliação de sua probabilidade e impacto de ocorrência, assim como outras características. A Análise Quantitativa dos Riscos é o processo de analisar numericamente o efeito combinado dos riscos individuais identificados e outras fontes de incerteza nos objetivos gerais do projeto. Para essa pesquisa a análise quantitativa não será realizada, pois não faz parte da proposta medir o impacto relacionado a possíveis prejuízos financeiros.

A ferramenta utilizada para realizar a análise dos riscos é a *Failure mode and effects analysis* (Modo de falha e análise de efeitos) FMEA (198), devido a sua simplicidade de aplicação e facilidade quanto ao uso. O FMEA requer a realização das atividades em equipe. Assim, essa etapa é conduzida por um time multidisciplinar de especialistas vindos de diferentes domínios e departamentos (199), os quais são especialistas de negócios relacionados à PNID, Administradores de Banco de Dados, Administradores de Dados, Analistas da infraestrutura e Analistas de Segurança da informação. Após a análise de riscos o passo seguinte é a realização da avaliação dos riscos. A análise dos riscos é realizada a partir da metodologia proposta, conforme pode ser observada na Figura 4.10.

4.4.4 Avaliação de riscos

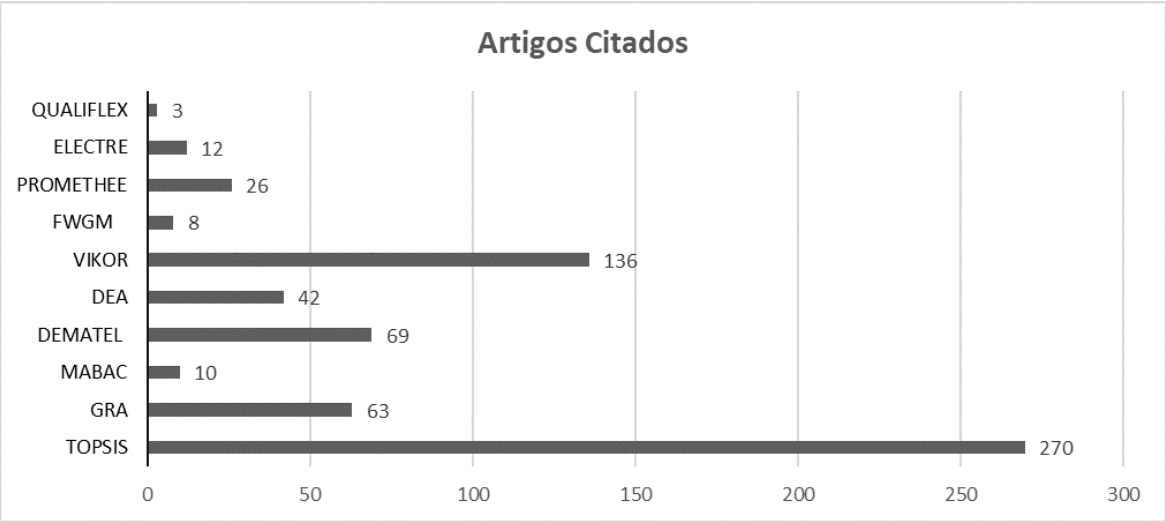
A avaliação de riscos permite que uma organização considere até que ponto eventos em potencial podem impactar a realização dos objetivos. Os impactos positivos e negativos dos eventos em potencial devem ser analisados isoladamente ou por categoria em toda a organização. Os riscos são avaliados com base em suas características inerentes e residuais (183).

Um fator importante elencado pela literatura para realização da avaliação dos riscos é inerente ao uso do FMEA, pois relaciona a possibilidade da análise dos riscos, realizadas pelos membros da equipe FMEA, possuírem algum fragmento de imprecisão, incerteza ou hesitações, devido à pressão de tempo, falta de conhecimento, deficiência de informação e recursos humanos limitados ao processamento de informação. Isto posto, para aumentar a eficácia do FMEA muitos métodos de tomada de decisão multicritério (MCDM) foram aplicados para avaliar adequadamente o risco de modos de falha nas últimas duas décadas (199). Uma série de metodologias multicritério foram desenvolvidas ao longo do tempo com o objetivo de fornecer uma estrutura sistemática a qual considera a natureza multidimensional do problema do mundo real (200). De acordo com os autores (201), os métodos MCDM permitem decisões a serem reguladas com base nos critérios ponderados mais relevantes para o problema a ser respondido pelos tomadores de decisão, em que a importância dos critérios é definida por eles em um processo interativo com outros atores.

Com interesse de fundamentar o uso de métodos MCDM com o FMEA, neste trabalho, foi realizada uma pesquisa na literatura, acesso em 19/12/2021, com uso de parâmetros dos quais compreendem o período de 2001 até 2022. O filtro foi aplicado nas bases indexadas da *Scopus*, *Web of Science* - Coleção Principal (*Clarivate Analytics*) - WOS e IEEE *Xplore* - IEEE.

A pesquisa resultou em 639 artigos relacionados aos métodos MCDM e sua frequência de uso na literatura com FMEA. A Figura 4.9 consolida esses resultados.

Figura 4.9: Métodos MCDM identificados na pesquisa.

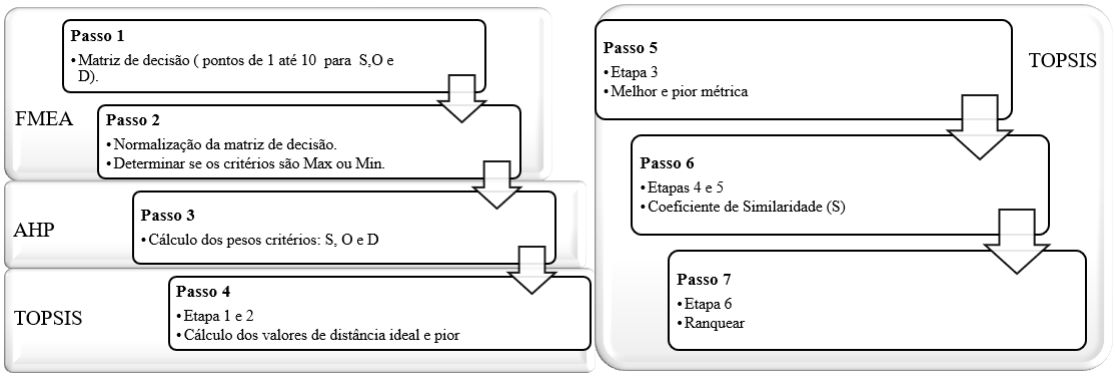


Fonte: *Scopus*, *WOS* e IEEE.

É possível observar que o método TOPSIS foi o mais utilizado para priorizar modos de falha em FMEA e contribuiu com 270 artigos (42%) do total geral de artigos identifica-

dos. Em seguida, VIKOR com 136 citações (21%) e DEMETEL com 69 (11%). A partir do resultado da pesquisa na literatura o TOPSIS, um método multicritério de tomada de decisão apresentado para classificar a preferência dos modos de falha em relação aos fatores de risco (202), foi o método estabelecido para aumentar a eficácia e superar as limitações do FMEA tradicional (203) no domínio dessa pesquisa de mestrado, além de realizar a avaliação dos riscos. A relação entre os métodos FMEA e TOPSIS pode ser observado na Figura 4.10. Com isso, as etapas de análise e avaliação de riscos são realizadas por uma metodologia composta pelo FMEA e uma hibridização entre AHP e TOPSIS.

Figura 4.10: Modelo FMEA modificado com uso de AHP e TOPSIS



Fonte: Autoria própria.

Os próximos passos pormenorizam a proposição da metodologia aplicada para fase de análise e avaliação dos riscos, as quais minudenciam como os métodos FMEA, AHP e TOPSIS trabalham de forma coesa e sinérgica, e em que o resultado da aplicação de um método gera os insumos para entrada do método seguinte, assim, possibilitando a geração do ranqueamento dos modos de falha, riscos, identificados na fase de identificação de riscos.

Metodologia proposta

A metodologia proposta é composta pelo método FMEA aplicado na etapa de análise dos riscos da fase 4, com o AHP aplicado para realizar o cálculo dos pesos relativos aos critérios. Nessa conjunção, são considerados critérios: severidade, ocorrência e detecção. Desta forma, o AHP é aplicado para complementar a etapa de análise de riscos. O TOPSIS é utilizado na avaliação dos riscos e visa ranquear os riscos elencados nas etapas de identificação e análise de riscos. A seguir, um maior detalhamento relacionado às metodologias utilizadas.

Análise de modo e efeito de falha - FMEA

Em uma pesquisa simples, ao utilizar como parâmetro o termo FMEA, base de dados da *Scopus*, foram retornados 5.355 documentos. Ao pesquisar na base da WOS - Coleção Principal (*Clarivate Analytics*), retornaram 3.347 artigos e, por fim, na base do IEEE *Xplore* retornaram 961 artigos.

FMEA foi concebida como uma metodologia de um projeto formal durante a década de 1960 pela indústria aeroespacial (198) e provou ser uma ferramenta útil para prevenir potenciais falhas em sistemas complexos e tem como objetivo fornecer informações para a tomada de decisões de gerenciamento de risco, além de fazer parte da norma ISO 31010 (2012) (95). É um método sistemático de avaliação de segurança e risco (204), o qual mitiga potenciais falhas em sistemas, processos, projetos ou serviços e tem sido usada em uma ampla série de indústrias (205).

É uma função de decisão de grupo e não pode ser realizada individualmente (206). Dessa forma, está em sinergia e justifica-se a escolha como ferramenta de análise de riscos para o ativo banco de dados da PNID, pois para essa atividade foram destacados o grupo multidisciplinar de especialistas (especialistas de negócios relacionados a PNID, DBAs, ADs, AI e ASI). É pertinente destacar, similarmente, que não existem dados históricos relacionados a análise de riscos para o ativo de banco de dados na alçada da PNID ou mesmo no contexto geral do Consórcio Multi-Institucional, assim, ratifica a justificativa da escolha do FMEA como ferramenta de análise de riscos.

FMEA possui os componentes chamados de Severidade (S), Ocorrência (O), Detecção (D) e *Risk Priority Number* (Número de Prioridade de Risco) - RPN para obter uma prioridade de risco, além de possibilitar a identificação do efeito gerado pelo risco e provável causa de geração do risco. Dessarte, é possível destacar:

- **Severidade** - é uma avaliação do nível de impacto de uma falha no projeto ou processo.
- **Ocorrência** - Refere-se à frequência em que a causa de uma falha pode ocorrer.
- **Detecção** - é uma avaliação de quão bem os controles de produto ou processo detectam a causa da falha ou modo de efeito de falha.
- **Efeito** - são as consequências causadas pela ocorrência do evento do risco, além de as formas como o desempenho do projeto, sob o ponto de vista dos especialistas, pode ser prejudicado.
- **Causa** - são os eventos, circunstâncias, os quais podem gerar as falhas.

Sua aplicação é simples e os parâmetros usados para determinar a criticidade de um modo de falha, para cada evento de risco identificado, são a Severidade, Ocorrência e Detecção. A multiplicação desses parâmetros (S x O x D) possibilita a identificação do RPN, utilizado para ranquear os riscos, em que:

$$\mathbf{RPN} = SxOxD(207). \tag{4.4}$$

No caso desse trabalho de pesquisa, os fatores de risco (S, O e D) foram avaliados pelo grupo multidisciplinar de especialistas, os quais utilizaram as escalas numéricas conforme as variações indicadas (208) para analisar os riscos, a saber:

Tabela 4.2: Cálculo dos pesos.

Fator	**Impacto mínimo**	**Impacto máximo**
Severidade	1 = Nenhuma	10 = Perigoso
Ocorrência	1 = Quase impossível	10 = Extremamente alto
Detecção	1 = Quase certo	10 = Incerteza absoluta

Fonte: FMEA (198) (adaptado).

Por consequência, com o aumento da escala, o critério analisado pode ficar cada vez mais importante, ou seja, gerar um maior impacto ao ativo. Logo, a imersão junto ao grupo de especialistas possibilitou, da mesma forma, a identificação do efeito causado pelo evento do risco, a provável causa, e, ainda por cima, os controles atuais existentes. Para essa pesquisa a aplicação do FMEA limitar-se-á a coletar a sensibilidade dos especialistas quanto a severidade, ocorrência, detecção, efeito, causas e se existem ou não controles atuais.

Os estágios de aplicação do FMEA (205) são realizados a partir da aplicação das etapas de 1 até 4. O modo de falha de cada evento de riscos é ranqueado a partir da aplicação do TOPSIS, conforme Figura 4.10. As etapas são as seguintes:

Etapa 1 - Determinar a função ou processo de serviço a ser avaliado.

No contexto desse trabalho a abordagem será direcionada ao ativo banco de dados, os quais foram categorizados na Figura 4.8.

Etapa 2 - Recrutar uma equipe multidisciplinar.

Para essa etapa foram convocados o grupo multidisciplinar de especialistas identificados na atividade de identificação dos riscos.

Etapa 3 - Realizar a reunião para determinar todas as etapas e tarefas do processo de avaliação de risco.

A equipe reuniu-se no formato de grupo de trabalho e as deliberações foram por consenso.

Etapa 4 - Listar os modos e as causas das falhas.

Foi relacionado tudo que pode dar errado, incluindo problemas menores e raros. Em seguida, identificou-se todas as causas possíveis para cada modo de falha listado. Essa etapa foi realizada a partir da EAR, Figura 4.8, e a tarefa de identificação dos riscos.

Processo Hierárquico Analítico - AHP

O método AHP, conforme explicações anteriores, foi proposto e concebido por Saaty (1980) (135) como uma abordagem multicritério de tomada de decisão. O AHP é utilizado de forma híbrida com o TOPSIS, e o método AHP fornece os pesos utilizados na realização dos cálculos dos valores de distância ideal e pior a partir do cálculo do Vetor de Eigen (206), (209), (210) e (211).

Técnica de Preferência de Pedido por Similaridade à Solução Ideal - TOPSIS

O TOPSIS é um método estabelecido sobre o conceito de solução ideal positiva e solução ideal negativa simultaneamente. Os autores Yoon e Hwang (1981) (212) desenvolveram a Técnica de Preferência de Pedidos por Similaridade à Solução Ideal baseada no conceito de que a alternativa escolhida deve ter a menor distância da solução ideal e a mais distante da solução ideal-negativa. O mesmo método empregou distâncias euclidianas para determinar a relação entre as alternativas e os dois "pontos de referência", tendo em vista o princípio de que a alternativa de primeiro nível deve estar mais próxima do ponto ideal positivo e simultaneamente longe do ponto ideal negativo (213). Acrescente-se que o método TOPSIS é aplicado para classificar e determinar as prioridades de risco dos modos de falha identificados com base nos fatores de risco definidos no contexto dessa pesquisa.

O método TOPSIS avalia uma matriz de decisão com m alternativas associadas a n atributos (ou critérios).

Os processos do método TOPSIS são apresentados a seguir, com adaptações de Hwang e Yoon (1981) (212) e Liu et al. (2014) (214):

$$\text{Matriz} = \begin{array}{c} \begin{matrix} \text{Cr1} & \text{Cr2} & & \text{Crj} & & \text{Crn} \end{matrix} \\ \begin{pmatrix} x_{11} & x_{12} & \dots & x_{1j} & \dots & x_{1n} \\ x_{21} & x_{22} & \dots & x_{2j} & \dots & x_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ x_{i1} & x_{i2} & \dots & x_{ij} & \dots & x_{in} \\ \vdots & \vdots & & \vdots & & \vdots \\ x_{m1} & x_{m2} & \dots & x_{mj} & \dots & x_{mn} \end{pmatrix} \end{array} \begin{matrix} \\ \text{Alternativa 1} \\ \text{Alternativa 2} \\ \vdots \\ \text{Alternativa i} \\ \vdots \\ \text{Alternativa m} \end{matrix} \tag{4.5}$$

Onde:

Alternativa $i = i_{\text{nésima}}$ alternativa considerada;

x_{ij} = resultado numérico da $i_{\text{nésima}}$ alternativa em relação ao $j_{\text{nésimo}}$ critério

Etapa 1 - Construir a matriz de decisão normalizada: este processo tenta transformar as várias dimensões dos atributos em atributos não dimensionais, o que permite a comparação entre os atributos.

$$r_{ij} = \frac{x_{ij}}{\sqrt{\sum_{i=1}^{m} x_{ij}^2}} \tag{4.6}$$

onde r_{ij} é a classificação do critério normalizado.

Etapa 2 - Construir a matriz de decisão normalizada ponderada. O conjunto de pesos $(w_1, w_2, w_j..., w_n)$, o qual seu somatório deve ser igual a 1. Ele é utilizado para ponderar o desempenho das alternativas em cada critério de acordo com seu grau de importância normalizado.

$$V = \begin{bmatrix} v_{11} & v_{12} & \dots & v_{1j} & \dots & v_{1n} \\ \vdots & \vdots & & \vdots & & \vdots \\ v_{i1} & v_{i2} & \dots & v_{ij} & \dots & v_{in} \\ \vdots & \vdots & & \vdots & & \vdots \\ v_{m1} & v_{m2} & \dots & v_{mj} & \dots & v_{mn} \end{bmatrix} = \begin{bmatrix} w_1 v_{11} & w_2 v_{12} & \dots & w_j v_{1j} & \dots & w_n v_{1n} \\ \vdots & \vdots & & \vdots & & \vdots \\ w_1 v_{i1} & w_2 v_{i2} & \dots & w_j v_{ij} & \dots & w_n v_{in} \\ \vdots & \vdots & & \vdots & & \vdots \\ w_1 v_{m1} & w_2 v_{m2} & \dots & w_j v_{mj} & \dots & w_n v_{mn} \end{bmatrix} \tag{4.7}$$

Etapa 3 - Determinar as soluções ideais positivas e negativas do seguinte modo:

considere duas alternativas postiças A^+ e A^-, as quais se propõem a representar, respectivamente, a alternativa de maior e menor preferência em cada critério. As alternativas são definidas por:

$$A^+ = \{(max\ v_{ij} \mid j \in J), (min\ v_{ij} \mid j \in J')\} = \left\{v_1^+, v_2^+, ..., v_j^+, ..., v_n^+\right\} \tag{4.8}$$

$$A^- = \{(min\ v_{ij} \mid j \in J), (max\ v_{ij} \mid j \in J')\} = \left\{v_1^-, v_2^-, ..., v_j^-, ..., v_n^-\right\} \tag{4.9}$$

onde:

J é o universo de critérios de benefícios

J' é o universo de critérios de custo

Etapa 4 - Calcular as distâncias euclidianas de cada alternativa a partir da solução ideal positiva e da solução ideal negativa da seguinte forma:

$$S_i^+ = \sqrt{\sum_{j=1}^{n}(V_{ij} - V_j^+)^2}, \qquad i = 1, 2, ..., m \tag{4.10}$$

$$S_i^- = \sqrt{\sum_{j=1}^{n}(V_{ij} - V_j^-)^2}, \qquad i = 1, 2, ..., m \tag{4.11}$$

Etapa 5 - Calcular a proximidade relativa de cada alternativa para a solução ideal da seguinte forma:

$$C_{i+} = \frac{S_{i-}}{(S_{i+} + S_{i-})}, \qquad 0 < C_{i+} < 1 \tag{4.12}$$

Etapa 6 - Classificar as alternativas de acordo com a ordem decrescente de seus coeficientes de proximidade relativa. Quanto maior for o C_{i+}, mais desejável será a alternativa. A melhor alternativa é aquela com maior proximidade relativa da solução ideal.

O método é bastante difundido como pode ser observado na aplicação realizada pelos autores (215), os quais utilizaram o método para classificar alternativas, além de sugerir algumas vantagens quanto ao seu uso:

- É simples de usar.
- Leva em consideração todos os tipos de critérios (subjetivos e objetivo).
- É racional e compreensível.
- Os processos de computação são diretos.
- O conceito permite a busca do melhor critério alternativo representado em uma forma matemática simples.
- Capacidade de identificar a melhor alternativa rapidamente (216).

A revisão da literatura demonstrou, também, que o TOPSIS pode ser utilizado com o AHP de forma híbrida (217) e (218), combinação AHP-TOPSIS, a qual possibilita a transformação de uma análise qualitativa em uma análise quantitativa. O uso do TOPSIS em conjunto com o AHP permite a comparação emparelhada de um maior número de alternativas, além de usar os pesos dos critérios encontrados com o AHP para gerar uma ordem de alternativas (209) a serem utilizadas como entrado no TOPSIS.

Em vista disso, o uso de ambos métodos resulta em mais equilíbrio na avaliação, orquestrando as alternativas em relação aos dois pontos de referência: solução ideal positiva (PIS), ou ponto ideal, e mais distante da solução ideal negativa (NIS), cujas distâncias

devem ser minimizadas e maximizadas, respectivamente (219). Dessa maneira, a combinação AHP-TOPSIS fornece um suporte de decisão mais preciso em campos que requerem múltiplas visualizações e considerações (220).

Por fim, a avaliação de riscos no contexto desse trabalho é realizada por uma proposta de metodologia, com adaptações. Essa metodologia utiliza FMEA com as técnicas de Tomada de Decisão Multicritério (MCDM) AHP e TOPSIS. Ambas técnicas MCDM podem ser combinadas para fornecer um suporte de decisão mais preciso em campos que requerem múltiplas visualizações e considerações (220), cenário ilustrado pelo caso concreto dos especialistas responsáveis pela aplicação do FMEA na alçada do CMI, por consenso.

Assim, a escolha dessas técnicas é fundamentada em pesquisas realizadas, as quais identificaram a combinação da aplicação do FMEA em conjunto com o AHP e TOPSIS (221), (202) e (222), caracterizando-se a hibridização das técnicas. O FMEA para realizar a Análise dos Riscos e AHP ((135), (167), (168) e (206)) e TOPSIS (212) para Avaliação de Riscos, conforme pode ser observado na Figura 4.10.

Metodologia - Modelo FMEA modificado proposto com base no AHP e TOPSIS

Os próximos passos buscam detalhar as atividades realizadas para cada um dos passos propostos para os métodos (FMEA, AHP e TOPSIS) utilizados na metodologia, de acordo com a Figura 4.10, a qual segue:

FMEA - Passo 1 - Matriz de decisão.

O passo 1 da aplicação do FMEA resulta na Matriz de decisão com a aplicação dos pontos de 1 até 10 para S, O e D de cada risco identificado, ou seja, serão analisados os 38 eventos elencados na fase de identificação dos riscos.

FMEA - Passo 2 - Normalização da matriz de decisão e determinar os critérios Max ou Min

O segundo passo da metodologia compreende a realização da normalização da matriz de decisão, além de determinar se os critérios são tipo máximo ou mínimo. Nessa etapa é realizada uma análise quanto a importância dos critérios severidade, ocorrência e detecção em relação ao impacto no ativo banco de dados. Essa informação será utilizada nos passos 1 e 2 do TOPSIS.

AHP - Passo 3 - Cálculo dos pesos critérios: S, O e D

Para o passo 3 da metodologia o AHP foi adotado para coletar a sensibilidade da equipe multidisciplinar de especialistas do CMI, a fim de determinar e calcular os pesos de normalização para os três fatores de riscos (critérios) S, O e D (206), (209), (210) e (211). Dessa forma, serão calculadas as categorias de impactos com o método AHP para os critérios severidade, ocorrência e detecção (206). Assim, devem ser calculados:

- Pesos de importância (*Eigen Vetor*).
- Razão de consistência.
- Índice de consistência.

Ao considerar os pesos de impacto dos critérios no AHP (S, O e D), cálculo resultante do Vetor de Eigen, o resultado obtido será utilizado para realizar os cálculos dos valores de distância ideal e pior, os quais compõem as etapas 1 e 2 do TOPSIS (206), (209), (210) e (211), passo 4 da metodologia.

TOPSIS – Passo 4 - Cálculo dos valores de distância ideal e pior.

A técnica de ordenar as preferências com base na similaridade com as soluções ideais (TOPSIS), como pode ser facilmente inferido do nome, adiciona duas alternativas artificiais à lista de preferências, usando os valores máximo e mínimo de cada critério e atribui os valores máximos e mínimos às preferências ideais e anti-ideais, respectivamente. Assim, as soluções ideal e anti-ideal devem ser compostas por números máximo e mínimo em cada critério, de maneira respectiva, quando um critério é de natureza negativa (ou seja, quanto menor for o número, mais ele é arriscado na perspectiva gerencial) (223). Desse jeito, essa etapa realiza o cálculo dos valores de distância ideal e pior. Corresponde as etapas 1 e 2 do método TOPSIS.

TOPSIS – Passo 5 - Melhor e pior métrica.

Realiza o cálculo da melhor e pior métrica. Para esse fim, o cálculo leva em consideração os valores de cada riscos para severidade, ocorrência e detecção. A melhor métrica busca valores, os quais sejam o mais próximo de zero. E a pior métrica considera o maior valor dentre o range dos riscos. Para esse cálculo, são considerados os 38 riscos identificados e corresponde às etapas 3 do método TOPSIS.

TOPSIS – Passo 6 - Coeficiente de Similaridade (S).

Realiza cálculo do coeficiente de similaridade. Para esse fim, o cálculo leva em consideração o resultado da melhor e pior métrica. Corresponde às etapas 4 e 5 do método TOPSIS.

TOPSIS – Passo 7 - Ranquear.

Realiza o ranqueamento dos modos de falha, riscos, a partir do resultado do coeficiente de similaridade. Corresponde à etapa 6 do método TOPSIS.

As próximas etapas são inerentes a realização e aplicação da metodologia proposta, de acordo com a Figura 4.10.

Aplicação da metodologia – Resultados obtidos.

Passo 1 - Aplicação do FMEA: Matriz de decisão.

A seguir serão listados os riscos elicitados ao considerar cada categoria identificada durante a etapa de identificação dos riscos, conforme segue:

Ataques de injeção: utiliza-se de falhas de segurança em sistemas, os quais possuem interação com bases de dados, para inserção de código malicioso apoiado em comandos SQL (Quadro 7).

Quadro 7: Ataques de injeção.

ID Risco	Evento	Efeito	Causa
R01-AI	Uso inadequado de instruções.	Injeção de SQL.	Desenvolvedores de software criam consultas dinâmicas de banco de dados as quais incluem entradas fornecidas pelo usuário.
R02-AI	Procedimentos inadequados armazenados.	Injeção de SQL.	Procedimentos armazenados não estão protegidos contra injeção, pois as instruções SQL com parâmetros não são parametrizadas automaticamente.
R03-AI	Inadequado uso de escape de entrada.	Vulnerabilidades de injeção de SQL.	Ambiguidade entre os dados de entrada do usuário com o código SQL escrito pelo desenvolvedor.
R04-AI	Não validar lista de permissões.	Injeção de SQL.	Falta de validação relacionada a consultas SQL, as quais podem fazer uso de variáveis de ligação, como nomes de tabelas ou colunas e o indicador de ordem de classificação (ASC ou DESC).

Banco de Dados vulneráveis: relacionada a fragilidades do SGBD, das quais podem variar desde sua configuração até o mau uso por parte de administradores de banco de dados (Quadro 8).

Quadro 8: BD vulneráveis.

ID Risco	Evento	Efeito	Causa
R05-BDV	Inadequado uso de acesso à rede.	Invasão a base de dados.	Configuração com permissão para o BD ter acesso à rede.
R06-BDV	Inadequada configuração de acesso.	Invasão a base de dados.	BD com acesso a host não locais, além de hosts comuns com regras frágeis de firewall.
R07-BDV	Configuração de Banco de Dados inadequada.	Invasão a base de dados.	BD permitir conexões que não sejam criptografadas.
R08-BDV	Falta de um certificado digital confiável no servidor.	Invasão a base de dados.	BD sem verificação de confiabilidade de certificado digital.
R09-BDV	Inadequado uso de contas e Bancos de Dados padrão.	Invasão a base de dados.	Falta de contas de usuário e instalações de SGBD configurados como padrão.

Dados confidenciais: caracteriza-se pela criticidade dos dados, dos quais são armazenados no SGBD. A LGPD (23), assim como GDPR (171), preveem a proteção e tratamento dos dados (Quadro 9).

Quadro 9: Dados confidenciais.

ID Risco	Evento	Efeito	Causa
R10-DC	Inadequado uso de procedimentos de autenticação.	Acesso indevido a dados confidenciais, além de possibilidade de acionamento via órgão regulador.	Falta de Procedimentos de autenticação para garantir que a pessoa que faz uma solicitação de acesso ao seu os dados pessoais são, de fato, o titular dos dados relevante.
R11-DC	Inadequado uso de identificadores de titulares de dados.	Possibilidade de uso indevido de dados pessoais.	Falta de mecanismos para manter detalhes sobre todos os identificadores de titulares de dados usados nos sistemas da organização.
R12-DC	Permitir localizar todos os dados pessoais.	Não atender a requisição do titular do dado, além de possibilidade de acionamento via órgão regulador.	Falta de mecanismos para localizar todos os dados pessoais mantidos no banco de dados da organização relativos a um único indivíduo.
R13-DC	Inadequado uso de dados que identificam o titular.	Não atender a requisição do titular do dado, além da possibilidade de acionamento via órgão regulador.	Falta de mecanismos para manter detalhes sobre quais dados identificam o titular dos dados e em qual contexto ele se encontra.
R14-DC	Permitir rastreabilidade de dados pessoais.	Não atender a requisição do titular do dado, além da possibilidade de acionamento via órgão regulador.	Falta de mecanismos para exclusão de informações e links, os quais permitem que os indivíduos sejam identificados.

ID Risco	Evento	Efeito	Causa
R15-DC	Inadequado uso de consentimentos dos titulares dos dados.	Não atender a requisição do titular do dado, além da possibilidade de acionamento via órgão regulador.	Falta de mecanismos para manter detalhes sobre os consentimentos dos titulares dos dados para processar seus dados pessoais, transferir suas informações para outras instituições ou publicar os dados pessoais na web.
R16-DC	Não distinguir dados pessoais.	Não atender a requisição do titular do dado, além da possibilidade de acionamento via órgão regulador.	Falta de mecanismos para distinguir dados pessoais entre sensíveis e não sensíveis e quais são processados para fins de pesquisa.
R17-DC	Permitir a rastreabilidade de manipulação de dados.	Perda de confiança na manutenabilidade dos dados pessoais, além de possibilidade de acionamento via órgão regulador.	Falta de rastreabilidade relativa as pessoas autorizadas a manipular os dados pessoais, as funções dos usuários autorizados dentro da organização, as fontes dos dados pessoais e as solicitações de acesso do titular dos dados.
R18-DC	Não ter transparência quanto ao objetivo do uso de dados dos titulares.	Não atender a requisição do titular do dado, além da possibilidade de acionamento via órgão regulador.	Falta de detalhes relativos aos objetivos do processo de armazenamento dos dados dos titulares dos dados.

Fator humano: relaciona-se a falhas de segurança. O invasor explora o fator humano, a fim de identificar senhas, dados, informações, dentre outras para completar o ataque (Quadro 10).

Quadro 10: Fator Humano.

ID Risco	**Evento**	**Efeito**	**Causa**
R19-FH	Não definir um programa de conscientização de segurança.	Possibilidade de ataque por engenharia social.	Estabelecer e manter um programa de conscientização de segurança.
R20-FH	Inadequada proteção contra ataques de engenharia social.	Possibilidade de ataque por engenharia social.	Falta de treinamentos para os membros da força de trabalho com o intuito de reconhecer ataques de engenharia social.
R21-FH	Não treinar a força de trabalho.	Possibilidade de ataque por engenharia social.	Falta de treinamento dos membros da força de trabalho nas melhores práticas de autenticação, melhores práticas de tratamento de dados, em relação as causas da exposição não intencional de dados, no reconhecimento e comunicação de incidentes de segurança e na identificação e comunicação se o se o ativo Banco de Dados corporativos está faltando atualizações de segurança.
R22-FH	Inadequadas competências e conscientização de segurança.	Possibilidade de ataque por engenharia social.	Falta de conduzir treinamento de competências e conscientização de segurança para funções específicas, além de os perigos ao se conectar e transmitir dados corporativos em redes inseguras.

Trilha de auditória: relaciona-se pela falta de mapeamento e acompanhamento de atividades que afetam um determinado conjunto de informações (Quadro 11)

Quadro 11: Trilha de auditória.

ID Risco	Evento	Efeito	Causa
R23-TA	Não auditar os processos de dados pessoais.	Falha de segurança relativa a rastreabilidade de alterações, exclusões e/u inclusões, além de ação movida pelos órgãos competentes.	Falta de auditar os processos de dados pessoais para garantir que a notificação cobre adequadamente as atividades de processamento.
R24-TA	Uso indevido de dados pessoais.	Falha de segurança relativa a rastreabilidade de alterações, exclusões e/u inclusões, além de ação movida pelos órgãos competentes.	Falta de implantação de mecanismos para garantir que o uso indevido de dados pessoais dentro da organização pode ser identificados e remediados.
R25-TA	Não restringir o processamento de dados pessoais.	Falha de segurança relativa a rastreabilidade de alterações, exclusões e/u inclusões, além de ação movida pelos órgãos competentes.	Falta de restrições para realização do processamento de dados pessoais não relacionados com as atividades da organização usando os recursos da organização.

Segurança de dados: relaciona-se à proteção das informações, das quais são compartilhadas. No Brasil, por exemplo, existe o Decreto nº 10.046 (177), além das Normas ISO 27005 (2018) (181) e 27001 (2013) (178) relacionadas à segurança de dados (Quadro 12).

Quadro 12: Segurança de Dados.

ID Risco	Evento	Efeito	Causa
R26-SD	Não permite divulgações ilegais de dados.	Divulgação ilegal de dados pessoais, além de acionamento a partir de órgãos de controle.	Não existência de garantia que o banco de dados não permite divulgações ilegais de dados pessoais.
R27-SD	Inadequado uso de solicitação de dados pessoais de outra pessoa.	Divulgação ilegal de dados pessoais, com possível acionamento a partir de órgãos de controle.	Não existência de garantir que quando alguém solicitar dados pessoais sobre outra pessoa, tais dados devem ser apenas divulgados, e na medida em que, requer os dados para o desempenho de suas funções oficiais.
R28-SD	Permitir a divulgação de dados pessoais errados.	Divulgação ilegal de dados pessoais, com possível acionamento a partir de órgãos de controle.	Não existência de garantia de que nenhum dado pessoal de outro titular de dados seja divulgado, quando um titular de dados solicitar para acessar seus registros pessoais.
R29-SD	Não implantar técnicas de segurança para proteger os dados de ataques.	Divulgação ilegal de dados pessoais, acionamento a partir de órgãos de controle.	Não existência de garantias de implantação de técnicas de segurança para proteger os dados de ataques eletrônicos internos e externos.
R30-SD	Falta de método seguro de transmissão.	Divulgação ilegal de dados pessoais, acionamento a partir de órgãos de controle.	Garantir o fornecimento de um método seguro de transmissão, quando os dados pessoais são coletados ou processados online.

ID Risco	Evento	Efeito	Causa
R31-SD	Não exclusão permanentemente os dados.	Acionamento a partir de órgãos de controle.	Não existência de garantir a correção e exclusão permanentemente dos dados, além da exclusão automática dos dados pessoais, quando o tempo de retenção expirar.
R32-SD	Não mesclar bancos de dados e integrar fontes de informação.	Armazenar dados pessoais sem a autorização do titular com possibilidade de acionamento a partir dos órgãos competentes.	Mesclar bancos de dados e integrar fontes de informação usando correspondências completas de todos os critérios, além de manter arquivos de papel digitalizados e outros arquivos de computador separados de bancos de dados, que contêm dados pessoais (por exemplo, bancos de dados multimídia) sem a autorização dos titulares.
R33-SD	Não alterar os sistemas de hardware e software da organização.	Perda na precisão dos dados e integridade.	Faltar de atualização de sistemas de hardware e software da organização, com isso evitariasse a perda na precisão dos dados e integridade.
R34-SD	Falta de arquivos de backup.	Perda de arquivos.	Faltar de garantir a realização de backup de arquivos.

Controle de acesso: remete-se ao nível de permissão para acessar as informações armazenadas na base de dados (Quadro 13).

Quadro 13: Controle de acesso.

ID Risco	Evento	Efeito	Causa
R35-CA	Não definir processo de concessão de acesso.	Acesso indevido aos dados da base de dados.	Falta de controles para concessão de acesso aos ativos corporativos mediante concessão de direitos ou mudança de função de um usuário.
R36-CA	Não definir um processo de revogação de acesso.	Acesso indevido aos dados da base de dados.	Falta de controles para revogar o acesso aos ativos corporativos, por meio da desativação de contas imediatamente após o encerramento, revogação de direitos ou mudança de função de um usuário.
R37-CA	Não implantar Múltiplo Fator de Autenticação (MFA) para aplicações expostas externamente.	Aplicações corporativas ou de terceiros expostas externamente sem aplicar o MFA.	Falta de implantação de MFA.
R38-CA	Não inventariar os sistemas de autenticação e autorização.	Sistemas de autenticação e autorização da empresa, incluindo aqueles hospedados no site local ou em um provedor de serviços remoto sem invetário e categorização de ativo.	Falta de política relacionada a inventário de sistemas.

Ao término da fase de Identificação dos Riscos, foi possível realizar a análise dos 38 eventos relacionados ao Ativo Banco de Dados, a partir do consenso da equipe de

especialistas. Para cada evento foi considerada a severidade, a ocorrência e o quanto o evento pode ser detectado. A Tabela 4.3 consolida os modos de falhas dos 38 riscos identificados, quanto a severidade, ocorrência e detecção.

É possível observar na Tabela 4.3 que o RPN não foi calculado com o FMEA tradicional utilizado nessa pesquisa devido a possibilidade da existência de subjetividade quanto ao ranqueamento dos riscos, pois as influências ambientais produzidas por falhas técnicas, erros e deficiências podem ser ignoradas no RPN convencional (224) e (225). A necessidade de aprimoramento do mecanismo e método de cálculo da classificação dos modos de falha para tornar seus resultados mais razoáveis e eficazes (226), quanto ao ranqueamento dos 38 eventos identificados, é suprimida pela metodologia proposta na Figura 4.10 (Modelo FMEA modificado proposto com base no AHP e TOPSIS). O próximo estágio consiste na normalização da matriz, formada pelos dados da Tabela 4.4, e definição dos critérios.

Passo 2 – FMEA: Normalização da matriz e critérios Max e Min.

O passo 2 da metodologia foi realizado a partir da aplicação na normalização da matriz estabelecida pelos dados da Tabela 4.3. Os resultados são os seguintes:

- **Severidade**: 53,8702144
- **Ocorrência**: 12,92284798
- **Detecção**: 33,28663395

Quanto a determinação, se os critérios são do tipo máximo ou mínimo, fundada na análise realizada, os resultados são os seguintes:

- **Severidade**: Max
- **Ocorrência**: Max
- **Detecção**: Max

A etapa subsequente consiste na aplicação do AHP para cálculo dos pesos.

Passo 3 – AHP: Cálculo dos pesos critérios: S, O e D.

A terceira etapa consiste em identificar os pesos relacionados aos critérios: S, O e D. Para esse fim, o método AHP foi empregado e a aplicação consistiu nos mesmos passos elencados durante a Fase 2, hierarquização de critérios e alternativas. A Tabela 4.4 apresenta o resultado da percepção dos especialistas.

Fonte: Saaty (1980) (135) (adaptado).

Os próximos passos são relativos ao cálculo do Vetor de Eigen, razão de consistência e índice de consistência, os quais seguem:

1. **Pesos de importância** - Vetor de Eigen.

Tabela 4.3: Modos de falhas inerentes aos riscos.

Riscos	**Severidade**	**Ocorrência**	**Detecção**
R01-AI	7	3	9
R02-AI	6	3	9
R03-AI	10	3	9
R04-AI	7	3	8
R05-BDV	8	2	3
R06-BDV	6	2	7
R07-BDV	8	2	2
R08-BDV	10	2	1
R09-BDV	7	2	1
R10-DC	7	1	3
R11-DC	9	1	2
R12-DC	8	1	2
R13-DC	8	2	3
R14-DC	8	1	1
R15-DC	9	2	1
R16-DC	10	1	2
R17-DC	10	4	7
R18-DC	9	2	2
R19-FH	10	3	9
R20-FH	9	2	7
R21-FH	10	1	8
R22-FH	8	1	7
R23-TA	9	2	7
R24-TA	9	1	7
R25-TA	10	1	6
R26-SD	10	1	9
R27-SD	10	1	7
R28-SD	10	1	6
R29-SD	10	1	3
R30-SD	10	1	2
R31-SD	9	1	3
R32-SD	10	3	3
R33-SD	9	4	2
R34-SD	9	1	1
R35-CA	10	2	2
R36-CA	9	4	8
R37-CA	6	1	2
R38-CA	2	2	2

Fonte: FMEA (198) (adaptado).

Tabela 4.4: Critérios com a percepção dos especialistas.

Critérios	**Severidade**	**Ocorrência**	**Detecção**
Severidade	1,000	0,333	0,500
Ocorrência	3,000	1,000	3,000
Detecção	2,000	0,333	1,000
Soma	6,000	1,667	4,500
Peso Coluna	0,493	0,137	0,370

- **Severidade**:0,159
- **Ocorrência**:0,589
- **Detecção**: 0,252

2. **Razão de consistência**: 0,046
3. **Índice de consistência**: 0,026

De acordo com os resultados do AHP com razão de consistência de 0,046 os pesos de importância foram calculados e identificados (0,159; 0,589 e 0,252) para severidade, ocorrência e detecção, nesta ordem. Como o índice de consistência é inferior a 0,10% (135), os cálculos são elegíveis para uso em avaliações, por consequência, a etapa seguinte consiste na aplicação do TOPSIS. Os valores identificados com o cálculo dos pesos, assim como na normalização, serão utilizados para realização dos cálculos dos valores de distância ideal e pior.

Passo 4 – TOPSIS: Cálculo dos valores de distância ideal e pior.

Decorrente dos cálculos realizados no passo 3 é possível realizar o cálculo dos valores de distância ideal e pior (equações 4.8 e 4.9). A Tabela 4.5 apresenta o resultado dos cálculos realizados, valores ideal e pior para os 38 modos de falha.

Por sua vez, a etapa seguinte consiste em apresentar o cálculo da melhor e pior métrica.

Passo 5 – TOPSIS: Melhor e pior métrica.

O passo 5 consiste no cálculo da melhor e pior métrica. O cômputo considera os valores de S, O e D para cada risco identificado (equações 4.10 e 4.11) e o resultado da aplicação pode ser observado na Tabela 4.6.

O resultado alcançado para cada valor inerente a melhor e pior métrica é a entrada para o cálculo da etapa seguinte: cálculo de similaridade.

Tabela 4.5: Cálculo dos valores de distância ideal e pior.

Riscos	Severidade	Ocorrência	Detecção
R01-AI	0,020660768	0,136734565	0,068135457
R02-AI	0,01770923	0,136734565	0,068135457
R03-AI	0,029515383	0,136734565	0,068135457
R04-AI	0,020660768	0,136734565	0,06056485
R05-BDV	0,023612306	0,091156377	0,022711819
R06-BDV	0,01770923	0,091156377	0,052994244
R07-BDV	0,023612306	0,091156377	0,015141213
R08-BDV	0,029515383	0,091156377	0,007570606
R09-BDV	0,020660768	0,091156377	0,007570606
R10-DC	0,020660768	0,045578188	0,022711819
R11-DC	0,026563845	0,045578188	0,015141213
R12-DC	0,023612306	0,045578188	0,015141213
R13-DC	0,023612306	0,091156377	0,022711819
R14-DC	0,023612306	0,045578188	0,007570606
R15-DC	0,026563845	0,091156377	0,007570606
R16-DC	0,029515383	0,045578188	0,015141213
R17-DC	0,029515383	0,182312754	0,052994244
R18-DC	0,026563845	0,091156377	0,015141213
R19-FH	0,029515383	0,136734565	0,068135457
R20-FH	0,026563845	0,091156377	0,052994244
R21-FH	0,029515383	0,045578188	0,06056485
R22-FH	0,023612306	0,045578188	0,052994244
R23-TA	0,026563845	0,091156377	0,052994244
R24-TA	0,026563845	0,045578188	0,052994244
R25-TA	0,029515383	0,045578188	0,045423638
R26-SD	0,029515383	0,045578188	0,068135457
R27-SD	0,029515383	0,045578188	0,052994244
R28-SD	0,029515383	0,045578188	0,045423638
R29-SD	0,029515383	0,045578188	0,022711819
R30-SD	0,029515383	0,045578188	0,015141213
R31-SD	0,026563845	0,045578188	0,022711819
R32-SD	0,029515383	0,136734565	0,022711819
R33-SD	0,026563845	0,182312754	0,015141213
R34-SD	0,026563845	0,045578188	0,007570606
R35-CA	0,029515383	0,091156377	0,015141213
R36-CA	0,026563845	0,182312754	0,06056485
R37-CA	0,01770923	0,045578188	0,015141213
R38-CA	0,005903077	0,091156377	0,007570606
Ideal	0,029515383	0,182312754	0,068135457
Pior	0,005903077	0,045578188	0,007570606

Fonte: TOPSIS (212) (adaptado).

Tabela 4.6: Melhor e pior métrica.

Riscos	Severidade	Ocorrência	Detecção	Melhor Métrica	Pior Métrica
R01-AI	0,020660768	0,136734565	0,068135457	0,046430329	0,110432674
R02-AI	0,01770923	0,136734565	0,068135457	0,047082444	0,110077116
R03-AI	0,029515383	0,136734565	0,068135457	0,045578188	0,111960382
R04-AI	0,020660768	0,136734565	0,06056485	0,047043486	0,106469077
R05-BDV	0,023612306	0,091156377	0,022711819	0,102017833	0,051188323
R06-BDV	0,01770923	0,091156377	0,052994244	0,093156463	0,065422193
R07-BDV	0,023612306	0,091156377	0,015141213	0,105606445	0,049480321
R08-BDV	0,029515383	0,091156377	0,007570606	0,109442159	0,051331396
R09-BDV	0,020660768	0,091156377	0,007570606	0,109799774	0,047907836
R10-DC	0,020660768	0,045578188	0,022711819	0,144353914	0,021143457
R11-DC	0,026563845	0,045578188	0,015141213	0,146674615	0,022004123
R12-DC	0,023612306	0,045578188	0,015141213	0,146763679	0,019259566
R13-DC	0,023612306	0,091156377	0,022711819	0,102017833	0,051188323
R14-DC	0,023612306	0,045578188	0,007570606	0,149663919	0,01770923
R15-DC	0,026563845	0,091156377	0,007570606	0,109481951	0,050042368
R16-DC	0,029515383	0,045578188	0,015141213	0,146644915	0,024796272
R17-DC	0,029515383	0,182312754	0,052994244	0,015141213	0,146004072
R18-DC	0,026563845	0,091156377	0,015141213	0,105482636	0,050611784
R19-FH	0,029515383	0,136734565	0,068135457	0,045578188	0,111960382
R20-FH	0,026563845	0,091156377	0,052994244	0,092452436	0,067583618
R21-FH	0,029515383	0,045578188	0,06056485	0,136943986	0,058016643
R22-FH	0,023612306	0,045578188	0,052994244	0,137696928	0,048753704
R23-TA	0,026563845	0,091156377	0,052994244	0,092452436	0,067583618
R24-TA	0,026563845	0,045578188	0,052994244	0,137601996	0,049901645
R25-TA	0,029515383	0,045578188	0,045423638	0,138607965	0,044613821
R26-SD	0,029515383	0,045578188	0,068135457	0,136734565	0,065004939
R27-SD	0,029515383	0,045578188	0,052994244	0,137570337	0,051194217
R28-SD	0,029515383	0,045578188	0,045423638	0,138607965	0,044613821
R29-SD	0,029515383	0,045578188	0,022711819	0,144082088	0,028049908
R30-SD	0,029515383	0,045578188	0,015141213	0,146644915	0,024796272
R31-SD	0,026563845	0,045578188	0,022711819	0,144112316	0,025614911
R32-SD	0,029515383	0,136734565	0,022711819	0,064348101	0,095374432
R33-SD	0,026563845	0,182312754	0,015141213	0,053076374	0,138493764
R34-SD	0,026563845	0,045578188	0,007570606	0,149576582	0,020660768
R35-CA	0,029515383	0,091156377	0,015141213	0,105441334	0,051886668
R36-CA	0,026563845	0,182312754	0,06056485	0,008125617	0,148093209
R37-CA	0,01770923	0,045578188	0,015141213	0,147119395	0,014024954
R38-CA	0,005903077	0,091156377	0,007570606	0,111960382	0,045578188
Ideal	0,029515383	0,182312754	0,068135457	0	0,151400077
Pior	0,005903077	0,045578188	0,007570606	0,151400077	0

Fonte: TOPSIS (212) (adaptado).

Passo 6 – TOPSIS: Coeficiente de similaridade (S).

O cálculo do coeficiente de similaridade utiliza como entrada de dado as informações da melhor e pior métrica relativa a cada risco elencado (equação 12). O resultado pode ser observado na Tabela 4.7.

O resultado atingido para cada valor inerente ao coeficiente de similaridade é utilizado para realização do ranqueamento dos métodos de falha, riscos, os quais podem ser observados no próximo passo.

Passo 7 – TOPSIS: Ranquear

A última etapa da metodologia proposta consiste no ranqueamento dos 38 riscos identificados, realizado a partir do resultado do cálculo do coeficiente de similaridade, o qual pode ser observado na Tabela 4.8 - Modos de falha ranqueados, que apresenta o ranque dos 38 riscos identificados ordenados pela coluna “Ranque -TOPSIS” de forma crescente.

Tabela 4.7: Coeficiente de similaridade.

Riscos	Severidade	Ocorrência	Detecção	Coeficiente de Similaridade (S)
R01-AI	0,020660768	0,136734565	0,068135457	0,704007139
R02-AI	0,01770923	0,136734565	0,068135457	0,700416291
R03-AI	0,029515383	0,136734565	0,068135457	0,710685527
R04-AI	0,020660768	0,136734565	0,06056485	0,693552861
R05-BDV	0,023612306	0,091156377	0,022711819	0,334114009
R06-BDV	0,01770923	0,091156377	0,052994244	0,412553586
R07-BDV	0,023612306	0,091156377	0,015141213	0,319049279
R08-BDV	0,029515383	0,091156377	0,007570606	0,31927761
R09-BDV	0,020660768	0,091156377	0,007570606	0,30377631
R10-DC	0,020660768	0,045578188	0,022711819	0,127757057
R11-DC	0,026563845	0,045578188	0,015141213	0,130449889
R12-DC	0,023612306	0,045578188	0,015141213	0,116005239
R13-DC	0,023612306	0,091156377	0,022711819	0,334114009
R14-DC	0,023612306	0,045578188	0,007570606	0,105806874
R15-DC	0,026563845	0,091156377	0,007570606	0,313697423
R16-DC	0,029515383	0,045578188	0,015141213	0,144634274
R17-DC	0,029515383	0,182312754	0,052994244	0,90603999
R18-DC	0,026563845	0,091156377	0,015141213	0,324238265
R19-FH	0,029515383	0,136734565	0,068135457	0,710685527
R20-FH	0,026563845	0,091156377	0,052994244	0,422302453
R21-FH	0,029515383	0,045578188	0,06056485	0,297581329
R22-FH	0,023612306	0,045578188	0,052994244	0,26148318
R23-TA	0,026563845	0,091156377	0,052994244	0,422302453
R24-TA	0,026563845	0,045578188	0,052994244	0,26613694
R25-TA	0,029515383	0,045578188	0,045423638	0,243496266
R26-SD	0,029515383	0,045578188	0,068135457	0,322222161
R27-SD	0,029515383	0,045578188	0,052994244	0,271206728
R28-SD	0,029515383	0,045578188	0,045423638	0,243496266
R29-SD	0,029515383	0,045578188	0,022711819	0,162955804
R30-SD	0,029515383	0,045578188	0,015141213	0,144634274
R31-SD	0,026563845	0,045578188	0,022711819	0,1509181
R32-SD	0,029515383	0,136734565	0,022711819	0,597125717
R33-SD	0,026563845	0,182312754	0,015141213	0,722940253
R34-SD	0,026563845	0,045578188	0,007570606	0,121364483
R35-CA	0,029515383	0,091156377	0,015141213	0,329799321
R36-CA	0,026563845	0,182312754	0,06056485	0,947985671
R37-CA	0,01770923	0,045578188	0,015141213	0,087033482
R38-CA	0,005903077	0,091156377	0,007570606	0,289314473
Ideal	0,029515383	0,182312754	0,068135457	1
Pior	0,005903077	0,045578188	0,007570606	0

Fonte: TOPSIS (212) (adaptado).

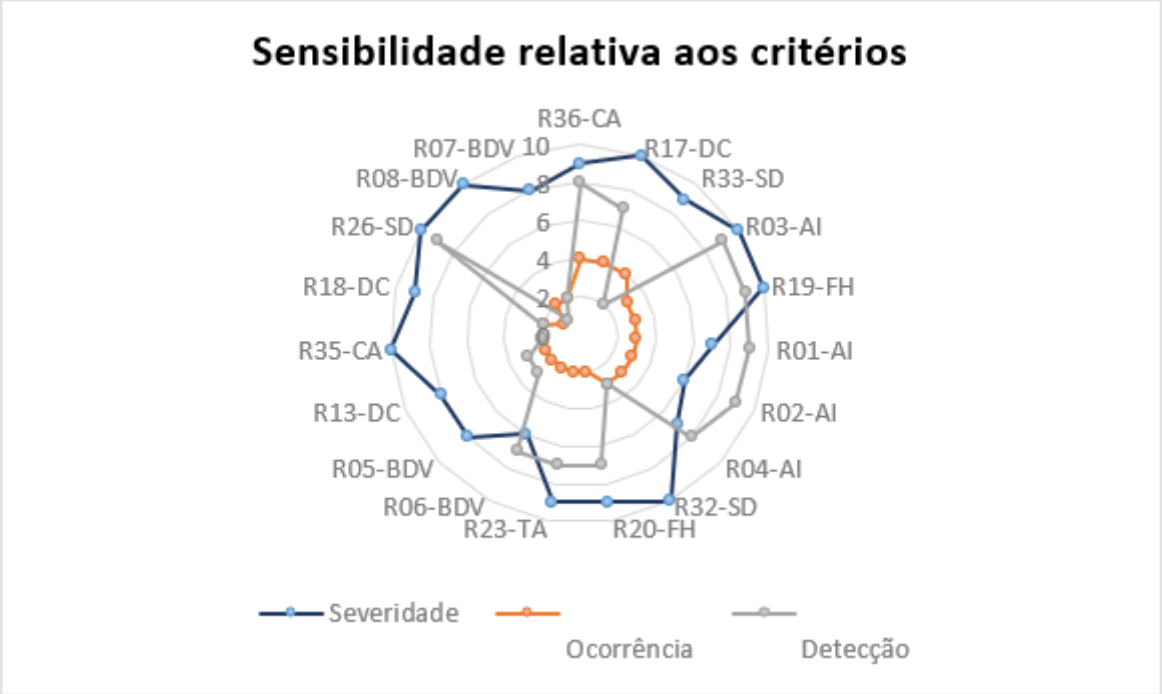
Tabela 4.8: Modos de falha ranqueados.

Riscos	**Ranque -TOPSIS**
R36-CA	1
R17-DC	2
R33-SD	3
R03-AI	4
R19-FH	4
R01-AI	6
R02-AI	7
R04-AI	8
R32-SD	9
R20-FH	10
R23-TA	10
R06-BDV	12
R05-BDV	13
R13-DC	13
R35-CA	15
R18-DC	16
R26-SD	17
R08-BDV	18
R07-BDV	19
R15-DC	20
R09-BDV	21
R21-FH	22
R38-CA	23
R27-SD	24
R24-TA	25
R22-FH	26
R25-TA	27
R28-SD	28
R29-SD	29
R31-SD	30
R16-DC	31
R30-SD	31
R11-DC	33
R10-DC	34
R34-SD	35
R12-DC	36
R14-DC	37
R37-CA	38

Fonte: TOPSIS (212) (adaptado).

Esse ranque expressa a classificação de importância quanto ao impacto que o risco pode causar ao ativo banco de dados, ou seja, quanto menor a colocação, ranque, maior o impacto. As preferências, sensibilidade, dos especialistas com relação à severidade, ocorrência e detecção, são representadas na Figura 4.11.

Figura 4.11: Preferências: sensibilidade, ocorrência e detecção.



Fonte: Autoria própria.

Mediante o exposto, a integração apresentada e aplicada pela metodologia, Figura 4.10, entre os métodos FMEA, AHP e TOPSIS neste estudo, resultou na classificação de importância dos 38 riscos identificados. O FMEA foi aplicado para análise dos riscos, por sua vez, o AHP contribuiu com a definição dos pesos relativos aos critérios severidade, ocorrência e detecção. O TOPSIS foi aplicado na etapa de avaliação dos riscos, a fim de rotular as prioridades de riscos relativos aos modos de falha de uma robustez ampla de acordo com a proximidade relativa às distâncias de soluções ideais positivas e negativas.

A técnica de preferência de pedido por similaridade à solução ideal viabilizou o aprimoramento do mecanismo de classificação dos modos de falha para tornar seus resultados mais razoáveis e eficazes, desta maneira, amplia a capacidade de identificação de riscos. Isso indica que a abordagem integrada de forma híbrida é eficaz. A etapa seguinte é composta por proposições de ações, tratamento dos riscos, relacionadas às ameaças identificadas.

4.4.5 Proposição de cursos de ação

A aplicação da metodologia proposta, vide Figura 4.10, resultou no ranqueamento dos riscos de forma eficaz e equilibrada, por certo, a combinação entre os métodos forneceu um suporte de decisão mais meticuloso. Sendo assim, as proposições de cursos de ação compõem o modelo de gestão de riscos de TI aplicado ao Consórcio Multi-Institucional de Ensino e Pesquisa no contexto do principal Ativo de TI identificado, no caso, a base de dados. O modelo é compósito por uma adaptação da ISO 31000 (2018) (94), composto pela identificação, análise, avaliação e tratamento dos riscos. A última etapa consiste no tratamento dos riscos, o qual tem como objetivo selecionar e implementar as opções para abordar os riscos.

O tratamento de riscos envolve a seleção de uma ou mais opções para modificar os riscos e a implementação dessas opções. Uma vez implementado, o tratamento fornece novos controles ou modifica os existentes (94). Para realizar as proposições de tratamento dos riscos o ponto de partida contou com a definição de quais riscos são indicados para a realização do tratamento de forma preliminar, pois nem todos os riscos identificados serão monitorados.

Nesse ínterim foram realizadas discussões com o grupo de especialistas, os quais realizaram as etapas de identificação, análise e avaliação dos riscos, das quais resultaram por consenso na priorização de ao menos três riscos por categoria. Foi definido, também, que os riscos devem ser evitados ou mitigados como respostas aos eventos. As categorias são: Ataques de injeção, BD vulneráveis, Dados confidenciais, Fator humano, Trilha de auditoria, Segurança de Dados e Controle de Acesso. Em vista disso, o resultado obtido na Tabela 4.8 foi utilizado para elencar os três principais riscos por categoria. Assim, é possível visualizar essa restrição aplicada a partir da Tabela 4.9.

Tabela 4.9: Principais riscos por categoria.

Riscos	Ranque -TOPSIS
R01-AI	6
R02-AI	7
R03-AI	4
R05-BDV	13
R06-BDV	12
R08-BDV	18
R13-DC	13
R17-DC	2
R18-DC	16
R19-FH	4
R20-FH	10
R21-FH	22
R23-TA	10
R24-TA	25
R25-TA	27
R26-SD	17
R32-SD	9
R33-SD	3
R35-CA	15
R36-CA	1
R38-CA	23

Fonte: TOPSIS (212) (adaptado).

A Tabela 4.9 mostra três riscos para cada categoria elencada na fase de identificação dos riscos. É importante destacar que a referida tabela está ordenada pela coluna "Riscos" de forma crescente. A partir da ordenação dos 21 riscos, é possível alvidrar uma proposta de tratamento dos riscos relacionados às categorias, e a literatura aborda várias estratégias para realizar esse tratamento e essas habilitações precisam ser compreendidas com o propósito de apoiar a sua eficácia. No contexto dessa pesquisa, optou-se por um tratamento que compreende:

- Definir controles.
- Respostas ao risco e responsáveis pelos riscos.
- Definir indicadores.
- Relatório de monitoramento e acompanhamento dos riscos.

Os próximos estágios detalham as propostas de tratamento de riscos ao considerar os principais riscos por categoria, de acordo com a Tabela 4.9.

Controles

As atividades de controle são políticas e procedimentos que direcionam as ações individuais na implementação das políticas de gestão de riscos, diretamente ou mediante a aplicação de tecnologia, a fim de assegurar que as respostas aos riscos sejam executadas. Essas atividades podem ser classificadas com base na natureza dos objetivos da organização aos quais os riscos de estratégia, operação, comunicação e cumprimento de diretrizes estão associados (183). A seguir, o detalhamento dos Controles relacionados a cada risco identificado e priorizado por categoria.

Quadro 14: Controles.

Riscos	Descrição do Controle	Controles	Referência
R01-AI	O sistema de informação verifica a validade de entradas de informações definidas pela organização. Verificar a sintaxe e semântica válidas das entradas do sistema de informação (por exemplo, conjunto de caracteres, comprimento, intervalo numérico e valores aceitáveis) verifica se as entradas correspondem às definições especificadas para formato e conteúdo.	O sistema de informação: a) Fornece uma capacidade de substituição manual para validação de entrada de definidas pela organizaçã o. b) Restringe o uso da capacidade de anulação manual apenas a indivíduos autorizados definidos pela organização. c) Audita o uso da capacidade de anulação manual • Revisão / resolução de erros • Comportamento previsível • Rever / criar interações • Restringir entradas a fontes confiáveis e formatos aprovados.	SI-10 – NIST (2015) (227)
R02-AI	Os procedimentos armazenados nem sempre estão protegidos contra injeção de SQL. No entanto, certas construções de programação de procedimento armazenado padrão têm o mesmo efeito que o uso de consultas parametrizadas quando implementadas com segurança, o que é a norma para a maioria das linguagens de procedimento armazenado.	a) Validação de entrada da lista de permissões. b) Visualizações SQL para aumentar a granularidade de acesso. c) Granularizar o controle de acesso, reduzindo ao máximo os privilégios. d) Minimizar os privilégios atribuídos a cada conta de banco de dados em seu ambiente. e) O desenvolvedor construa apenas instruções SQL com parâmetros que são parametrizados automaticamente. f) Usar validação de entrada ou escape adequado • Atualizações somente por usuários privilegiados • Validação de entrada de informações • Detectar comandos não autorizados • Proteção de código malicioso • Detecção não baseada em assinatura • Detectar comandos não autorizados • Autenticar comandos remotos • Análise de código maliciosa	SQL Prevenção de injeção - OWASP (2021) (195);SI-3 – NIST (2015) (227)

Riscos	Descrição do Controle	Controles	Referência
R03-AI	A organização implementa serviços e componentes do sistema de informação definidos pela organização não persistentes que são iniciados em um estado conhecido e encerrados Seleção (uma ou mais) ao final da sessão de uso; periodicamente em frequência definida pela organização.	a) A organização garante que o software e os dados empregados durante as atualizações de componentes e serviços do sistema de informações sejam obtidos em fontes confiáveis definidas pela organização. • Atualizar a partir de fontes confiáveis	SI-14 – NIST (2015) (227)
R05-BDV	O sistema de informações impede que usuários não privilegiados executem funções privilegiadas para incluir desabilitar, contornar ou alterar proteções / contramedidas de segurança implementadas.	• Proibição de usuários não privilegiados de executarem funções privilegiadas	AC6 (10) – NIST (2015) (227)
R06-BDV	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	• Não autorizar acesso às funções de segurança (AC-6 (1) - NIST) • Acesso não privilegiado para não segurança. • Acesso à rede privilegiado somente com autorização. • Domínios de processamento separados. • Contas privilegiadas. • Acesso privilegiado por não organizacional comercial. • Revisão dos privilégios do usuário. • Níveis de privilégio para execução de código. • Auditoria de uso de privilegiado. • Proíbe os usuários não privilegiados de executar funções. privilegiadas.	AC3 – NIST (2015) (227)

Riscos	Descrição do Controle	Controles	Referência
R08-BDV	Os certificados digitais são arquivos armazenados no dispositivo do usuário, fornecidos automaticamente junto com a senha do usuário durante a autenticação. Os certificados devem ser vinculados a uma conta de usuário individual para evitar que os usuários tentem se autenticar em outras contas.	• Implementar a Autenticação Multifator (MFA) ou autenticação de dois fatores (2FA). • Manter controle de validade dos certificados instalados no SGBD. • Projete controles para proteger o armazenamento confiável contra injeção de certificados raiz de terceiros. • Implemente controles de integridade em objetos armazenados no armazenamento confiável. • Não permita a exportação de chaves mantidas no armazenamento confiável sem autenticação e autorização. • Configure políticas e procedimentos estritos para exportar. • Implemente um processo seguro para atualizar o armazenamento confiável.	OWASP (2021) (195) e NIST (2015) (227)
R13-DC	Fornece aos indivíduos a capacidade de ter acesso às suas informações de Identificação Pessoal (PII) mantidas em seu (s) sistema (s) de registros. O acesso oferece aos indivíduos a capacidade de revisar as PII sobre eles mantidos nos sistemas organizacionais de registros. O acesso é oportuno, simplificado e barato aos dados. Os processos organizacionais para permitir o acesso aos registros podem diferir com base nos recursos, requisitos legais ou outros fatores.	• The Privacy Act de 1974, 5 U.S.C. §§ 552a (c) (3), (d) (5), (e) (4); (j), (k), (t); OMB Circular A-130. • LGDP CAPÍTULO VII, Seção I, Seção II, CAPÍTULO VIII. • Revisão da precisão, relevância, oportunidade e integridade das informações de identificação pessoal em todo o ciclo de vida da informação. • Correção ou exclusão de informações de identificação pessoal imprecisas ou desatualizadas. • Divulgar notificação de correção ou exclusão de informações de identificação pessoal para indivíduos ou outras entidades apropriadas. • Recursos de decisões adversas sobre solicitações de correção ou exclusão. • Monitore o processamento permitido nas interfaces externas do sistema e nos principais limites internos do sistema. • Documente cada exceção de processamento	IP-2, SC-7(24), PM-22 - NIST (2015) (227) e LGPD (2020) (23)

Riscos	Descrição do Controle	Controles	Referência
R17-DC	Estabelece, mantém e atualiza frequência definida pela organização um inventário que contém uma lista de todos os programas e sistemas de informação identificados como coletando, usando, mantendo ou compartilhando (PII)	• The Privacy Act de 1974, 5 U.S.C. § 552a (e) (10); Seção 208 (b) (2), E-Government Act de 2002 (P.L. 107-347); OMB Memorandum 03-22; OMB Circular A-130, Apêndice I; Publicação 199 do FIPS; Publicações Especiais do NIST 800-37, 800-122. • LGPD - Dado anonimizado.	SE-1 - NIST (2015) (227) e LGPD (2020) (23)
R18-DC	A organização descreve a (s) finalidade (s) para a (s) qual (is) as Informações de Identificação Pessoal são coletadas, usadas, mantidas e compartilhadas em seus avisos de privacidade.	• The Privacy Act de 1974, 5 U.S.C. § 552a (e) (3) (A) - (B); Seções 208 (b), (c), E-Government Act de 2002 (P.L. 107-347). • LGPD Capítulo II, Seção I, CAPÍTULO VI, Seção I, Seção II, Seção III, Capítulo VII, Seção I, Da Segurança e do Sigilo de Dados	AP-2 - NIST (2015) (227) e LGPD (2020) (23)
R19-FH	Esse controle trata do estabelecimento de políticas e procedimentos para a implementação eficaz de controles de segurança selecionados e aprimoramentos de controle na família de Conscientização e Treinamento. A política e os procedimentos refletem as leis federais aplicáveis, ordens executivas, diretivas, regulamentos, políticas, padrões e orientações. As políticas e procedimentos do programa de segurança no nível da organização podem tornar desnecessária a necessidade de políticas e procedimentos específicos do sistema. Bem como pode ser incluída como parte da política geral de segurança da informação para organizações ou, inversamente, pode ser representada por várias políticas que refletem a natureza complexa de certas organizações.	a) Desenvolve, documenta e dissemina para pessoal ou funções definidas pela organização: • Uma política de conscientização e treinamento de segurança que aborda o propósito, escopo, funções, responsabilidades, compromisso de gerenciamento, coordenação entre entidades organizacionais e conformidade. • Procedimentos para facilitar a implementação da política de conscientização e treinamento de segurança e dos controles de conscientização e treinamento de segurança associados b) Revisa e atualiza o atual: • Política de conscientização e treinamento de segurança frequência definida pela organização. Procedimentos de conscientização e treinamento de segurança frequência definida pela organização.	AT-1- NIST (2015) (227)

Riscos	Descrição do Controle	Controles	Referência
R20-FH	As organizações determinam o conteúdo apropriado do treinamento de segurança com base nas funções e responsabilidades atribuídas aos indivíduos e nos requisitos de segurança específicos das organizações e dos sistemas de informação aos quais o pessoal tem acesso autorizado.	• Controles ambientais • Controles de segurança física • Exercícios práticos • Comunicações suspeitas e comportamento do sistema anômalo.	AT-3 - NIST (2015) (227)
R21-FH	A organização oferece treinamento básico de conscientização de segurança para usuários de sistemas de informação (incluindo gerentes, executivos seniores e contratados), sobre como reconhecer e relatar indicadores potenciais de ameaças internas	• Exercícios práticos • Ameaça interna	AT-2 - NIST (2015) (227)
R23-TA	Auditar os processos de dados pessoais para garantir que a notificação cobre adequadamente as atividades de processamento.	a) É fundamental para garantir o processamento justo de dados pessoais e o processamento de tais dados de acordo com finalidades especificadas e legais. b) Convém que a organização informe ao cliente se, na sua opinião, uma instrução de tratamento viola uma regulamentação e/ou legislação aplica.(183) • The Privacy Act de 1974, 5 U.S.C. § 552a (e) (3) (A) - (B); Seções 208 (b), (c), E-Government Act de 2002 (P.L. 107-347). • LGPD CAPÍTULO IV, Seção I, Seção II, CAPÍTULO V, Seção III, CAPÍTULO VII, Seção I	8.2.4 Violando instruções - ISO 27701 (2019) (180)

Riscos	Descrição do Controle	Controles	Referência
R24-TA	Configurar o log de auditoria detalhado para ativos corporativos contendo dados sensíveis, os quais possam envolver dados pessoais.	• Inclusão de origem do evento, data, nome de usuário, carimbo de data/hora, endereços de origem. • Endereços de destino e outros elementos úteis que podem ajudar em uma investigação forense.	Controles CIS Versão 8, maio, 2021 - CIS(2021) (188)
R25-TA	Trilha de auditoria também deve ser usada para verificar se todo processo realizado em dados pessoais está relacionado a um propósito de processo notificado, garantindo, assim, a adequação da notificação.	• Convém que a organização determine e mantenha os registros necessários para apoiar a demonstração do Compliance com suas obrigações (como especificado no contrato aplicável) para tratamento de • DP realizado em nome do cliente. • Detecta o uso indevido de dados. • Categorias de tratamento realizadas em nome de cada cliente. • Transferências para outros países ou organizações internacionais. • Uma descrição geral das medidas de segurança técnicas e organizacionais.	8.2.6 Registros relativos ao tratamento de DP - ISO 27701 (2019) (180)
R26-SD	O Dado Pessoal - DP pode ser divulgado durante o curso das operações normais. Convém que estas divulgações sejam registradas como também que quaisquer divulgações adicionais para terceiros, como aquelas que surgem de investigações legais ou de auditorias externas, sejam registradas. Convém, ainda, que os registros incluam as fontes da divulgação e a fonte da autoridade que fez a divulgação.	• Convém que a organização registre a divulgação de DP para terceiros, incluindo qual DP foi divulgado, para quem e quando.	7.5.4 Registro de divulgação de DP para terceiros - ISO 27701 (2019) (180)

Riscos	Descrição do Controle	Controles	Referência
R32-SD	A transferência de DP entre jurisdições pode estar sujeita à legislação e/ou regulamentação, a depender da jurisdição ou organização para a qual DP serão transferidos (e de onde se originam). Convém que a organização documente o Compliance com estes requisitos como a base para transferência.	• Convém que a organização informe ao cliente em um tempo hábil sobre as bases para a transferência de DP entre jurisdições e de qualquer mudança pretendida nesta questão, de modo que o cliente tenha a capacidade de contestar estas mudanças ou rescindir o contrato.	8.5.1 Bases para a transferência de DP entre jurisdições - ISO 27701 (2019) (180)
R33-SD	A organização deve aplicar o processo de avaliação de riscos de segurança da informação para identificar os riscos associados à perda de confidencialidade, integridade e disponibilidade, dentro do escopo do SGPI.(183)	• Sistema e política de integridade de informações que aborda propósito, escopo, funções, responsabilidades, compromisso de gestão, coordenação entre entidades organizacionais e conformidade. • Procedimentos para facilitar a implementação do sistema e da política de integridade da informação e sistemas associados e controles de integridade da informação.	SI-1- NIST (2015) (227)
R35-CA	O sistema de informações impõe autorizações aprovadas para acesso lógico às informações e recursos do sistema de acordo com as políticas de controle de acesso aplicáveis.	• Não autorizar acesso às funções de segurança (AC-6 (1) - NIST) • Acesso não privilegiado para não segurança. • Acesso à rede privilegiado somente com autorização. • Domínios de processamento separados. • Contas privilegiadas. • Acesso privilegiado por não organizacional comercial. • Revisão dos privilégios do usuário. • Níveis de privilégio para execução de código. • Auditoria de uso de privilegiado. • Proíbe os usuários não privilegiados de executarem funções privilegiadas.	AC3 - NIST (2015) (227)

Riscos	Descrição do Controle	Controles	Referência
R36-CA	A organização define as políticas e procedimentos relativos ao controle de acesso.	a) Desenvolve, documenta e dissemina para pessoal ou funções definidas pela organização: • Uma política de controle de acesso que aborda propósito, escopo, funções, responsabilidades, compromisso de gestão, coordenação entre entidades organizacionais e conformidade. • Procedimentos para facilitar a implementação da política de controle de acesso e controles de acesso associados. b) Revisa e atualiza o atual: • Política de controle de acesso e frequência definida pela organização. • Procedimentos de controle de acesso frequência definida pela organização. • Controles, conforme ISO/IEC 27.001: A.5.1.1, A.5.1.2, A.6.1.1, A.9.1.1, A.12.1.1, A.18.1.1, A.18.2.2	AC-1 - NIST (2015) (227)
R38-CA	Desenvolve e documenta um inventário dos componentes do sistema de informação, além de revisar e atualizar o inventário de componentes do sistema de informações com a frequência definida pela organização	• Atualizações durante as instalações / remoções. • Manutenção automatizada. • Detecção automatizada de componentes não autorizados. • Informações de responsabilidade. • Sem contabilidade duplicada de componentes. • Configurações avaliadas / desvios aprovados. • Repositório centralizado. • Rastreamento de localização automatizado. • Atribuição de componentes a sistemas.	CM-8 – NIST (2015) (227)

Fonte: (23), (180), (188), (195) e (227) (adaptados).

A respeito dos controles, quando utilizado o termo organização, entenda-se como CMI, pois, nesse caso, as deliberações estão relacionadas ao alinhamento estratégico realizado entre o consórcio e a área de TI. O próximo item relaciona as respostas aos riscos com os responsáveis por manter um constante monitoramento.

Respostas ao risco e responsáveis pelos riscos

No que toca as respostas aos riscos, além dos responsáveis pelo monitoramento, podem ser observados a partir do Quadro 15.

Quadro 15: Resposta aos riscos e responsáveis pelos riscos.

Riscos	**Resposta ao risco**	**Responsabilidade**
R01-AI	Mitigar	Gestores do CMI e Infraestrutura e DBA.
R02-AI	Mitigar	Gestores do CMI e Infraestrutura e DBA.
R03-AI	Mitigar	Gestores do CMI e Arquitetura e DBA.
R05-BDV	Mitigar	Infraestrutura e DBA.
R06-BDV	Mitigar	Infraestrutura e DBA.
R08-BDV	Mitigar	DBA.
R13-DC	Mitigar	DBA.
R17-DC	Mitigar	Gestores do CMI e Administrador de dados
R18-DC	Mitigar	Gestores do CMI e Administrador de dados
R19-FH	Mitigar	Gestores do CMI e Infraestrutura e DBA.
R20-FH	Mitigar	Gestores do CMI e SI e DBA
R21-FH	Mitigar	Gestores do CMI e Arquitetura e DBA.
R23-TA	Mitigar	Arquitetura e DBA.
R24-TA	Mitigar	Arquitetura e DBA.
R25-TA	Mitigar	Arquitetura e DBA.
R26-SD	Mitigar	SI e DBA.
R32-SD	Mitigar	Infraestrutura e DBA.
R33-SD	Mitigar	Infraestrutura e DBA.
R35-CA	Mitigar	Gestores do CMI e Infraestrutura e DBA.
R36-CA	Mitigar	Gestores do CMI e Infraestrutura e DBA.
R38-CA	Mitigar	SI e DBA.

Fonte: PMBoK (2017) (22) (adaptado).

Com respeito aos responsáveis pelos riscos, é importante destacar que o monitoramento está indicado para o perfil e não cita o nome de pessoas, uma vez que pode existir rotatividade de profissionais acarretando prejuízos para o monitoramento. O mesmo é aplicado ao CMI, pois é sabido a existência da possibilidade de novos membros assumirem ou deixarem as funções para assumir novas responsabilidades. A etapa, a qual segue, está relacionada à proposição de indicadores.

Indicadores

Indicadores permitem realizar monitoramento quantitativo de forma a possibilitar o acompanhamento das tendências e efetividade na implementação do programa. Eles precisam ser mensuráveis e apropriados para as unidades de negócios de forma a garantir a melhoria contínua. Os indicadores de desempenho possibilitam monitorar os resultados

ou processos (por exemplo: desempenho consistente das ações de tratamento de risco) (228).

O indicador é uma medida, de ordem quantitativa ou qualitativa, dotada de significado particular e utilizada para organizar e captar as informações relevantes dos elementos que compõem o objeto da observação. É um recurso metodológico que informa empiricamente sobre a evolução do aspecto observado (229). Nesse contexto, os indicadores estão em conformidade com o Quadro 16 e Quadro 17, os quais relacionam-se aos controles propostos para mitigar os riscos priorizados.

Quadro 16: Indicador de resultado relacionado aos controles.

Elemento	**Descrição**
Indicador	Taxa de efetividade dos controles
Meta	No máximo 5 problemas relacionados aos controles, de acordo com a indicação: • Ataques de injeção = 0 • BD vulneráveis = 0 • Dados confidenciais = 0 • Fator humano = 5 • Trilha de auditoria = 0 • Segurança de dados = 0 • Controle de acesso = 0 O indicador deve apresentar um índice menor que 6,5%, ou seja, no mínimo 93% de efetividade.
Periodicidade de Apuração	Mensal
Prazo máximo para apuração	Primeiro dia útil de cada mês
Responsabilidade pela apuração	Equipe de monitoramento de incidentes de TI
Fonte de dados	Central de Incidentes, *Zabbix* e *Graylog* (ferramentas de monitoramento)
Forma de coleta dos dados	Verificação junto à equipe de incidentes a ocorrência de algum evento relacionado aos controles propostos para cada um dos riscos identificados.
Como apurar o indicador	Apurar a quantidade de incidentes relacionados a qualquer um dos controles propostos na Tabela de Modos de falha ranqueados. • Problemas relacionados aos controles = numerador. • 76 controles propostos = denominador • Dividir o numerador pelo denominador e multiplicar por 100.
O que o indicador Mostra	Qualidade na aplicação, monitoramento e eficácia dos controles propostos.
O que pode causar um resultado aquém da meta	Deficiência na aplicação, monitoramento ou eficácia dos controles.
Qual o impacto de um resultado aquém da meta	Aumento do índice de incidentes relacionados as categorias de riscos: Ataques de injeção, BD vulneráveis, Dados confidenciais, Fator humano, Trilha de auditoria, Segurança de dados e Controle de acesso.

Fonte: (228) e (229) (adaptados).

O Quadro 16 enumera os resultados relacionados ao desempenho dos controles propostos, ou seja, mede a efetividade dos controles. É um indicador de resultado. Por sua vez, o Quadro 17 pauta o indicador de esforço relacionado aos controles.

Quadro 17: Indicador de esforço relacionado aos controles.

Elemento	**Descrição**
Indicador	Percentual de usuários da PNID treinados em Segurança da Informação com ênfase a riscos de Fatores Humanos.
Meta	Treinar 200 usuários da PNID.
Periodicidade de Apuração	Mensal.
Prazo máximo para apuração	Primeiro dia útil de cada mês.
Responsabilidade pela apuração	Equipe de Gestão do CMI.
Fonte de dados	Equipe de Gestão do CMI
Forma de coleta dos dados	Verificação junto à equipe de gestão do consócio mensalmente a quantidade de usuários treinados em voltada para Fatores Humanos (Engenharia Social).
Como apurar o indicador	Apurar a quantidade de usuários treinados • Quantidade usuários treinados = numerador. • Meta de treinar 200 usuários = denominador. • Dividir o numerador pelo denominador e multiplicar por 100.
O que o indicador Mostra	A divulgação e aprimoramento dos usuários quanto ao risco de eventos relacionados à Fatores Humanos.
O que pode causar um resultado aquém da meta	Aumento do risco de problemas relacionados à Engenharia Social.
Qual o impacto de um resultado aquém da meta	Pode demonstrar uma falta de interesse por parte dos treinandos, falta de recursos para implementação ou realização dos treinamentos, ou mesmo, falta de política de conscientização dos problemas causados por Engenharia social.

Fonte: (228) e (229) (adaptados).

A partir da implantação dos indicadores de resultado, o CMI pode medir sistematicamente o seu desempenho em relação aos controles propostos, além de monitorar e gerir os riscos identificados. Com isso, à medida que ocorrem variações relacionadas ao processo os gestores, podem realizar ações das quais melhorem o desempenho do consórcio. O passo seguinte do Tratamento dos riscos refere-se ao monitoramento e acompanhamento dos riscos.

Monitoramento e acompanhamento dos riscos

O monitoramento e acompanhamento dos riscos fazem parte da fase de Tratamento dos riscos. Nesse sentido, a etapa é composta por: formulário para monitoramento e análise crítica de riscos (Figura 4.12) e formulário para comunicação de riscos (Figura 4.13), conforme podem ser observados. Essas ferramentas buscam estabelecer (228):

- O contexto adequado.
- Garantir que as partes interessadas sejam ouvidas, entendidas e consideradas.
- Assegurar que os riscos sejam devidamente identificados.
- Envolver diferentes áreas de atuação para a análise de riscos e
- Garantir que os diferentes pontos de vista sejam considerados, quando da análise crítica e comunicação dos riscos.

A comunicação e consulta às partes interessadas é importante para que sejam conhecidas, entendidas e justificadas as necessidades do tratamento dos riscos mediante o fortalecimento da percepção dos riscos, . Essas percepções podem variar em função das diferenças dos valores, necessidades, premissas, conceitos e as preocupações , o que abre margem para influenciar nas decisões a serem tomadas (228).

Figura 4.12: Formulário para monitoramento e análise crítica de riscos

<< Logo >>	Tipo de Doc. FRM	Doc. Nº FRM XXX.X	Revisão 00
	Data Emissão DD/MM/AAAA	Data Vigência DD/MM/AAAA	Página 01 de 01
	Formulário para monitoramento e análise dos riscos		

Compilado por:	
Data:	
Analisado por:	
Data:	

Riscos				Categoria do Risco	Controles Existentes*	Novos Controles*	Nível do Risco	Risco Residual	Tendência	Melhoria		
ID	Eventos	Causas	Consequências							Requerida	Responsável	Status

Fonte: Autoria própria.

Figura 4.13: Formulário para comunicação de riscos

<< Logo >>	Tipo de Doc. **FRM**	Doc. Nº **FRM XXX.X**	Revisão **00**
	Data Emissão **DD/MM/AAAA**	Data Vigência **DD/MM/AAAA**	Página **01 de 01**
	Formulário para Comunicação de Riscos		

Compilado por:	
Data:	
Analisado por:	
Data:	

Parte Interessada	Comunicador	Propósito.	Descrição do Risco	Método de Comunicação	Data da Comunicação	Frequência

Fonte: Autoria própria.

A próxima etapa envolve a conclusão e considerações finais relativas a esta pesquisa de mestrado.

Capítulo 5

Conclusão

O último capítulo desse estudo dedica-se às considerações finais, ademais, proposições de pesquisas futuras e trabalhos correlatos.

5.1 Considerações Finais

O trabalho de pesquisa apresenta uma solução voltada para Gestão de Riscos relativa ao Ativo Banco de Dados, o qual apresenta um alto índice de sensibilidade à continuidade dos negócios inerentes ao Consórcio Multi-Institucional.

A principal informação compartilhada pelo CMI são dados pessoais, científicos, dados de fomento relacionados aos principais órgãos financiadores de pesquisa no Brasil, informações de livros, resultados de pesquisas, dentre outros.

A pesquisa possui um grau de sofisticação significativo, uma vez que é composta por quatro fases complexas, a saber:

• Fase 1 - Cenário de tomada de decisões, fase a qual se buscou identificar as nuances do CMI.

• Fase 2 - Hierarquização de critérios e alternativas, fase responsável por identificar o método adequado ao negócio central das instituições envolvidas no projeto da PNID

• Fase 3 - Definição do ativo de TI, responsável por absorver, entender e identificar o principal ativo de TI para continuidade da PNID e CMI.

• Fase 4 - Modelo de Gestão de riscos, nesta fase é apresentado o modelo proposto para GR conforme as necessidades do Consórcio Multi-Institucional e da PNID.

A composição das quatro fases demandou revisões sistemáticas de literatura, que culminou em uma proposição composta por metodologias distintas e ao mesmo tempo complementares, caso do PMBOK (22) e norma ISO 31.000 (94). Foram empregadas, também, ferramentas de apoio alicerçadas pela norma ISO 31.010 (95). Um outro importante elemento aplicado na pesquisa foi o emprego de métodos MCDM com o FMEA (Fase 4),

em que foram empregados a Análise de Modo e Efeito de Falha para conhecer os eventos de riscos e o Processo Hierárquico Analítico para identificação dos pesos inerentes aos critérios Severidade, Ocorrência e Detecção. Esse resultado foi utilizado como entrada para os cálculos realizados pela Técnica para Ordem de Preferência por Similaridade com a Solução Ideal, a qual resultou na ordenação dos eventos de riscos identificados.

Com os eventos ordenados, por seu grau de importância sob os olhos dos especialistas, a pesquisa apresenta um plano de ação bem detalhado, que granularizou para um trabalho mais completo. Esse plano é composto por controles, definição de respostas aos riscos com os respectivos responsáveis pelos eventos, indicadores e relatórios de acompanhamento dos riscos. No geral a proposta da GR identificou 38 riscos relacionados as categorias: Ataques de injeção, Banco de Dados vulneráveis, Dados confidenciais, Fator humano (Engenharia Social), Trilha de auditoria, Segurança de dados e Controle de acesso. Com isso, a GR possibilita o monitoramento e controle efetivo relacionado aos riscos priorizados, e a repercussão construtiva obtida por essa GR viabiliza que outras instituições, como os órgãos de fomento financiadores do CMI, adotem esse modelo como forma de maximizar os serviços realizados para sociedade.

O resultado logrado quanto as proposições de metodologia foram ascendidas graças ao apoio dos patrocinadores do consórcio, além do engajamento de toda equipe de especialistas, os quais participaram ativamente de todas as fases que requeriam conhecimento técnico especializado. O modelo de Gestão de Riscos foi apresentado aos patrocinadores do Consórcio, os quais o classificaram como fundamental para continuidade do negócio, pois trouxe uma visão de gestão de riscos que não era conhecida por eles ou mesmo por equipes técnicas envolvidas. O desfecho da pesquisa demonstra a efetividade da relação entre academia, iniciativa pública e privada, maximizando a importância do mestrado profissional ao aplicar o conhecimento científico às práticas e necessidades ágeis requeridas pela sociedade e pelos entes públicos e privados.

Por fim, o objetivo geral, bem como os específicos, foram alcançados e o problema de pesquisa foi tocado com a confecção do Modelo de gestão riscos de TI aplicado a um Consórcio Multi-Institucional de ensino e pesquisa.

5.2 Trabalhos Futuros

Este trabalho se propôs a priorizar ações de Governança de TI e aplicar a Gestão de Riscos no contexto do principal ativo de Tecnologia da Informação vinculado a Governança TI do Consórcio Multi-institucional, que é o responsável pelo desenvolvimento da PNID.

A PNID mantem em sua base de dados informações pessoais, dados de autores, pesquisadores, informações de fomento a pesquisa e de instituições públicas. São dados sensíveis

enviados e recebidos pelos membros do consórcio. Para um trabalho futuro uma análise dos riscos relacionados a potenciais falhas em ativos de infraestrutura de informações, que sejam responsáveis pela segurança de dados pessoais, poderia ser objeto de estudo.

Referências Bibliográficas

1 REDE Nacional de Ensino e Pesquisa. fev 2021. Disponível em: <https://www.rnp.br/>. Acesso em: 07/02/2021. 1, 2

2 3.825, P. interministerial número. Reformula o programa interministerial de implantação e manutenção da rede nacional para ensino e pesquisa - rnp e de seu comitê gestor. *DOU ISSN 1677-7042 Nº 240*, dec 2018. 1

3 CAPES. Coordenação de aperfeiçoamento de pessoal de nível superior. feb 2021. Disponível em: <https://www.gov.br/capes/pt-br>. Acesso em: 07/02/2021. 1

4 BRASIL, C. C. Consórcio nacional em educação, ciência, tecnologia e inovação. feb 2021. Disponível em: <https://www.conectibrasil.org/>. Acesso em: 07/02/2021. 1, 3, 4, 6, 51

5 CNPQ. Conselho nacional de desenvolvimento científico e tecnológico. Disponível em: <https://www.gov.br/cnpq/pt-br>. Acesso em: 07/02/2021. 2

6 CONFAP. Conselho nacional das fundações estaduais de amparo à pesquisa. feb. Disponível em: <https://confap.org.br/>. Acesso em: 07/02/2021. 2

7 IBICT. Instituto brasileiro de informação em ciência e tecnologia. Disponível em: <https://www.ibict.br/>. Acesso em: 07/02/2021. 2

8 SCIELO. Scientific electronic library online. Disponível em: <https://scielo.org/>. Acesso em: 07/02/2021. 2

9 SCHöPFEL, J.; AZEROUAL, O. 2 - current research information systems and institutional repositories: From data ingestion to convergence and merger. In: BAKER, D.; ELLIS, L. (Ed.). *Future Directions in Digital Information*. Chandos Publishing, 2021, (Chandos Digital Information Review). p. 19–37. ISBN 978-0-12-822144-0. Disponível em: <https://www.sciencedirect.com/science/article/pii/B9780128221440000021>. 3

10 HAAK, L.; BAKER, D.; HOELLRIGL, T. Casrai and orcid: Putting the pieces together to collaboratively support the research community. *Procedia Computer Science*, v. 33, p. 284–288, 2014. ISSN 1877-0509. 12th International Conference on Current Research Information Systems, CRIS 2014. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1877050914008357>. 4

11 MOREIRA, J. M.; CUNHA, A.; MACEDO, N. An orcid based synchronization framework for a national cris ecosystem [version 1; peer review: 2 approved, 1 approved with reservations]. *F1000Research*, v. 4, n. 181, 2015. 4

12 BRASIL. Lei nº 11.107, de 6 de abril de 2005. Dispõe sobre normas gerais de contratação de consórcios públicos e dá outras providências. *Diário Oficial*, 2005. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2005/lei/l11107.htm>. Acesso em: 07/02/2021. 4

13 BRASIL. Constituição da república federativa do brasil de 1988. *DOU*, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 15/02/2021. 4

14 BRASIL. Lei 11079. *DOU*, 2004. Disponível em: <https://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2004/Lei/L11079.htm>. Acesso em: 07/02/2021. 4

15 AERTS G.; GRACE, T. D. M. H. E. Public-private partnerships for the provision of port infrastructure: An explorative multi-actor perspective on critical success factors. *The Asian Journal of Shipping and Logistics*, Vol: 30, n. 273-298, 2014. 5

16 VERGER, A.; MOSCHETTI, M. C.; FONTDEVILA, C. How and why policy design matters: understanding the diverging effects of public-private partnerships in education. *Comparative Education*, Routledge, v. 56, n. 2, p. 278–303, 2020. Disponível em: <https://doi.org/10.1080/03050068.2020.1744239>. 5

17 ISSAYEVA G.K., A. A. A. Z. K. M.-B. Z.-A. A. K. Z. Y. A. Public private partnerships in education: Modes of governance in developing economy. *Journal of Entrepreneurship Education*, v. 21, 2018. ISSN 10988394. 5

18 VIRKAR, S. Information and communication technology platform design for public administration reform: Tensions and synergies in bangalore. *Public Administration and Information Technology*, v. 21, 2014. 5

19 ABRUCIO, F. L. Disciplina 3.1: debate contemporâneo da gestão pública. *Escola Nacional de Administração Pública (Enap).*, 2021. Disponível em: <http://repositorio.enap.gov.br/handle/1/1021>. Acesso em: 27/05/2021. 8

20 ACCOUNTANTS, I. F. of. Good governance in the public sector: consultation draft for an international framework. *IFAC*, 2013. Disponível em: <https://www.ifac.org/publications-resources/good-governance-public-sector>. Acesso em: 26/05/2021. 8

21 ACCOUNTANTS, I. F. of. Comparison of principles. *IFAC*, 2013. Disponível em: <http://www.ifac.org/sites/default/files/publications/files/Comparison-of-Principles.pdf>. Acesso em: 26/05/2021. 8

22 INSTITUTE, P. M. *Um Guia do Conhecimento em Gerenciamento de Projetos (Guia PMBOK)*. sixth. [S.l.]: Project Management Institute, 2017. 9, 31, 61, 63, 72, 112, 120

23 BRASIL. Lei geral de proteção de dados pessoais. *DOU*, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 03/06/2021. 10, 55, 56, 58, 84, 106, 107, 111

24 VERGER, A. Framing and selling global education policy: the promotion of public–private partnerships for education in low-income contexts. *Journal of Education Policy*, Routledge, v. 27, n. 1, p. 109–130, 2012. Disponível em: <https://doi.org/10.1080/02680939.2011.623242>. 12

25 SHARAFANOVA E.E., F. Y. S. A. Regional labor market: Forecasting the economic effect of cooperation between universities and entrepreneurs. *Journal of Advanced Research in Law and Economics*, p. 1133–1156, 2017. 12

26 ROBERTSON S., V. A. The emergence of public-private partnerships in the global governance of education. *Educacao e Sociedade 33(121)*, p. 1133–1156, 2012. 12

27 CHATTOPADHAY T., N. O. Public-private partnership in education: A promising model from brazil. *Journal of International Development 26(6)*, p. 875–886, 2014. 12, 13

28 FONTANELA C., S. M. D. S. A. J. Brazilian community universities and regional policies for technology and innovation. *IAMOT 2016 - 25th International Association for Management of Technology Conference, Proceedings: Technology - Future Thinking*, p. 1820–1831, 2016. 13

29 BRITO S.H.A., M. G. de. Lemann foundation and the connected education innovation program: public-private relations in the field of educational policies. *Educar em Revista*, 2020. 13

30 DAGNINO G. B., P. G. Coopetition strategy: A new kind of interfirm dynamics for value creation. *In II Annual Conference of EURAM*, p. 9–11, may 2002. 13

31 DAL-SOTO F., M. J. Coopetition strategies in the brazilian higher education. *RAE-Revista de Administração de Empresas*, 2017. 13

32 MUNDIM, M. A. P.; SILVA, L. N. Duarte e. Gerencialismo estatal e a relaÇÃo pÚblico-privada na educaÇÃo em goiÁs. *Práxis Educacional*, v. 15, n. 31, p. 102–122, jan. 2019. Disponível em: <https://periodicos2.uesb.br/index.php/praxis/article/view/4662>. 14

33 HOPPER, T.; LASSOU, P.; SOOBAROYEN, T. Globalisation, accounting and developing countries. *Critical Perspectives on Accounting*, v. 43, p. 125–148, 2017. ISSN 1045-2354. 25th Anniversary issue. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1045235416300260>. 14

34 CARVALHO, J. R. H. et al. Industry and academia partnership for short-time high-level qualification. In: *2018 IEEE Frontiers in Education Conference (FIE)*. [S.l.: s.n.], 2018. p. 1–8. 14

35 MIRANDA M.D., C. M. P. R. Institutional arrangements for education management in bahia territories: tensions between public and private. *Educar em Revista*, 2020. 14

36 FERREIRA, F. M. F. et al. University-industry partnership as a teaching-learning strategy. *IEEE Potentials*, v. 38, n. 6, p. 32–37, 2019. 15

37 CARVALHO, J. R. H.; OLIVEIRA, E. H. T. de; CARVALHO, I. A. V. A. Stem education program evaluation survey: A report of experience. In: *2016 IEEE Frontiers in Education Conference (FIE)*. [S.l.: s.n.], 2016. p. 1–8. 15

38 BRITO, C. D. R.; CIAMPI, M. M. Research relevance in the world scenario. In: *2015 International Symposium on Computers in Education (SIIE)*. [S.l.: s.n.], 2015. p. 1–4. 15

39 JAIN, S. D.; DETHE, C. G. Knowledge center initiative for transforming india into a knowledge destination. In: *2015 IEEE 3rd International Conference on MOOCs, Innovation and Technology in Education (MITE)*. [S.l.: s.n.], 2015. p. 52–57. 15, 17

40 FOSCHI E., D. F. . B. A. Plastic waste management: a comprehensive analysis of the current status to set up an after-use plastic strategy in emilia-romagna region (italy). *Environ Sci Pollut Res 28*, may 2021. 15

41 HOGAN, A. Naplan and the role of edu-business: New governance, new privatisations and new partnerships in australian education policy. *Aust. Educ. Res. 43*, p. 93–110, 2016. 15

42 OSEI-KYEI, R.; CHAN, A. Public sector's perspective on implementing public – private partnership (ppp) policy in ghana and hong kong. *Journal of Facilities Management*, Vol. 16, n. 2, p. 175–196, 2018. 15

43 CARPINTERO, S.; SIEMIATYCKI, M. Ppp projects in local infrastructure: evidence from schools in the madrid region, spain. *Public Money & Management*, Routledge, v. 35, n. 6, p. 439–446, 2015. Disponível em: <https://doi.org/10.1080/09540962.2015.1083690>. 16

44 STEINER-KHAMSI, G.; DUGONJIć-RODWIN, L. Transnational accreditation for public schools: Ib, pisa and other public–private partnerships. *Journal of Curriculum Studies*, Routledge, v. 50, n. 5, p. 595–607, 2018. Disponível em: <https://doi.org/10.1080/00220272.2018.1502813>. 16

45 HENDRE P.S., M. S. K. R. e. a. African orphan crops consortium (aocc): status of developing genomic resources for african orphan crops. *Planta*, v. 250, p. 989–1003, 2019. 16

46 GRAHAM M. J., K. S. R. B. E. C. A.-S. M. B. C. B. N. . S. B. The zwicky transient facility: Science objectives. *Publications of the Astronomical Society of the Pacific*, v. 131, 2019. 16

47 MENGAL, P. et al. Bio-based industries joint undertaking: The catalyst for sustainable bio-based economic growth in europe. *New Biotechnology*, v. 40, p. 31–39, 2018. ISSN 1871-6784. Bioeconomy. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1871678416325638>. 16

48 CAPURRO D., E. A. F. R. G. S. T. C.-G. C. A. A. G. A. H. S. Chile's national center for health information systems: A public-private partnership to foster health care information interoperability. *Studies in Health Technology and Informatics*, v. 245, n. 693 - 695, 2017. 16

49 PATEL J.N., V. D. B. G. B. J. C. A.-B. L. F. A. H. I. M. A. S. N. I. S. W. T. North carolina's multi-institutional pharmacogenomics efforts with the nc precision health collaborative. *Pharmacogenomics*, 2021. 16

50 JONGBLOED, B.; VOSSENSTEYN, H. University funding and student funding: international comparisons. *Oxford Review of Economic Policy*, v. 32, n. 4, p. 576–595, 10 2016. ISSN 0266-903X. Disponível em: <https://doi.org/10.1093/oxrep/grw029>. 16

51 MILENKOVIć, M.; RAšIć, M.; VOJKOVIć, G. Using public private partnership models in smart cities - proposal for croatia. In: *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. [S.l.: s.n.], 2017. p. 1412–1417. 16

52 DEY, S. Securing majority-attack in blockchain using machine learning and algorithmic game theory: A proof of work. In: *2018 10th Computer Science and Electronic Engineering (CEEC)*. [S.l.: s.n.], 2018. p. 7–10. 16

53 KASSEN, M. Adopting and managing open data: Stakeholder perspectives, challenges and policy recommendations. *Aslib Journal of Information Management*, v. 70, n. 5, p. 518–537, 2018. 16

54 DíAZ-DíAZ R., . P.-G. D. Implementation of social media concepts for e-government: Case study of a social media tool for value co-creation and citizen participation. *Journal of Organizational and End User Computing (JOEUC)*, v. 28(3), p. 104–121, 2016. 16

55 WEERAKKODY, V. et al. Factors influencing user acceptance of public sector big open data. *Production Planning & Control*, Taylor Francis, v. 28, n. 11-12, p. 891–905, 2017. Disponível em: <https://doi.org/10.1080/09537287.2017.1336802>. 16

56 ATMO G.U., D. C. Z.-L. W. D. Comparative performance of ppps and traditional procurement projects in indonesia. *International Journal of Public Sector Management*, v. 30, n. 2, p. 118–136, 2017. 16

57 SHAOUL J., S. A. S.-P. Accountability and corporate governance of public private partnerships. *Critical Perspectives on Accounting*, 2012. 17

58 F.M. YáNEZ R.L., B. E. H. E. G. It governance—models and application. *Advances in Intelligent Systems and Computing*, p. 467–480, 2016. 17

59 GARTNER. It governance (itg). *Gartner*, 2021. Disponível em: <https://www.gartner.com/en/information-technology/glossary/it-governance>. Acesso em: 22/04/2021. 17

60 ITGI. It governance institute. *ITGI*, 2021. Disponível em: <https://www.itgovernance.co.uk/it_governance>. Acesso em: 22/04/2021. 17

61 ISACA. It governance institute. *ISACA*, 2021. Disponível em: <https://www.isaca.org/resources/cobit>. Acesso em: 22/04/2021. 17

62 ISO. Information technology — governance of it for the organization. *ISO*, 2021. Disponível em: <https://www.iso.org/standard/62816.html>. Acesso em: 26/04/2021. 17, 32, 43

63 QUEZADA-SARMIENTO, P. A. et al. Referent framework to government of it using standards: Cobit 5 and iso 38500. In: *2017 12th Iberian Conference on Information Systems and Technologies (CISTI)*. [S.l.: s.n.], 2017. p. 1–6. 17

64 A. MAURICIO D., A.-M. G. P. D. O.-A. The application and use of information technology governance at the university level. *Intelligent Computing*, p. 1028–1038, may 2018. 17

65 ESPINOZA-AGUIRRE, C.; PILLO-GUANOLUISA, D. It governance model for public institutions with a focus on higher education. In: *2018 13th Iberian Conference on Information Systems and Technologies (CISTI)*. [S.l.: s.n.], 2018. p. 1–14. 17

66 GUNEY, Y.; HERNANDEZ-PERDOMO, E.; ROCCO, C. M. Does relative strength in corporate governance improve corporate performance? empirical evidence using mcda approach. *Journal of the Operational Research Society*, Taylor Francis, v. 71, n. 10, p. 1593–1618, 2020. Disponível em: <https://doi.org/10.1080/01605682.2019.1621216>. 17

67 UNIãO, T. de Contas da. Tcu divulga dados ineditos sobre governança na administracao pública federal. *TCU*, 2021. Disponível em: <https://portal.tcu.gov.br/imprensa/noticias/tcu-divulga-dados-ineditos-sobre-governanca-na-administracao-publica-federal.htm>. Acesso em: 27/02/2021. 18

68 UNIãO, T. de Contas da. Grupo i – classe v – plenário.tc 017.245/2017-6. natureza: Relatório de levantamento. *TCU*, 2018. 18

69 MEIRELLES HELY LOPES, F. J. E. B. *Direito Administrativo Brasileiro,42ª edição, atualizada até a Emenda Constitucional 90.* [S.l.]: Malheiros Editores, 2015. 18

70 GRAEF ALDINO, S. V. Relações de parceria entre poder público e entes de cooperação e colaboração no brasil. *Editora IABS*, 2012. 18, 30

71 GOMES L. F. A.; GOMES, C. F. S. A. A. T. d. Tomada de decisão gerencial: O enfoque multicritério. *Ed. Atlas*, 2006. 18

72 LAKS, I.; WALCZAK, Z. Efficiency of polder modernization for flood protection. case study of golina polder (poland). *Sustainability*, v. 12, n. 19, 2020. ISSN 2071-1050. Disponível em: <https://www.mdpi.com/2071-1050/12/19/8056>. 19

73 BRONIEWICZ, E.; OGRODNIK, K. Multi-criteria analysis of transport infrastructure projects. *Transportation Research Part D: Transport and Environment*, v. 83, p. 102351, 2020. ISSN 1361-9209. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1361920920305381>. 19

74 MARTTUNEN, M.; LIENERT, J.; BELTON, V. Structuring problems for multi-criteria decision analysis in practice: A literature review of method combinations. *European Journal of Operational Research*, v. 263, n. 1, p. 1–17, 2017. ISSN

0377-2217. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0377221717303880>. 19, 31

75 S. BRANCIA A., S. F. L. I. G. Decision support systems and environment: Role of mcda. *Springer, Boston, MA*, 2009. 19

76 PRAKASH B., V. V. A comparative study of meta-heuristic optimisation techniques for prioritisation of risks in agile software development. *International Journal of Computer Applications in Technology*, v. 62, n. 2, p. 175–188, 2020. 19

77 TEKLEMARIAM, M. A.; MNKANDLA, E. Software project risk management practice in ethiopia. *THE ELECTRONIC JOURNAL OF INFORMATION SYSTEMS IN DEVELOPING COUNTRIES*, v. 79, n. 1, p. 1–14, 2017. 19

78 WU, D. et al. A multiobjective optimization method considering process risk correlation for project risk response planning. *Information Sciences*, v. 467, p. 282–295, 2018. ISSN 0020-0255. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0020025518305279>. 19

79 BOEHM, B. Software risk management: principles and practices. *IEEE Software*, v. 8, n. 1, p. 32–41, 1991. 19, 60

80 BUYYA, R. et al. Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, v. 25, n. 6, p. 599–616, 2009. ISSN 0167-739X. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167739X08001957>. 20

81 REED A. H., . A. M. Risk management usage and impact on information systems project success. *International Journal of Information Technology Project Management (IJITPM)*, v. 9, n. 2, p. 1–19, 2018. 20

82 GROUP, T. S. Chaos. *The Standish Group*, 2018. 20

83 GROUP, T. S. Chaos 2020: Beyond infinity overview. *The Standish Group*, 2021. 20

84 BHUKYA S.N., P. S. S. software engineering: risk features in requirement engineering. *Cluster Comput*, v. 22, p. 14789–14801, 2019. 20

85 A.V., G. A. L. Cognitive maps for risk estimation in software development projects. in: Samsonovich a. (eds) biologically inspired cognitive architectures 2019. bica 2019. *Springer, Cham.*, v. 948, 2019. 20

86 CASTRO-RIVERA, V. P.; A, R. A. A. H.-A.; VILLALOBOS-ABARCA, M. A. Desarrollo de un software web para la generaciÃde planes de gestiÃde riesgos de software. *InformaciÃtecnolÃ*, scielocl, v. 31, p. 135 – 148, 06 2020. ISSN 0718-0764. Disponível em: <http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-07642020000300135&nrm=iso>. 20

87 YM. MUñOZ M., M. J. G. G. M. A. G. Application of a risk management tool focused on helping to small and medium enterprises implementing the best practices in software development projects. in: Rocha Á., adeli h., reis l., costanzo s. (eds) trends and advances in information systems and technologies. *WorldCIST'18 2018. Advances in Intelligent Systems and Computing /Springer, Cham.*, v. 746, 2018. 20

88 CHADLI S.Y., I. A. Identifying and mitigating risks of software project management in global software development. *ACM International Conference Proceeding*, p. 12–22, 2017. 21

89 MOUSAEI, M.; GANDOMANI, T. J. A new project risk management model based on scrum framework and prince2 methodology. *International Journal of Advanced Computer Science and Applications*, The Science and Information Organization, v. 9, n. 4, 2018. Disponível em: <http://dx.doi.org/10.14569/IJACSA.2018.090461>. 21

90 SADIA H., A. S. F. M. A systematic literature review of multi-criteria risk factors (vuca) in requirement engineering. *International Journal of Scientific and Technology Research*, v. 8, n. 11, p. 13–20, 2019. 21

91 MENEZES J., G. C. . M. H. Risk factors in software development projects: a systematic literature review. *Software Qual J*, v. 27, p. 1149–1174, 2019. 21

92 KUMAR, C.; YADAV, D. K. A probabilistic software risk assessment and estimation model for software projects. *Procedia Computer Science*, v. 54, p. 353–361, 2015. ISSN 1877-0509. Eleventh International Conference on Communication Networks, ICCN 2015, August 21-23, 2015, Bangalore, India Eleventh International Conference on Data Mining and Warehousing, ICDMW 2015, August 21-23, 2015, Bangalore, India Eleventh International Conference on Image and Signal Processing, ICISP 2015, August 21-23, 2015, Bangalore, India. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1877050915013654>. 21

93 HU Y., Z. X. N. E. W. T. C. R. L. M. Software project risk analysis using bayesian networks with causality constraints. *Decision Support Systems*, v. 56, p. 439–449, 2013. 21

94 INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Iso 31000:2018 risk management — guidelines. 2018. 21, 22, 23, 35, 36, 57, 61, 62, 63, 72, 101, 120

95 INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Nbr iso/iec 31010 - gestão de riscos - técnicas para o processo de avaliação de riscos. 2012. 21, 23, 24, 35, 36, 58, 63, 64, 75, 120

96 POVEDA-ORJUELA, P. P. et al. Parameterization, analysis, and risk management in a comprehensive management system with emphasis on energy and performance (iso 50001: 2018). *Energies*, v. 13, n. 21, 2020. ISSN 1996-1073. Disponível em: <https://www.mdpi.com/1996-1073/13/21/5579>. 23

97 CHEMWENO, P.; PINTELON, L.; DECRE, W. Orienting safety assurance with outcomes of hazard analysis and risk assessment: A review of the iso 15066 standard for collaborative robot systems. *Safety Science*, v. 129, p. 104832, 2020.

ISSN 0925-7535. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0925753520302290>. 23

98 PRINCIPLES OF RISK-BASED ROCK ENGINEERING DESIGN. *Spross, J., Stille, H., Johansson, F. et al.* 2020. 23

99 ASGARI A., K. M. B. Y. A framework for the risk assessment of residual hazardous material in the dynamic environment of a composite production process considering operational time variation. *Process Safety Progress*, 2020. 23

100 DIPPENAAR A., B. S. The development of a robust risk management plan for the continuous supply of water to hospitals in the western cape province. *South African Journal of Industrial Engineering*, v. 30, p. 190–204, 2019. 23

101 PANIć M., V. M. V. D. V. Z. The impact of enterprise risk management on the performance of companies in transition countries: Serbia case study. *Journal of Operational Risk*, v. 14, p. 105–132, 2019. 23

102 BENETTI, K. Challenges of corporate risk management after the global financial crisis. *Contributions to Economics*, p. 3–11, 2019. 23

103 ISHAQUE, M.). managing conflict of interests in professional accounting firms: A research synthesis. *Journal of Business Ethics*, 2019. 23

104 MCSHANE, M. Enterprise risk management: history and a design science proposal. *Journal of Risk Finance*, v. 19, n. 2, p. 137–153, 2018. 23

105 PAULUS, F. Risk management in the proces of the czech republic security management. *Scientific Papers of the University of Pardubice-Series D: Faculty of Economics and Administration*, v. 24, p. 118–128, 2017. 23

106 PARVIAINEN, T. et al. Implementing bayesian networks for iso 31000:2018-based maritime oil spill risk management: State-of-art, implementation benefits and challenges, and future research directions. *Journal of Environmental Management*, v. 278, p. 111520, 2021. ISSN 0301-4797. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0301479720314456>. 23

107 RODRíGUEZ-ROSALES, B. et al. Risk and vulnerability assessment in coastal environments applied to heritage buildings in havana (cuba) and cadiz (spain). *Science of The Total Environment*, v. 750, p. 141617, 2021. ISSN 0048-9697. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0048969720351469>. 23

108 IGRAS, J. D.; CREED, I. F. Uncertainty analysis of the performance of a management system for achieving phosphorus load reduction to surface waters. *Journal of Environmental Management*, v. 276, p. 111217, 2020. ISSN 0301-4797. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0301479720311427>. 23

109 BILSKA, B.; TOMASZEWSKA, M.; KOŁOżYN-KRAJEWSKA, D. Managing the risk of food waste in foodservice establishments. *Sustainability*, v. 12, n. 5, 2020. ISSN 2071-1050. Disponível em: <https://www.mdpi.com/2071-1050/12/5/2050>. 23

110 CREED I. F., D. P. N. S. J. N. S. J. W. N. Managing risks to canada's boreal zone: transdisciplinary thinking in pursuit of sustainability. *Environmental Reviews*, v. 27, n. 3, p. 407–418, 2019. 23

111 BARAFORT, B.; MESQUIDA, A.-L.; MAS, A. Integrating risk management in it settings from iso standards and management systems perspectives. *Computer Standards Interfaces*, v. 54, p. 176–185, 2017. ISSN 0920-5489. Standards in Software Process Improvement and Capability Determination. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0920548916301866>. 23

112 NI, S. et al. A formal model and risk assessment method for security-critical real-time embedded systems. *Computers Security*, v. 58, p. 199–215, 2016. ISSN 0167-4048. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404816000079>. 23

113 GROßMANN J., S. F. Combining security risk assessment and security testing based on standards. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, v. 9488, p. 18–33, 2015. 23

114 CHEMWENO, P. et al. Development of a risk assessment selection methodology for asset maintenance decision making: An analytic network process (anp) approach. *International Journal of Production Economics*, v. 170, p. 663–676, 2015. ISSN 0925-5273. Current Research Issues in Production Economics. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0925527315000857>. 23

115 MATHEU-GARCíA, S. N. et al. Risk-based automated assessment and testing for the cybersecurity certification and labelling of iot devices. *Computer Standards Interfaces*, v. 62, p. 64–83, 2019. ISSN 0920-5489. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0920548918301375>. 23

116 AVEN, T.; YLöNEN, M. Safety regulations: Implications of the new risk perspectives. *Reliability Engineering System Safety*, v. 149, p. 164–171, 2016. ISSN 0951-8320. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0951832016000168>. 23

117 ZHARINOV, S. The role of the library in the digital economy. *Information Technology and Libraries*, v. 39, n. 4, Dec. 2020. Disponível em: <https://ejournals.bc.edu/index.php/ital/article/view/12457>. 24

118 NAMBISAN, S.; WRIGHT, M.; FELDMAN, M. The digital transformation of innovation and entrepreneurship: Progress, challenges and key themes. *Research Policy*, v. 48, n. 8, p. 103773, 2019. ISSN 0048-7333. The Digital Transformation of Innovation and Entrepreneurship. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0048733319300812>. 24

119 MALONE, T. How human-computer' superminds' are redefining the future of work. *MIT Sloan Manage*, v. 59, n. 4, p. 34–41, 2018. 24

120 SUNDARARAJAN, A. The sharing economy: The end of employment and the rise of crowd-based capitalism. *Mit Press*, 2016. 24

121 GAWER, A. Digital platforms' boundaries: The interplay of firm scope, platform sides, and digital interfaces. *Long Range Planning*, v. 54, n. 5, p. 102045, 2021. ISSN 0024-6301. Strategizing in a digital world: Overcoming cognitive barriers, reconfiguring routines and introducing new organizational forms. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0024630120302442>. 24

122 HERMES S., R.-T. C. E. B. M. K. H. The digital transformation of the healthcare industry: exploring the rise of emerging platform ecosystems and their influence on the role of patients. *Business Research*, 2020. 24

123 LI, Y. et al. The impact of sharing economy practices on sustainability performance in the chinese construction industry. *Resources, Conservation and Recycling*, v. 150, p. 104409, 2019. ISSN 0921-3449. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0921344919303040>. 24

124 EMMANOUILIDIS, C. et al. Enabling the human in the loop: Linked data and knowledge in industrial cyber-physical systems. *Annual Reviews in Control*, v. 47, p. 249–265, 2019. ISSN 1367-5788. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1367578818301366>. 24

125 TäUSCHER, K.; LAUDIEN, S. M. Understanding platform business models: A mixed methods study of marketplaces. *European Management Journal*, v. 36, n. 3, p. 319–329, 2018. ISSN 0263-2373. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0263237317300853>. 24

126 BAER, H. Redoing feminism: digital activism, body politics, and neoliberalism. *Feminist Media Studies*, Routledge, v. 16, n. 1, p. 17–34, 2016. Disponível em: <https://doi.org/10.1080/14680777.2015.1093070>. 24

127 HEIN A., S.-M. R. T. S. D. S. W. M. B. M. . K. H. Digital platform ecosystems. *Electronic Markets*, 2019. 24

128 JACOBIDES, M. G.; CENNAMO, C.; GAWER, A. Towards a theory of ecosystems. *Strategic Management Journal*, v. 39, n. 8, p. 2255–2276, 2018. Disponível em: <https://onlinelibrary.wiley.com/doi/abs/10.1002/smj.2904>. 24

129 GUTIéRREZ, V. et al. Empowering citizens toward the co-creation of sustainable cities. *IEEE Internet of Things Journal*, v. 5, n. 2, p. 668–676, 2018. 25

130 EU. The international organisation for research information eurocris. Disponível em: <https://www.eurocris.org/>. Acesso em: 18/02/2021. 25

131 USDA. The united states department of agriculture. Disponível em: <https://reeis.usda.gov/>. Acesso em: 18/02/2021. 25

132 PTCRIS. Portuguese current research information system. Disponível em: <https://ptcris.pt/>. Acesso em: 18/02/2021. 25

133 ICPSR. Inter-university consortium for political and social research. Disponível em: <https://www.icpsr.umich.edu/web/pages/>. Acesso em: 18/02/2021. 26

134 CANARIE. Canarie research software. Disponível em: <https://science.canarie.ca/researchsoftware/home/main.html>. Acesso em: 19/02/2021. 26

135 SAATY, T. L. The analytic hierarchy process. *New York: McGraw-Hill.* 27, 31, 32, 33, 42, 45, 46, 47, 48, 77, 80, 92, 94

136 WU, Z.; XU, J. A concise consensus support model for group decision making with reciprocal preference relations based on deviation measures. *Fuzzy Sets and Systems*, v. 206, p. 58–73, 2012. ISSN 0165-0114. Theme : Operational Research. Disponível em: <https://www.sciencedirect.com/science/article/pii/S016501141200142X>. 27

137 BELTON V.; STEWART, J. *Multiple criteria decision analysis – an integrated approach.* [S.l.]: London: Kluver Academic Publishers, 2002. 28, 31

138 GARTNER. Analysts to explore application strategies at gartner application architecture, development integration summit. *Summit, March 2-3, 2020 in Mumbai, India*. Disponível em: <https://www.gartner.com/en/newsroom/press-releases/2020-01-15-gartner-predicts-50--of-organizations-will-experience>. Acesso em: 29/04/2021. 29

139 FLEURY, M. T. L. A gestão de competência e a estratégia organizacional. As Pessoas na organização. São Paulo: Editora Gente, 2002. 29

140 FORMAN E. H., . G. S. I. The analytic hierarchy process—an exposition. *Operations Research*, v. 49, n. 4, p. 469–486, 2001. 31

141 ABDULLAH L., N. L. Evaluating social sustainable development factors using multi-experts z-fuzzy ahp. *Journal of Intelligent and Fuzzy Systems*, p. 6181–6192, 2014. 33

142 ISO. ecnologia da informação — técnicas de segurança — código de prática para controles de segurança da informação. *ISO*, 2013. 34, 35, 57, 58

143 ISO. Gestão de ativos — visão geral, princípios e terminologia. *ISO*, 2014. 34, 35

144 MáRQUEZ A., G. L. A. J. S. R. A. P. M. C. C. On the family of standards une-iso 55000 and how to effectively manage assets. *Advanced Maintenance Modelling for Asset Management*, p. 1–16, 2017. 35

145 ITGI. Board briefing on it governance, 2nd edition. *IT Governance Institute, Rolling Meadows, Illinois, USA.*, 2003. 38

146 ISACA. Cobit 5 implementation, an isaca framework. *ISACA – Information System Audit and Control Association, Rolling Meadows, Illinois, USA.*, 2012. 38

147 VUGEC D.S., S. M. B. M. It governance adoption in banking and insurance sector: Longitudinal case study of cobit use. *International Journal for Quality Research*, v. 11, n. 3, p. 691–716, 2017. 38

148 CONECTIBRASIL. Instituições oficializam lançamento do conecti. Disponível em: <https://www.conectibrasil.org/instituicoes-oficializam-lancamento-do-conecti/>. Acesso em: 23/08/2021. 38, 39

149 IBICT. Portal brasileiro de publicações científicas em acesso aberto - oasisbr. Disponível em: <https://oasisbr.ibict.br/vufind/>. Acesso em: 26/08/2021. 41

150 CAPES. Plataforma sucupira. Disponível em: <http://portal.mec.gov.br/component/tags/tag/35995>. Acesso em: 26/08/2021. 41

151 CNPQ. Plataforma lattes. Disponível em: <https://lattes.cnpq.br/>. Acesso em: 26/08/2021. 41

152 CONFAP. Confap cris. Disponível em: <https://fapemig.br/pt/noticias/418/>. Acesso em: 26/08/2021. 41

153 SCIELO. Scielo. Disponível em: <http://socialsciences.scielo.org/>. Acesso em: 26/08/2021. 41

154 WINTER, R. Design of situational artefacts-conceptual foundations and their application to it/business alignment. *Information Systems Development - Business Systems and Services: Modeling and Development*, p. 35–49, 2011. 42

155 STEFANO A., C. C.; RICCARDO, O. Policy modeling as a new area for research: perspectives for a systems thinking and system dynamics approach? *Business Systems Laboratory 2nd International Symposium, Universitas Mercatorum, Rome, Italy.*, p. 35–49, 2014. 42

156 BRZK, W. Regulation impact assessment (ria) at poland and at some eu countries. *Procedia-Social and Behavioral Sciences*, v. 109, p. 45–50, 2014. 42

157 IBRAHIM O., L. A. A systems tool for structuring public policy problems and design of policy options. *International Journal of Electronic Governance*, v. 9, n. 1-2, p. 4–26, 2017. 42

158 KANGAS A., K. J. P. J. Outranking methods as tools in strategic natural resources planning open access. *Silva Fennica*, v. 35, n. 2, p. 215–227, 2001. 42

159 ISHIZAKA, A.; LABIB, A. Selection of new production facilities with the group analytic hierarchy process ordering method. *Expert Systems with Applications*, v. 38, n. 6, p. 7317–7325, 2011. ISSN 0957-4174. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0957417410013679>. 43

160 AKHAVI F., H. C. A comparison of two multi-criteria decision-making techniques. *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*, v. 1, p. 956–961, 2003. 43

161 TAHVILI, S. et al. Dynamic integration test selection based on test case dependencies. p. 277–286, 2016. 43

162 LIAO, C. A fuzzy approach to business travel airline selection using an integrated ahp-topsis-msgp methodology. *International Journal of Information Technology & Decision Making*, v. 12, n. 1, p. 119–137, 2013. 43

163 ARASTEH M. A., S. S. Y. P. L. Using multi-attribute decision-making approaches in the selection of a hospital management system. *Technology and Health Care*, v. 26, n. 2, p. 279–295, 2018. 43

164 ITO, T. Soft computing approaches towards design and decision support applications. p. 1–6, 2007. 43

165 LIU Y. N., . W. S. Y. A rule-based approach for dynamic analytic hierarchy process decision-making. *International Journal of Information and Decision Sciences*, v. 12, n. 1, 2020. 43

166 GOOGLE. Formulários. Disponível em: <https://docs.google.com/forms/d/1urYZbYwi-UiIrdAEwnWIfxmX843-7bUrOOhtVa7762Y/edit>. 43, 45

167 SAATY, T. L. Decision-making with the ahp: Why is the principal eigenvector necessary. *European Journal of Operational Research*, v. 145, n. 1, p. 85–91, 2003. ISSN 0377-2217. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0377221702002278>. 45, 80

168 SAATY, T. L. How to make a decision: The analytic hierarchy process. *European Journal of Operational Research*, v. 48, n. 1, p. 9–26, 1990. ISSN 0377-2217. Desicion making by the analytic hierarchy process: Theory and applications. Disponível em: <https://www.sciencedirect.com/science/article/pii/037722179090057I>. 45, 46, 80

169 HO W., D. P. H. H. Multiple criteria decision making techniques in higher education. *International Journal of Educational Management*, v. 20, n. 5, p. 319–337, 2006. 45

170 DECISION, S. Super decision version 3.2. Disponível em: <https://www.superdecisions.com/downloads/>. Acesso em: 13/10/2021. 47, 48, 49

171 UE. Regulamento geral de proteção de dados) – gdpr, regulamento (ue) 2016/679 do parlamento europeu e do conselho,(2016), relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. *Jornal Oficial da União Europeia, L119*, 2016. Disponível em: <https://www.superdecisions.com/downloads/>. 52, 53, 84

172 DECISION, S. Data protection laws for the world. Disponível em: <https://www.dlapiperdataprotection.com/index.html?t=authority&c=US>. Acesso em: 19/09/2021. 53

173 DECISION, S. Federal trade commission. Disponível em: <https://www.ftc.gov/>. Acesso em: 19/09/2021. 54

174 CCPA. California consumer privacy act. Disponível em: <https://oag.ca.gov/privacy/ccpa>. Acesso em: 27/09/2021. 54

175 DPA. Data protection act. Disponível em: <https://www.gov.uk/data-protection>. Acesso em: 19/09/2021. 55

176 DPA. Lei geral de proteção de dados pessoais (lgpd) e setor público.um guia da lei 13.709/2018, voltado para os órgãos e entidades públicas. 2019. Disponível em: <itsrio.org>. 56, 58

177 BRASIL. Decreto nº 10.046, de 9 de outubro de 2019. 2019. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm>. Acesso em: 19/09/2021. 56, 88

178 ABNT. Normas iso 27.001-tecnologia da informação – técnicas de segurança – sistemas de gestão da segurança da informação - requisitos. 2013. 57, 58, 88

179 ISO. Iso/iec 29100:2011-information technology — security techniques — privacy framework. 2011. 57

180 ISO/IEC. Técnicas de segurança — extensão da abnt nbr iso/iec 27001 e abnt nbr iso/iec 27002 para gestão da privacidade da informação — requisitos e diretrizes. 2019. 58, 108, 109, 110, 111

181 ISO/IEC. Tecnologia da informação — técnicas de segurança — gestão de riscos de segurança da informação. 2018. 58, 88

182 SONI S., M. R. Database security: Attacks and solutions.department of i.t. *Mukesh Patel School of Technology and Management,NMIMS, Mumbai, India.A. P. Pandian et al. (Eds.): ICCBI 2019, LNDECT*, v. 49, p. 917–925, 2020, 2019. 58

183 COSO. Gerenciamento de riscos corporativos - estrutura integrada: Sumário executivo e estrutura e gerenciamento de riscos na empresa – integrated framework: Application techniques 2 vol. set, item 990015. 60, 63, 72, 103

184 KONTIO, J. The riskit method for software risk management version 1.00 (cs-tr-3782; umiacs-tr-97-38). *Comput. Sci. Tech. Rep. no. CS-TR-3705*, p. 1–45, 1996. 60

185 WILLIAMS R. C., P. G. J. B. S. G. Software risk evaluation (sre) method description (version 2. 0). *Evaluation*, p. 284, 1999. 60

186 ELMASRI R., N. S. *Sistema de Banco de Dados, 6º Edição*. [S.l.]: Pearson, 2011. ISBN 8579360854. 61

187 SILBERSCHATZ A., K. H. S. S. *Sistema de Banco de Dados, tradução da 5º edição*. [S.l.]: Campus, 2006. ISBN 9788535211078. 61

188 CIS. Center for internet security. 2021. Acesso em: 24/10/2021. 61, 64, 109, 111

189 PAPPAS, V. et al. Blind seer: A scalable private dbms. p. 359–374, 2014. 61

190 SHYAMASUNDAR R. K., C. P. J. A. K. A. Approaches to enforce privacy in databases: Classical to information flow-based models. *Information Systems Frontiers*, v. 23, n. 4, p. 811–833, 2021. 62

191 FISCH, B. A. et al. Malicious-client security in blind seer: A scalable private dbms. p. 395–410, 2015. 62

192 SALAS J., D.-F. J. Some basics on privacy techniques, anonymization and their big data challenges. *Mathematics in Computer Science*, 2018. 62

193 DATA Base Management Systems (DBMSs): Meeting the requirements of the EU data protection legislation. *International Journal of Information Management*, v. 23, n. 3, p. 185–199, 2003. ISSN 0268-4012. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0268401203000239>. 62, 66

194 DOSHI, J. C.; TRIVEDI, B. Hybrid intelligent access control framework to protect data privacy and theft. p. 1766–1770, 2015. 62

195 OWASP. Open web application security project owasp. 2021. Disponível em: <https://owasp.org/>. Acesso em: 27/10/2021. 64, 65, 66, 104, 106, 111

196 DISA. Defense information systems agency disa. 2021. Disponível em: <https://www.disa.mil/>. Acesso em: 27/10/2021. 64

197 PONEMON. Ponemon institute cost of data breach. 2021. Disponível em: <https://www.ponemon.org/>. Acesso em: 27/10/2021. 66

198 BOWLES, J. B.; PELáEZ, C. Fuzzy logic prioritization of failures in a system failure mode, effects and criticality analysis. *Reliability Engineering System Safety*, v. 50, n. 2, p. 203–213, 1995. ISSN 0951-8320. Disponível em: <https://www.sciencedirect.com/science/article/pii/095183209500068D>. 72, 75, 76, 93

199 LIU, H.-C. et al. Failure mode and effect analysis using multi-criteria decision making methods: A systematic literature review. *Computers Industrial Engineering*, v. 135, p. 881–897, 2019. ISSN 0360-8352. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0360835219303857>. 72, 73

200 PUJADAS F. PARDO-BOSCH, A. A.-R. P.; AGUADO, A. Mives multi-criteria approach for the evaluation, prioritization, and selection of public investment projects. a case study in the city of barcelona. *Land Use Policy*, v. 64, p. 29–37, 2017. 73

201 SARRAZIN, R.; SMET, Y. D. Applying multicriteria decision analysis to design safe road projects. *European Journal of Transport and Infrastructure Research*, v. 15, n. 4, p. 613–634, 2015. 73

202 BIAN T., Z. H.-Y. L. . D. Y. Failure mode and effects analysis based on d numbers and topsis. *Quality and Reliability Engineering International*, v. 34, n. 4, p. 501–515, 2018. 74, 80

203 SACHDEVA A., K. D.-K. P. Multi-factor faillure mode critically analysis using topsis. *Journal of industrial engineering international [online]*, v. 5, n. 8, p. 1–9, 2009. Disponível em: <https://www.sid.ir/en/journal/ViewPaper.aspx?id=137520>. 74

204 OZDEMIR, Y.; GUL, M.; CELIK, E. Assessment of occupational hazards and associated risks in fuzzy environment: A case study of a university chemical laboratory. *Human and Ecological Risk Assessment: An International Journal*, Taylor Francis, v. 23, n. 4, p. 895–924, 2017. Disponível em: <https://doi.org/10.1080/10807039.2017.1292844>. 75

205 LIU, H.-C.; LIU, L.; LIU, N. Risk evaluation approaches in failure mode and effects analysis: A literature review. *Expert Systems with Applications*, v. 40, n. 2, p. 828–838, 2013. ISSN 0957-4174. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0957417412009712>. 75, 76

206 OTURAKCI, M.; DAGSUYU, C. Integrated environmental risk assessment approach for transportation modes. *Human and Ecological Risk Assessment: An International Journal*, Taylor Francis, v. 26, n. 2, p. 384–393, 2020. Disponível em: <https://doi.org/10.1080/10807039.2018.1510730>. 75, 77, 80, 81

207 CHANG, K.-H. Evaluate the orderings of risk for failure problems using a more general rpn methodology. *Microelectronics Reliability*, v. 49, n. 12, p. 1586–1596, 2009. ISSN 0026-2714. Special Section on Electrostatic Discharge Reliability. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0026271409003096>. 76

208 COMPANY, F. M. Potential failure mode and effects analysis (fmea) reference manual. 1988. 76

209 OZTAYSI, B. A decision model for information technology selection using ahp integrated topsis-grey: The case of content management systems. *Knowledge-Based Systems*, v. 70, p. 44–54, 2014. ISSN 0950-7051. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0950705114000598>. 77, 79, 81

210 LI F., W. X.-H. Z. Y. C. Research on computing weight of customer satisfaction based on fuzzy ahp. *Computer Engineering and Applications*, v. 42, n. 3, p. 100–102, 2006. 77, 81

211 KIRIS, S. Ahp and multichoice goal programming integration for course planning. *International Transactions in Operational Research*, v. 21, p. 819–833, 2014. 77, 81

212 HWANG C.-L., Y.-K. Methods for multiple attribute decision making. *Lecture Notes in Economics and Mathematical Systems*, p. 58–191, 1981. 77, 80, 95, 96, 98, 99, 102

213 ERTUğRUL İrfan; KARAKAşOğLU, N. Performance evaluation of turkish cement firms with fuzzy analytic hierarchy process and topsis methods. *Expert Systems with Applications*, v. 36, n. 1, p. 702–715, 2009. ISSN 0957-4174. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0957417407005349>. 77

214 LIU H.-C., Y.-J.-X. S. M.-M. S. L.-N. Failure mode and effects analysis using intuitionistic fuzzy hybrid topsis approach. *Soft Computing*, v. 19, n. 4, p. 1085–1098, 2014. 77

215 PW, P. R. B. Appication of ahp and topsis method for supplier selection problem. *IOSR J Eng*, v. 2, n. 10, p. 43–50, 2012. 79

216 F FALLAHNEJAD R, N. N. H. L.). ranking efficient units in dea by using topsis method. *Appl Math Sci*, v. 5, n. 17, p. 805–815, 2011. 79

217 SOUZA L. P., G. C. F. S.-D. B. A. P. D. Implementation of new hybrid ahp–topsis-2n method in sorting and prioritizing of an it capex project portfolio. *International Journal of Information Technology & Decision Making*, v. 17, n. 4, p. 977–1005, 2018. 79

218 ZYOUD S. H., K. L. S. H. S.-S. F.-H. D. A framework for water loss management in developing countries under fuzzy environment: Integration of fuzzy ahp with fuzzy topsis. *Expert Systems With Applications*, v. 61, p. 86–105, 2016. 79

219 WALCZAK D., R. A. Rutkowska, project rankings for participatory budget based on the fuzzy topsis method. *European Journal of Operational Research*, v. 60, p. 706–714, 2017. 80

220 ANDRADE J.M.M., L. A. C. M. S. A.-L. E.-J. O. A multi-criteria approach for fmea in product development in industry 4.0. *Transdisciplinary Engineering for Complex Socio-technical Systems – Real-life Applications J. Pokojski et al. (Eds.).*, 2020. 80

221 FILHO J.C. BATTIROLA, P. F. L. E. S.-E. Process-aware fmea framework for failure analysis in maintenance. *Journal Of Manufacturing Technology Management*, v. 28, p. 822–848, 2017. 80

222 ZYOUD S.H., F.-H. D. A bibliometric-based survey on ahp and topsis techniques. *Expert systems with applications*, v. 78, p. 158–168, 2017. 80

223 AHSAN, K.; RAHMAN, S. Green public procurement implementation challenges in australian public healthcare sector. *Journal of Cleaner Production*, v. 152, p. 181–197, 2017. 81

224 ROSZAK M., S.-M. K. A. Environmental failure mode and effects analysis (fmea) - a new approach to methodology. *Metalurgija*, v. 54, n. 2, p. 449–451, 2015. 92

225 WANG, W. et al. A risk evaluation and prioritization method for fmea with prospect theory and choquet integral. *Safety Science*, v. 110, p. 152–163, 2018. ISSN 0925-7535. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0925753517320635>. 92

226 WAN, N. et al. Risk assessment in intelligent manufacturing process: A case study of an optical cable automatic arranging robot. *IEEE Access*, p. 105892–105901, 2019. 92

227 STANDARDS, N. I. of; TECHNOLOGY-NIST. Security and privacy controls for federal information systems and organizations. *Special Publication 800-53 - Revision 4*, 2015. 104, 105, 106, 107, 108, 110, 111

228 MORAES, G. Sistema de gestão de riscos - princípios e diretrizes - iso 31.000 comentada e ilustrada. *GVC Editora*, 2016. 113, 114, 115, 116

229 FERREIRA H., C. M. G. R. Uma experiência de desenvolvimento metodológico para avaliação de programas: o modelo lógico do programa segundo tempo. *IPEA*, 2009. 113, 114, 115