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

Gestão de riscos e continuidade de negócios aplicado ao sistema SEI na Universidade de Brasília

Cristiano Magno de Morais

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

Orientador
Prof. Dr. Ricardo Matos Chaim

Brasília
2022

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

Mg

Magno de Morais, Cristiano
Gestão de riscos e continuidade de negócios aplicado ao sistema SEI na Universidade de Brasília / Cristiano Magno de Morais; orientador Ricardo Matos Chaim. -- Brasília, 2022.
117 p.

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

1. Gestão de Riscos. 2. Continuidade de negócios. 3. Sistema Eletrônico de Informações. I. Matos Chaim, Ricardo, orient. II. Título.

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

Gestão de riscos e continuidade de negócios aplicado ao sistema SEI na Universidade de Brasília

Cristiano Magno de Morais

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

Prof. Dr. Ricardo Matos Chaim (Orientador)
CIC/UnB

Prof. Dr. João de Souza Neto
UBEC/UCB

Prof. Dr.a Leticia Lopes Leite
CIC/UnB

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

Brasília, 25 de Março de 2022

Dedicatória

A Deus, pela vida e oportunidades. A minha esposa, pilar fundamental de meus esforços e vitórias. Aos meus pais pela formação e educação e a todos que participaram desta jornada importante em minha formação pessoal e profissional.

Agradecimentos

Agradeço a todos cuja participação e conhecimentos contribuíram para realização deste trabalho.

Ao orientador, Ricardo Chaim, pelos ensinamentos, paciência e ajuda, seu entusiasmo nos conselhos me incentivaram a continuar mesmo em momentos de pensamento de desistência.

Aos meus colegas de setor na STI que me ajudaram a entender processos e informações durante o período de coleta de dados.

Aos Professores João de Souza Neto e Letícia Lopes Leite pela ajuda na pesquisa e orientações valiosas durante a elaboração deste trabalho.

Aos professores do Programa de Pós-Graduação em Computação Aplicada da Universidade de Brasília pelo comprometimento, pela seriedade e dedicação a nós, alunos.

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

Como qualquer instituição de ensino superior a Universidade de Brasília (UnB) possui informações críticas que são tratadas como ativos de informação e não estão livres de indisponibilidades oriundas de diversos riscos e ameaças internas e externas à organização.

Neste estudo de caso o objetivo é analisar a aplicabilidade de um Sistema de Gestão de Continuidade de Negócios (SGCN) para mitigar riscos operacionais relacionados a sustentação do Sistema Eletrônico de Informação (SEI) sobe guarda técnica da Secretaria de Tecnologia da Informação (STI) da Universidade de Brasília (UnB). Foram realizados levantamentos de estudos relacionados à gestão de continuidade de negócios; Pesquisas para conhecer processos e documentos utilizados para tratamento, desenvolvimento e sustentação do SEI; Identificados os ativos primários e de suporte ao sistema suas vulnerabilidades e ameaças; Foi realizada a análise de riscos em termos de probabilidade e impacto em eventos do sistema e por fim, foi feita a análise da aplicabilidade da proposta de desenvolvimento de um SGCN para o SEI disponibilizado a comunidade acadêmica da UnB. Desta forma, foi possível concluir que a STI pode utilizar um SGCN para aprimorar a resiliência e mitigar riscos operacionais relacionados ao sistema SEI utilizado na UnB.

Palavras-chave: Continuidade de negócios, Gestão de Riscos, Recuperação, Sistema eletrônico de informações, Risco Operacional

Abstract

Like any higher education institution, the University of Brasília (UnB) has critical information that is treated as information assets and is not free from unavailability arising from various risks and threats, internal and external to the organization.

In this case study, the objective is to analyze the applicability of a Business Continuity Management System (SGCN) to mitigate operational risks related to the maintenance of the Electronic Information System (SEI) system under the technical guard of the Information Technology Department (STI) of the University of Brasília (UnB). Surveys of studies related to the management of business continuity were carried out; Researches to know the processes and documents used for the treatment, development and support of the SEI; Identified the primary and system support assets, their vulnerabilities and threats; A risk analysis was carried out in terms of probability and impact on system events and, finally, an analysis of the applicability of the proposal to develop a SGCN for the SEI was made available to the academic community of UnB. In this way, it was possible to conclude that the STI can use a SGCN to improve resilience and mitigate operational risks related to the SEI system used at UnB.

Keywords: Business continuity, Risk management, Recovery, electronic information system, Operational Risk

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas e Siglas

ACE Arquivo Central.

BCE Biblioteca Central.

BIA Business Intelligence Analyst.

CAD Conselho de Administração.

CAPES Coordenação de Aperfeiçoamento de Pessoal de Nível Superior.

CPD Centro de Informática.

DPO Decanato de Planejamento, Orçamento e Avaliação Institucional.

DRP Disaster Recovery Plan.

ETIR Equipe de Tratamento de Resposta a Incidentes.

FUB Fundação Universidade de Brasília.

GCN Gestão de Continuidade de Negócios.

GED Gerenciamento de Documentos Eletrônicos.

GR Gestão de Riscos.

ISO Organização Internacional de Normalização.

ITIL Information Technology Infrastructure Library.

LAI Lei de acesso a informação.

LGPD Lei geral de proteção de dados.

MEC Ministério da Educação.

PCN Plano de Continuidade de negócios.

PDTI Plano Diretor de Tecnologia da Informação e Comunicação.

POSIC Política de Segurança da Informação e Comunicação.

SEI Sistema Eletrônico de Informação.

SGCN Sistema de Gestão de Continuidade de Negócios.

SI Segurança da Informação.

SLA Service Level Agreement.

STI Secretaria de Tecnologia da Informação.

TCU Tribunal de Contas da União.

TEMAC Teoria do Enfoque Meta Analítico Consolidado.

TI Tecnologia da Informação.

TIC Tecnologia da informação e comunicação.

UnB Universidade de Brasília.

WoS Web Of Science.

Capítulo 1

INTRODUÇÃO

Este capítulo apresenta a contextualização do tema investigado, o problema de pesquisa, a justificativa e os objetivos geral e específicos.

1.1 Contextualização

A continuidade de negócios é fundamentada na gestão de riscos, sendo definido os passos a serem seguidos no caso de um evento adverso. As instituições de ensino superior, com o avanço da tecnologia e da ciência, utilizam-se de recursos tecnológicos como ferramenta de pesquisa e manutenção administrativa. Atualmente o mundo está cada vez mais dependente de tecnologia, sendo praticamente impossível imaginar como algumas atividades podem ser realizadas sem o uso de um computador, tablet ou smartphone. A indisponibilidade de serviços criticos de tecnologia causam perdas financeiras e de imagem as instituições.

Gerir riscos e documenta-los é essencial para conter eventos de indisponibilidade. Grande parte das empresas tratam indisponibilidades apenas no momento em que ocorrem de maneira reativa, sem documentações e conhecimento de eventos semelhantes que ocorreram anteriormente, que já tenham sido tratados e que poderiam auxiliar na resolução de novos problemas. Possivelmente isso ocorre porque o planejamento de riscos é um procedimento que gera custos financeiros e tempo, não sendo um processo evidente nas organizações. Assim, quando se planeja o tratamento de riscos não se sabe se realmente vai utilizar esse planejamento, porém, com o avanço da tecnologia, um planejamento de risco não é visto como se será utilizado, mas agora o pensamento é de quando será utilizado.

A necessidade de oferecer serviços digitais com alta disponibilidade se tornou ainda mais evidente para empresas e órgãos públicos com a pandemia do novo Coronavírus (Covid-19). O trabalho remoto tornou-se realidade de muitas empresas, o sistema de ensino passou a ser muito mais a distância e os serviços de entrega tornaram-se muito

mais atrativos. Todos esses serviços são dependentes de tecnologia. Esse movimento obriga um maior cuidado com a infraestrutura de TI, que deve ser capaz de suportar a demanda com eficiência.

A Universidade de Brasília UnB foi inaugurada em 1962 com a promessa de reinventar a educação superior, entrelaçar as diversas formas de saber e formar profissionais engajados na transformação do país. Possuí missão de ser uma universidade inovadora e inclusiva, comprometida com as finalidades essenciais de ensino, pesquisa e extensão integradas para a formação de cidadãs e cidadãos éticos e qualificados para o exercício profissional, empenhados na busca de soluções democráticas para questões nacionais e internacionais, por meio de atuação de excelência [1]. Foi constituída como fundação, de acordo com Darcy Ribeiro,

> "A UnB foi organizada como uma Fundação, a fim de libertá-la da opressão que o burocratismo ministerial exerce sobre as universidades federais. Ela deveria reger a si própria, libre e responsavelmente, não como uma empresa, mas como um serviço público autônomo"[2].

A Secretaria de Tecnologia da Informação (antigo Centro de Informática Centro de Informática (CPD)) foi criado em 1991, com a sigla CIn, para suceder ao então Centro de Processamento de Dados e posteriormente para Secretaria de Tecnologia da Informação STI em 2020 de acordo com a resolução do Conselho Universitário nº 0012/2020, sendo um órgão complementar, criado na época da instalação da Universidade de Brasília com o intuito de desenvolver as atividades de caráter permanente de apoio, necessárias ao desenvolvimento do ensino,da pesquisa e da extensão no que se refere ao processamento de dados, de acordo com informações da página web da Secretaria [3].

A STI armazena dados cadastrais, científicos, administrativos e organizacionais de aproximadamente 50.000 discentes de graduação e pós-graduação e cerca de 10.000 prestadores de serviço, servidores públicos técnicos administrativos, estagiários e professores, conforme anuário estatístico [4], este documento traz informações sobre a população universitária da UnB. Os dados armazenados pela STI, apesar de alguns deles serem informações particulares, ao momento do ingresso no órgão público, passaram a ser tratados também com informações públicas devendo ser preservadas de acordo com a lei nº 8.159 de 1991 que dispõe sobre a política nacional de arquivos públicos e privados e a lei nº 12.527 de 2011 que regula o acesso a informação em órgão públicos.

O SEI foi introduzido na Universidade de Brasília com o intuito de revolucionar a forma de produzir e tramitar documentos no contexto administrativo e com isso, resolver vários problemas já identificados como os diversos arquivos físicos localizados em vários departamentos. Sendo assim, resolveria o acúmulo de documentos físicos, ou seja, a falta

de espaço nos setores de trabalho para armazenamento, extravio de documentos, perda de tempo para localização de peças e processos.

O SEI utilizado na Universidade de Brasília é um dos serviços críticos sobre guarda da Secretaria de Tecnologia da Informação e gestão do Arquivo Central (ACE). A indisponibilidade deste serviço impacta diretamente a continuidade da prestação de serviços a comunidade acadêmica. Por isso, é de extrema importância o levantamento de riscos, ameaças e planejamento de ações a serem realizadas em momentos de indisponibilidade. Esses levantamentos tem como objetivo mitigar riscos operacionais relacionados a este serviço e tornar o sistema e sua infraestrutura mais resiliente.

A proposta desta pesquisa visa analisar as melhores estratégias para mensura a resiliência do ambiente tecnológico que comporta o Sistema Eletrônico de Informações utilizado na UnB, no âmbito da gestão de riscos e continuidade de negócios, no contexto da criticidade que este sistema representa para a instituição.

1.2 Definição do problema

Os recentes eventos de indisponibilidade de serviços de Tecnologia da Informação (TI) de órgãos de grande importância do governo federal e gigantes do ramo de tecnologia, sinalizaram com um ponto de atenção os gestores de TI, o qual, diz respeito à disponibilidade e continuidade de serviços de tecnologia em casos de eventos extremos.

A Secretaria de tecnologia da informação da Universidade de Brasília, destaca-se no comprometimento em garantir o efetivo atendimento às demandas de Tecnologia da informação e comunicação (TIC) e a constante disponibilidade e guarda de dados de sistemas e serviços prestados à comunidade da UnB, visando o atendimento com excelência as atividades de ensino, pesquisa, extensão, inovação e gestão da instituição de ensino superior, conforme seu Plano Diretor de Tecnologia da Informação e Comunicação (PDTI) [5], cujo os objetivos são definidos com o intuito de se alcançar maior eficácia e eficiência no suporte as atividades da UnB no uso de tecnologia da informação.

Assim sendo, a seguinte indagação para simplificar essa exploração pode ser sintetizada da seguinte forma:

Um sistema de continuidade de negócios e seus elementos podem tornar o Sistema Eletrônico de Informações, sobe guarda tecnológica da STI, mais resiliente?

1.3 Justificativa

A comunidade acadêmica demanda cada dia mais novas tecnologias e armazenamento de informações. Fornecer e proteger dados e serviço é função da área de tecnologia da

Universidade de Brasília. Se preparar para eventos de indisponibilidade é fundamental para qualquer organização, não sendo diferente em relação a instituições de ensino. O sistema SEI é um dos serviços críticos sobre guarda tecnológica da STI, sendo evidente a necessidade de processos bem estruturados para manter a disponibilidade deste serviço aos usuários.

Analisar riscos em tecnologia é parte fundamental do processo de continuidade de negócios. De acordo com a ISO 27005:2019 [6], "O risco de segurança da informação está associado com o potencial de que ameaças possam explorar vulnerabilidades de um ativo de informação ou grupo de ativos de informação e, consequentemente, causar danos a uma organização."

Uma gestão de riscos adequada busca dentre outros benefícios, o aumento da probabilidade de alcance dos objetivos traçados, o aprimoramento do processo de identificação de oportunidades e ameaças, o fornecimento de uma base sólida e segura para a tomada de decisão e planejamento, o aprimoramento da eficácia na alocação e do uso de recursos, a melhoria da eficiência e a redução das perdas e dos custos, a melhora da conformidade com os requisitos legais e normativos, além do aprimoramento do controle e da governança institucional.

A crescente demanda por alocação de recursos computacionais gerados pelo crescimento exponencial das informações a serem administradas pela STI, impulsionou a necessidade constante de revisão de processos e capacidade computacional, com o intuito de fazer frente as necessidades requeridas pela comunidade universitária. Desta forma, sabe-se da forte dependência dos meios de comunicação como internet, e-mails e sistemas administrativos, tornando-se vital para a UnB a alta disponibilidade de serviços de TI. A gestão de TI deve estar preparada não só para demandas do dia a dia, mas também para aquelas derivadas de eventos que coloquem em risco a continuidade dos serviços, de modo a evitar possíveis interrupções no atendimento e prestação continuada de serviços à comunidade acadêmica.

O sistema SEI, atualmente um dos serviços críticos sobre guarda da STI, possui infraestrutura de tecnologia robusta e pessoal técnico para administração. Devido a sua criticidade e importância na rotina administrativa da instituição, é de extrema importância a gestão de riscos relacionados a disponibilidade deste sistema e o planejamento para continuidade deste serviço em casos de indisponibilidade.

Para a instituição de ensino e para a Secretaria tecnologia, esta pesquisa apresentará uma oportunidade de definir padrões de continuidade de negócio e levantamento de riscos, adequando a Secretaria há normas e requisitos internos e externos de qualidade de serviços de tecnologia, assim como, possibilitará maior entendimento dos riscos relevantes a serem avaliados, possibilitando maior eficiência e contribuindo para a melhoria do resultado

junto a comunidade acadêmica, sociedade e órgãos reguladores.

Sobre a ótica do autor, esta pesquisa se faz motivadora como forma de apresentação da cultura de continuidade de negócios e levantamento de analise de risco sobre serviços críticos de tecnologia ofertados a comunidade acadêmica da Universidade de Brasília. Tendo em vista que o foco da área de TI da instituição é o atendimento com excelência das atividades de ensino, pesquisa, extensão, inovação e gestão, a busca da eficiência operacional, acredita-se que seja uma contribuição relevante com grande possibilidade de implementação, sendo útil para a organização.

Desta forma, pretende-se que os resultados obtidos nesta pesquisa sejam úteis para levantamento de métodos e modelos de gestão de continuidade de negócios, que possam contribuir no sentido de representar coerentemente a realidade e as especificidades da área de tecnologia da instituição de ensino.

1.4 Objetivos

Nesta pesquisa de mestrado pretende-se alcançar o objetivo geral descrito, assim como seus objetivos específicos.

1.4.1 Objetivo Geral

O objetivo geral desta pesquisa é analisar a aplicabilidade de um Sistema de Gestão de Continuidade de Negócios para tratar riscos operacionais ao Sistema Eletrônico de Informações sobe guarda da Secretaria de Tecnologia da Informação da UnB.

1.4.2 Objetivos Específicos

Para alcançar o objetivo geral desta pesquisa, destacam-se os seguintes objetivos específicos, que considerados em seu conjunto contribuirão para o alcance do resultado final da pesquisa:

1. Realizar levantamento de estudos relacionados à metodologia de desenvolvimento de continuidade de negócio que possam ser analisados no contexto desta pesquisa;
2. Conhecer processos e documentações utilizadas para tratamento de eventos críticos ocorridos no sistema SEI utilizado na UnB;
3. Identificar ativos primários e suporte ao sistema SEI, assim como suas ameaças e vulnerabilidades;
4. Analisar riscos em termos de probabilidade e impacto relacionados ao sistema SEI;

5. Analisar a importância e a aplicabilidade da proposta de desenvolvimento de um Sistema de Gestão de Continuidade de Negócios para o Sistema Eletrônico de Informação em produção na Universidade de Brasília.

1.5 Estrutura do Trabalho

Esta pesquisa está estruturada da seguinte forma: O capítulo 1 se divide em seis tópicos que retratam respectivamente a contextualização, define o problema que motivou a elaboração do estudo, define os objetivos, central e intermediários, compreendendo na sequência os limites deste estudo e se conclui com a descrição da estrutura de trabalho.

A fundamentação teórica dos assuntos relevantes para a avaliação de trabalhos de continuidade de negócios é apresentada no capítulo 2. Neste capítulo é realizada uma revisão sistemática da literatura utilizando a Teoria do Enfoque Meta Analítico Consolidado (TEMAC). O Objetivo deste capítulo é direcionar os esforços da pesquisa e garantir que trabalhos relevantes tenham sido considerados. Desta forma, são apresentados os principais temas de pesquisa relacionados a continuidade de negócios.

A metodologia aplicada, com detalhamento do ambiente, é dissertada no capitulo 3. As etapas metodológicas e recursos utilizados na elaboração da pesquisa a metodologia do trabalho através de quatro grupos. O primeiro sobre o objetivo, a classificação, finalidade, estrutura e tipo da pesquisa, o segundo sobre o local e objeto estudado, o terceiro sobre as técnicas, instrumentos e os procedimentos na coleta de dados, o quarto sobre os critérios e ferramentas de análise de dados e coleta.

No capítulo 4 são apresentados e analisados, em detalhes os resultados, dada sua importância para melhorar o entendimento das técnicas estudadas.

Por fim, no capítulo 5 são discutidas as implicações práticas, importância e aplicabilidade de um modelo de continuidade de negócios, finalizando o estudo com as conclusões.

O apêndice têm por intuito contribuir com outros pesquisadores que queiram replicar este trabalho, apresentando tabelas de informações e documentações utilizadas durante o processo de construção de resultados desta pesquisa.

Capítulo 2

REFERENCIAL TEÓRICO

Para atender o objetivo específico 1 desta pesquisa, nesta seção são apresentados os principais temas de pesquisa relacionados à gestão de continuidade de negócios, como esta pesquisa foi desenvolvida e de que maneira tem evoluído, bem como suas vantagens e dificuldades de implementação.

2.1 Sistema de Gestão de Continuidade de Negócios

A continuidade de negócios contribui para organizações mais resilientes sendo um importante mecanismo de prevenção à ocorrência de desastres, assim como, é possível afirmar que a continuidade de negócios é fundamentada na gestão de riscos. De acordo com a ISO 15999-1:2008 [7], a gestão de continuidade de negócios é complementar a uma estrutura de gestão de riscos que busca entender os riscos às operações de negócio e suas consequências. Ainda de acordo com a norma, a Gestão de Continuidade de Negócios (GCN) é um elemento importante da gestão de negócios, fornecimento de serviços e prudência empresarial, sendo que em alguns casos, as organizações têm obrigações legais ou regulamentares de efetuar uma GCN.

Quando se fala em Plano de Continuidade de negócios (PCN), estamos falando de prevenção em TI, onde o seu objetivo é garantir que os sistemas críticos de uma empresa retornem à condição operacional regular em um prazo aceitável após o uma ocorrência de incidente. De acordo com Bajgoric [8], "[...] O objetivo geral da continuidade de negócios é identificar, planejar, implementar e manter de várias formas a operação se uma organização enfrentar uma crise."

Um PCN reforça a importância de entender as necessidades da organização e a necessidade de estabelecer políticas e objetivos para a gestão de continuidade de negócios, assim como, implementar e operar controles e medidas para a gestão da capacidade geral da organização, a fim de gerenciar incidentes de interrupção.

> "[...] O plano de continuidade de negócios pode ser um indicador de quão bem uma organização se prepara para defender seus negócios para que as atividades possam continuar a funcionar mesmo em eventos de indisponibilidade ou por desastres inesperados"[9].

O ciclo de vida de GCN é composto por elementos que podem ser implementados em organizações de todos os tamanhos, em todos os setores: público, privado, sem fins lucrativos, educacional, etc. O escopo e a estrutura proposto podem variar e o esforço gasto pode ser adaptado às necessidades de cada organização.

De acordo com a figura 2.1 a gestão do programa possibilita que a capacidade de continuidade de negócios seja restabelecida e mantida de forma apropriada ao tamanho do negócio e complexidade. O entendimento da organização fornece informações que permitem a priorização dos produtos e serviços e as urgências das atividades. Determinar estratégias permite uma resposta rápida e apropriada para cada serviço e o desenvolvimento e implementação de um GCN resulta na criação de uma estrutura de gestão e numa estrutura de gerenciamento de incidentes, continuidade e recuperação de negócios que detalhem os passos a serem tomados durante e após um incidente, para manter e restaurar as operações.

Figura 2.1: Ciclo de vida da gestão de continuidade de negócios
Fonte: ABNT NBR ISO 15999-1:2007

A participação da alta direção é fundamental para garantir que o processo de gerenciamento de continuidade de negócios seja corretamente introduzido, suportado e estabelecido como parte da cultura da organização. Para Graham e Kaye [10], "O plano de continuidade de negócios requer o comprometimento de toda a administração e terceiros para manter o serviço disponível".

A ISO 22301:2013 [11], refere-se ao SGCN e define os requisitos para implantação do sistema. Esta norma reforça a importância de se entender as necessidades da organização e a condição imprescindível do estabelecimento de políticas e objetivos para a GCN e ainda demonstrar os requisitos necessários para estabelecer e gerenciar de forma eficaz um plano de continuidade de negócios sendo aplicável a qualquer organização, independentemente do tamanho, setor e tipo de produto ou serviço prestado.

De acordo com a norma 15999-1:2007 [7], a gestão de continuidade de negócios é um processo da organização que estabelece a estrutura estratégica e operacional adequada para melhorar proativamente a resiliência da organização contra possíveis interrupções de sua capacidade em atingir seus principais objetivos e promover uma prática para restabelecer a capacidade de uma organização fornecer seus principais serviços e obter capacidade de gerenciar uma interrupção nos serviços do negócio.

A norma ISO 22301:2013 [11] emprega a abordagem de processos para incorporar o ciclo PDCA com o objetivo de planejar, estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a continuidade e a eficácia do SGCN.

Plan (Estabelecer)	Estabelecer uma política de continuidade de negócios, objetivos, metas, controles, processos e procedimentos pertinentes para a melhoria da continuidade de negócios de forma a ter resultados alinhados com os objetivos e políticas gerais da organização.
Do (Implementar e operar)	Implementar e operar a política de continuidade de negócios, controles, processos e procedimentos.
Check (Monitorar e analisar criticamente)	Monitorar e analisar criticamente o desempenho em relação aos objetivos e política de continuidade de negócios, reportar os resultados para a direção para análise crítica, e definir e autorizar ações de melhorias e correções.
Act (Manter e melhorar)	Manter e melhorar o SGCN tomando ações corretivas e preventivas, baseadas nos resultados da análise crítica pela direção e reavaliando o escopo do SGCN e as políticas e objetivos de continuidade de negócios.

Tabela 2.1: Explicação do modelo PDCA ISO 22301:2013

O ciclo PDCA explicado na tabela 2.1 é mundialmente utilizado visando um controle mais eficiente de processos e atividades, sendo eles externos ou internos, minimizando as chances de erros na tomada de decisões e padronizando informações de relevância priorizando a melhoria continua do processo.

Desta forma, é possível que seja necessário envolver no processo de recuperação a comunidade em geral, assim como outras organizações em função do impacto no ambiente organizacional [11].

2.1.1 Recuperação de Desastres

Pode-se argumentar que um possível impedimento ao planejamento de recuperação de desastres é o público, indiferente do desastre. O estudioso Raymond Burby [12], observa que desastres naturais se enquadram em uma classe geral de questões de planejamento que têm um público fraco. Ao contrário de questões que atraem amplo interesse público, como melhorias em transporte público ou revitalização de um bairro, a recuperação de desastre carece de representantes que visualizam os problemas e estão ativamente envolvidos em uma forma de como poderão lidar com eles. A falta de apoio pode ser porque os custos de planejamento de recuperação são imediatos, os benefícios são a longo prazo e incertos, e as manifestações físicas do planejamento de recuperação pré-desastre não são visíveis até o pós-desastre [13].

Incidentes recentes de grande divulgação ilustram a exposição a desastres naturais. Por exemplo, os autores Engemann, Miller e Yager [14], relatam em seu trabalho as crescentes dependências em relação a computação, telecomunicação e tecnologias, onde todas elas sobrecarregam a gestão de TI com vulnerabilidades e expõem o porquê novas tecnologias dependem tanto de Data Centers e os possíveis riscos e preocupações que envolvem esse tido de guarda de ativos. Os exemplos citados pelos autores são: Tempestades, Furações, Terremotos, falta de energia e outros.

A abordagem gerencial para facilitar o planejamento de guarda de informações em Data Centers em relação a problemas ocorridos por eventos de desastres naturais é desenvolver um plano de recuperação de desastres ou o termo mais utilizado em inglês Disaster Recovery Plan (DRP). Tais fatos elevaram a importância e expansão do estudo do GCN, que é um programa holístico de gerenciamento que identifica eventos potenciais que ameaçam uma organização e fornecem uma estrutura para resiliência desses serviços [15] [16].

A recuperação de desastres, tende a atender à infraestrutura de TI de qualquer organização, enquanto o plano de continuidade de negócios tende a atender a todos os aspectos do negócio, embora o plano de recuperação de desastres ajude a economizar

muito dinheiro e esforço do negócio, existem algumas questões práticas que precisam ser analisadas, documentadas e testadas para validação do plano [17].

2.1.2 Business Intelligence Analyst - BIA

A análise de impacto nos negócios ou em inglês Business Intelligence Analyst (BIA) é um processo cujo objetivo é analisar e priorizar as funções operacionais de uma determinada empresa com base nos impactos ao longo do tempo de paradas não programadas, com perfil disruptivo, que podem causar à organização. Este processo analisa as atividades e os efeitos que uma interrupção de negócio pode ter sobre elas, é o ponto de partida da GCN, sendo considerado um processo bastante importante dentro do ciclo de gestão. De acordo com a norma ISO 22301:2013 [11], dentro da perspectiva de GCN, o BIA em conjunto com a análise de riscos, constitui duas etapas de extrema importância para se entender a organização e suas fragilidades.

Conforme mostra a figura 2.2, o SGCN nos mostra como são as entradas das partes interessadas e os requisitos de continuidade de negócio e, por meio de ações necessárias e processos, produz resultados de continuidade que atendem aqueles requisitos.

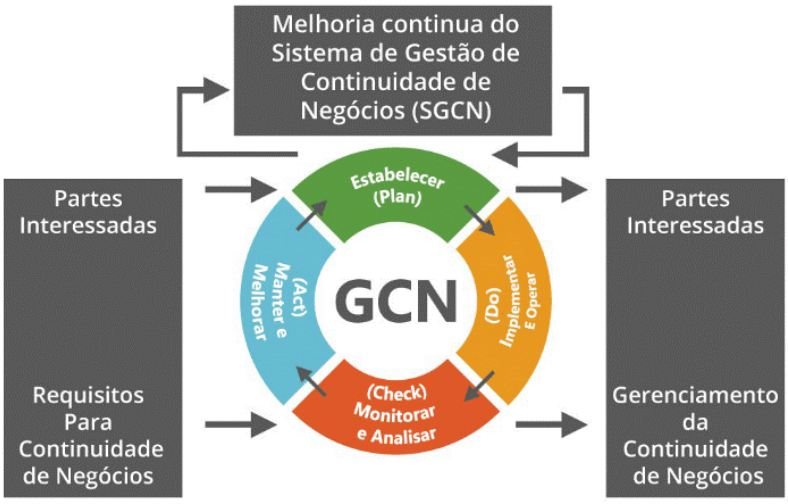

Figura 2.2: Modelo PDCA aplicado aos processos de SGCN ISO 22301:2013

O BIA tem por objetivo revelar as vulnerabilidades e subsidiar o desenvolvimento de estratégias para minimizar os riscos. O resultado da análise gera um relatório de impacto, que descreve os riscos potenciais específicos para a entidade no caso de uma interrupção do negócio, quantificando a importância dos processos do negócio e sugere alocação de recursos para defender determinados ativos críticos da organização. Sendo assim, o BIA identificará os critérios para aferir a relevância e criticidade dos processos, as atividades críticas realizadas em cada processo, a dependência de sistemas e pessoas os impactos financeiros e operacionais da indisponibilidade do serviço para a organização.

2.2 Gestão de riscos

O risco é um efeito de incerteza, um desvio em relação ao curso e objetivos esperados pelos gestores. A gestão de riscos tem o efeito de tornar um sistema mais seguro. De acordo com o Guia de Gestão de Riscos da UnB [18], gestão de riscos é "Um processo contínuo estabelecido, direcionado e monitorado pela alta administração, contemplando as atividades de identificação, avaliação e gerenciamento de potenciais eventos que possam afetar a organização ...". Ainda de acordo com o guia, em seu artigo 5º informa que, são objetivos: estabelecer o conceito, as diretrizes, as atribuições e as responsabilidades do processo de gestão de riscos, bem como orientar a identificação, a análise, o tratamento, o monitoramento e a comunicação dos riscos. Além disso, entende-se os passos e a importância de gerir riscos no contexto acadêmico, refletindo também esta importância ao ambiente de tecnologia da instituição.

Conforme Ferreira [19], a gestão de riscos é um meio para atingir um fim e não um fim em si mesmo. É um processo educativo que nos consciencializa para a existência de riscos e que aos gestores cabe a responsabilidade de os gerir.

Uma gestão de riscos adequada, dentre outros benefícios, fornece o aumento da probabilidade de alcance dos objetivos traçados, o aprimoramento do processo de identificação de oportunidades e ameaças, o fornecimento de uma base sólida e segura para a tomada de decisão e planejamento, o aprimoramento da eficácia na alocação e do uso de recursos, a melhoria da eficiência operacional e a redução das perdas e custos, a melhora da conformidade com os requisitos legais e normativos, e o aprimoramento do controle de governança corporativa [20].

De acordo com o manual de gestão de riscos do Tribunal de Contas da União (TCU) [21], a análise do risco se refere ao desenvolvimento da compreensão sobre o risco e à determinação do nível de risco. Ainda de acordo com o manual, para a realização da gestão de riscos, as seguintes etapas são recomendadas:

- Estabelecimento do contexto;
- Identificação dos riscos;
- Análise dos riscos;
- Avaliação dos riscos;
- Tratamento dos riscos;
- Comunicação e consulta com partes interessadas;
- Monitoramento;

- Melhoria contínua.

A gestão de riscos apoia em evitar eventos indesejados e considera-se uma gestão com capacidade de reduzir a probabilidade e a gravidade desses eventos. A possibilidade de antecipar sistematicamente os riscos possibilitam uma gestão proativa identificando aos riscos de forma futura, assim, sendo considerado um gerenciamento proativo ao invés de reativo. Para ser proativo com a possibilidade de antecipar os riscos é criado as condições para identificá-los, avaliá-los e evitá-los [22].

A ISO 31000:2018 [23], relacionada as diretrizes de gerenciamento de gestão de riscos, fornece princípios, diretrizes, estrutura e processos para gerenciar riscos e pode ser usada por organizações de todos os tamanhos. Conforme a norma, o propósito da identificação de riscos é encontrar, reconhecer e descrever riscos que possam ajudar ou impedir que uma organização alcance seus objetivos. Já na análise de riscos, o objetivo é compreender a natureza do risco e suas características, incluindo o nível do risco, onde apropriado. Completando com o propósito da avaliação de risco que é apoiar as decisões, contudo, não basta avaliar o risco em si, ele deve ser contextualizado em razão de já poder ter sido feita alguma atividade para, mesmo de forma não padronizada ou organizada, mitigar parte do risco.

Themsen [24] na sua revisão sistemática aborda que a ISO é a referência mais utilizada nas últimas três décadas por diferentes áreas, setores públicos e privados. Essa propõe-se a ser aplicada em qualquer ciclo de vida da organização e em uma ampla variedade de atividades, incluindo estratégias, operacionais, processos, funções, projetos, produtos, serviços, e em quaisquer tipos de riscos, que apresentem ou não consequências positivas ou negativas [25].

A ISO 31000:2018 foi utilizada para definir o processo de avaliação de riscos identificados no contexto deste estudo que visa Identificar, Analisar, Avaliar e Tratar os riscos.

De acordo com Wildavsky, "Nenhum risco é o risco mais alto de todos". Assumir riscos é uma pré-condição necessária para o desenvolvimento humano; se deixássemos de assumir riscos, as inovações necessárias para resolver muitos dos problemas do mundo diminuiriam. De fato, muitos dos riscos na sociedade moderna são resultados de benefícios derivados da inovação social e tecnológica [22].

A gestão de riscos na Universidade de Brasília foi instituída através da resolução 0004/2019 do Conselho de Administração (CAD). Esta resolução dispõe sobre governança, gestão de riscos e controles internos no âmbito da UnB. De acordo com o Guia de Gestão de Riscos UnB [18], a metodologia apresentada foi construída considerando a adequação ao contexto interno e externo da Universidade, a missão, a visão e os valores institucionais, os macroprocessos finalísticos e de apoio, além da maturidade institucional no tocante à gestão de riscos.

Conforme o artigo 2º do guia, a gestão de riscos caracteriza-se como um processo institucional contínuo e interativo, formulado para orientar e controlar eventos que possam afetar o cumprimento dos objetivos da Universidade. Destaca-se que esse processo pode ser aplicado a todas as unidades acadêmicas e administrativas da UnB, em todos os níveis institucionais.

O guia de gestão de riscos utilizado na UnB busca fornecer uma orientação integrada sobre o processo de gestão de riscos em consonância com as diretrizes da Política de Gestão de Riscos da UnB e as normas nacionais e internacionais que dispõem sobre a implementação da gestão de riscos. O processo de Gestão de risco na UnB abrange as etapas de identificação, análise, avaliação e tratamento de riscos de acordo com a figura 2.3.

Figura 2.3: Processo de gestão de riscos estabelecido na UnB
Fonte:Guia de Gestão de Riscos UnB

2.2.1 Riscos e Ameaças

Todos os processos de uma empresa envolvem riscos e ameaças. Um risco é qualificado pela probabilidade da ocorrência e pelo impacto que pode causar na organização, caso ocorra, seja explorando vulnerabilidades de um ativo ou de um conjunto de ativos, visando prejudicar a organização, podendo ou não causar um incidente. Também pode ser

compreendido como um evento ou condição incerta que pode causar um efeito positivo ou negativo nos objetivos da empresa [26].

Uma ameaça é uma potencial violação de segurança que pode gerar um evento que cause danos e prejuízos aos sistemas, sendo normalmente extremas, não estando sob controle de uma pessoa específica [27]. Ainda neste contexto, ameaças podem ser classificadas conforme abaixo:

- Ameaças naturais: normalmente vinculadas a questões de natureza, tais como: incêndios, tempestades, poluição e outros.
- Ameaças involuntárias: vinculadas ao desconhecido, exemplo: acidentes, erros, interrupções elétricas, e outros.
- Ameaças voluntárias: relacionadas às intenções humanas, tais como hackers, vírus, invasores e outros.

Portanto, de acordo com o TCU:

> "as organizações públicas precisam gerenciar riscos, identificando-os, analisando-os, em seguida, avaliando se devem ser modificados por algum tratamento, de modo a criar as condições para o alcance dos seus objetivos e, posteriormente, monitorando os riscos tratados para verificar se as medidas adotadas cumprem sua função [28]."

2.2.2 Risco Residual

A redução gerenciada de um risco é obtida por meio da introdução de controles, produzindo o risco residual. De acordo com a norma ISO 27005:2019 [6], risco residual é o risco remanescente após o tratamento do risco. Desta forma, sabe-se que o risco residual pode conter riscos não identificados.

É importante estruturar o apetite de riscos de uma organização, a fim de, levantar o quanto que uma empresa está disposta a perder para alcançar determinados objetivos, levando-se em consideração os riscos levantados. Desta forma, o gestor de riscos precisa encontrar um ponto de equilíbrio entre o ganho no aumento de confiança do risco em comparação com as perdas decorrentes de investimentos em controle e aquelas relacionadas à perda de flexibilidade organizacional [27]. Assim, é preciso compreender que cada novo controle introduzido para tratar um risco específico produz um risco residual e pode introduzir surgimento ou desaparecimento de novos riscos.

A presença de risco residual implica uma necessidade contínua de desenvolver e apoiar de forma eficaz capacidades para serviços de emergência, preparação, resposta e recuperação, juntamente com políticas econômicas, como redes de segurança e mecanismos de transferência de risco.

2.2.3 Avaliação de Riscos

O processo de avaliação de riscos permite identificar eventos que possam causar a perda dos ativos e mapear as ações a serem executadas [6]. O mapeamento destas ações é efetuado com base na probabilidade e impacto de cada risco identificado por meio de pesos previamente definidos. Desta forma, poderá se definir com maior precisão o tratamento e plano de resposta ao risco.

De acordo com o Guia de Gerenciamento de Risco da UnB [18] [23], a análise de riscos é o processo de compreensão da natureza do risco e determinação do nível de risco a partir da identificação de sua probabilidade de ocorrência e do nível de potencial impacto em caso de materialização do risco. Dessa forma, a análise de riscos compreende a seguinte relação:

Severidade = (Probabilidade(P) x Impacto(I))

Figura 2.4: Formula de severidade de risco
Fonte: Elaboração própria.

Probabilidade (P): chance de algo acontecer [23]

Impacto/Efeito (I): Desvio em relação ao esperado, podendo ser positivo, negativo ou ambos e resultar em oportunidade ou ameaças [23]

2.2.4 Tratamento e plano de resposta ao risco

Após a análise dos riscos, se faz necessário definir um plano de resposta ao risco com a definição das ações a serem realizadas. Esse direcionamento pode variar dependendo do que cada organização aceita como risco [29].

Neste contexto, a norma 27005:2019 define algumas tratativas para o plano de resposta ao risco. Nesta pesquisa de mestrado, será utilizada a denominação de Pereira e Bergamaschi [30] para os elementos do plano de resposta ao risco: mitigar (ou reduzir); aceitar (ou tolerar); transferir (ou compartilhar) ou evitar (ou eliminar) o risco.

Mitigar o risco

Ao mitigar o risco, são efetuadas ações para reduzir a probabilidade e/ou impacto do risco. Caso o risco ocorra, os impactos gerados serão menores e de mais fácil ajuste. Dessa forma, mitigar significa restringir os riscos a um nível aceitável pela organização [30].

Evitar o risco

Ao evitar o risco significa modificar o que for necessário para eliminar o objeto sujeito ao risco, eliminando a ameaça na origem [30].

Aceitar o risco

Ao aceitar o risco, a organização não atua no risco encontrado pois encontra-se um nível tolerável para a organização. Normalmente, estes riscos possuem probabilidade e impacto baixos que não justificam as ações a serem realizadas [30].

Transferir o risco

A transferência do risco ocorre quando o risco não é de responsabilidade única de uma organização ou setor ou até mesmo quando a organização não possui acesso para modificar o cenário de risco. Em alguns casos, essa decisão pode ser registrada contratualmente [30].

Definir ações

A partir da definição do tratamento e plano de resposta ao risco deverão ser mapeadas as ações a serem realizadas. Desta forma, pode-se utilizar o ciclo PDCA (Plan, Do, Check e Act) que permitirá o acompanhamento dos riscos do início ao fim, conforme apresentado na norma 27005:2019 [6].

Após a identificação dos controles internos, torna-se necessário avaliar a eficácia, eficiência e efetividade dos mesmos no tocante aos objetivos do processo. A tabela 2.2 mostra os níveis de avaliação de controles utilizados no guia de gestão de riscos da UnB.

Nível	**Descrição**
Inexistente	Não formatado: Controle inexistente ou mal implementado.
Fraco	Falta sistematização: Controles em andamento com ações caso a caso e baseado na confiança das pessoas.
Mediano	Controles parciais: Para algumas causas há controle efetivo para mitigação do risco, porém para outras não há controle.
Satisfatório	Necessidade de aprimoramento: há controles implementados com ações adequadas que mitigam os riscos, porém requer melhoria.
Forte	Sem falhas detectadas: ações mitigadoras de risco em todos os aspectos relevantes com controle consolidados.

Tabela 2.2: Avaliação de controles
Fonte: Guia de gestão de riscos da UnB

A atitude perante o risco só será eficaz se a sua classificação estiver correta, permitindo a ação preventiva perante cada risco classificado, assim, agregando valor aos ativos e sistemas da organização.

2.3 Segurança da Informação

A Segurança da Informação (SI) visa proteger a informação das ameaças, garantindo a integridade, disponibilidade e confidencialidade [31]. No contexto da SI, de acordo com a norma ISO 27005:2019:

> "a informação é um ativo que possui grande valor para a organização e será protegido pela área de segurança de qualquer ameaça ou acesso não autorizado visando garantir a continuidade do negócio e minimizar os possíveis danos com o intuito de maximizar o retorno e utilizar as oportunidades de negócio visando manter a perenidade do ambiente corporativo"[6].

De acordo com Côrte [32], a SI necessita que os três pilares estabelecidos se integrem em consonância, sendo eles: processos, tecnologia, e pessoas. Por meio dos processos que estruturam e definem as ações nas organizações, junto a tecnologia utilizada para otimizar o funcionamento destes processos, temos as pessoas que garantem que estes processos funcionem da melhor forma possível.

A partir da consonância dos pilares da SI será possível sustentar a tríade: confidencialidade, integridade e disponibilidade. A confidencialidade garante que os dados sejam acessados somente por aqueles que devem ter acesso aos mesmos. A integridade assegura que os dados estejam em sua totalidade durante todo o seu ciclo de vida, sem haver qualquer modificação. A disponibilidade garante que os dados estejam disponíveis a qualquer momento, sem interrupções.

2.3.1 Eventos e Incidentes de Segurança

Eventos negativos para a segurança da informação são mais comumente chamados de incidentes de segurança da informação. A ISO 27005:2019 relacionada a gestão de riscos em segurança da informação define eventos e incidentes. Um evento de segurança é uma ocorrência identificada de um sistema, serviço ou rede que indica uma possível violação da política de segurança da informação ou falha de controle, ou ainda uma situação previamente desconhecida que possa ser relevante para a segurança de dados da instituição [6]. Ainda de acordo com a norma, um incidente de segurança da informação, é indicado por um simples evento ou uma série de eventos de segurança da informação de forma indesejada ou inesperada, que tenha grande probabilidade de comprometer as operações do negócio e ameaçar as informações da organização. Sendo que, os incidentes de organização:

- Provocam obstrução ou erro na execução de um ou mais processos organizacionais;
- A obstrução ou erro decorre de dificuldades na ação dos agentes organizacionais humanos ou computacionais, no desempenho de suas atividades;

- Provocam queda de desempenho de uma ou mais funções organizacionais;
- Impactam o alcance de metas organizacionais.

Dado que alguns eventos de segurança são classificados como incidentes, quanto mais eventos ocorrerem, maior a chance de incidentes serem provocados. A gestão de riscos de segurança da informação busca mapear o risco de ocorrência dos incidentes de segurança da informação.

2.3.2 POSic UNB

A Política de Segurança da Informação e Comunicação (POSIC) da Universidade de Brasília, foi publicada em 24 de abril de 2019 pela câmara de planejamento e administração da UnB.

A POSIC tem por objetivo instituir princípios e diretrizes de Segurança da Informação e Comunicação no âmbito da UnB, com o propósito de limitar a exposição ao risco a níveis que garantam a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações e comunicações que suportam as atividades precípuas de ensino, pesquisa e extensão da instituição [33].

De acordo com a POSIC [33], gestão de continuidade de negócios abrange processos de gestão que identificam ameaças potenciais para uma organização e os possíveis impactos nas operações da atividade institucional caso essas ameaças se concretizem, de forma a fornecer uma estrutura para que se desenvolva resiliência organizacional capaz de recuperar perdas de ativos de informação a um nível aceitável preestabelecido, por intermédio de ações de prevenção, resposta e recuperação, de forma a salvaguardar os interesses das áreas envolvidas, a reputação, a marca da organização e suas atividades de valor agregado. Ainda de acordo com a norma, em seu artigo 30, a STI em conjunto com áreas responsáveis pelos ativos de informação da Universidade, deverão instituir normas, procedimentos e controles que estabeleçam a gestão de continuidade de negócios, a fim de minimizar os impactos decorrentes de potenciais eventos que causem a indisponibilidade sobre serviços de Tecnologia da informação e comunicação da UnB.

2.3.3 Identificação de Ameaças

De acordo com a ISO 27005:2019 [6], uma ameaça tem o potencial de comprometer ativos e, por isso, também as organizações. A norma ainda esclarece que, ameaças podem ser de origem natural ou humana e podem ser acidentais ou intencionais. Desta forma, uma ameaça pode surgir de dentro ou de fora da organização.

A tabela 2.3 de acordo com a ISO 27005:2019 descreve algumas ameaças comuns descritas na norma.

Tipo	Ameaças	Origem
Dano Físico	Fogo	A,I,N
	Água	A,I,N
	Poluição	A,I,N
	Acidente Grave	A,I,N
	Destruição de equipamento ou mídia	A,I,N
	Poeira, corrosão, congelamento	A,I,N
Eventos naturais	Fenômeno climático	N
	Fenômeno sísmico	N
	Fenômeno vulcânico	N
	Fenômeno meteorológico	N
	Inundação	N
Falhas técnicas	Falha de equipamento	A
	Defeito de equipamento	A
	Defeito de software	A
Ações não autorizadas	Uso não autorizado de equipamento	I
	Cópia ilegal de software	I
	Comprometimento dos dados	I
	Processamento ilegal de dados	I
Comprometimento de funções	Erro durante o uso	A
	Abuso de direito	A,I
	Forjamento de direitos	I
	Repúdio de ações	I
	Indisponibilidade de recursos humanos	A,I,N

Tabela 2.3: Exemplos de ameaças comuns
Fonte: Adaptada ABNT NBR ISO 27005:2019

De acordo com a norma [6], a lista da tabela 2.3 pode ser usada durante o processo de avaliação de ameaças. Assim, as ameaças podem ser de origem intencional (I), acidental (A) e natural (N).

Nesta pesquisa é analisado outras ameaças, também descritas na norma, como por exemplo, ameaças por seres humanos, muito comuns atualmente pelos ataques hacker e cracker, ataques terroristas ou crimes digitais.

2.4 Relações causa e efeito

Em vez de se dizer que um evento é causado por outro evento, diz-se que os eventos são função de outros eventos como defende Mach [34]. Para o autor "os conceitos de causa e efeito não expressam adequadamente a dependência mútua entre os elementos".

A exemplo, na situação em que os elementos são dependentes imediatamente, os conceitos de causa e efeito podem ser intercambiáveis: o elemento A pode causar B e vice-versa.

A análise de causa-efeito, de acordo com Rohleder e Silver [35], é uma aproximação comum usada na melhoria da qualidade ou melhoria de processo. O contexto na qual é usada envolve a averiguação de um efeito indesejável e a procura para sua verdadeira causa. Inicialmente, várias possíveis causas são listadas e a identificação das causas mais prováveis normalmente é o resultado de um processo subjetivo e criativo que envolve, por exemplo brainstorming.

Para o senso comum, de acordo com Almeida, Pinto e Cruzeiro [36] causa é um acontecimento que produz sempre determinado resultado: em outras palavras X é condição suficiente e necessária para que Y ocorra.

2.5 Gestão de Documentos

No Brasil, a gestão de documentos institucionalizou-se com a aprovação da Lei 8.159, de 08 de janeiro de 1991, onde é definida como "[...] o conjunto de procedimentos e operações técnicas à sua produção, tramitação, uso, avaliação e arquivamento em fase corrente e intermediária, visando à sua eliminação ou recolhimento para guarda permanente".

Para os pesquisadores Bartalo e Moreno [37], o objetivo da gestão documental é:

> "[...] objetiva e entre outros, assegurar uma documentação adequada, garantir a preservação e o acesso aos documentos, permitindo a recuperação das informações de forma ágil e eficaz, proporcionar o cuidado adequado e o armazenamento a baixo custo, reduzir ao essencial a massa documental produzida, otimizar recursos humanos, físicos e materiais."

O estudo de uma gestão documental eficiente exige considerações sobre seu potencial custo-benefício que segundo Jardim [38]:

> "é possível imaginar como o custo público da informação governamental tende à alcançar níveis reduzidos, aplicando-se o princípio básico de gestão de documentos, segundo o qual a informação deve estar disponível no lugar certo, na hora certa, para as pessoas certas e com o menor custo possível."

O conceito Gerenciamento de Documentos Eletrônicos (GED), que está relacionado aos documentos criados em meio eletrônico. Inclui os documentos que passaram pelo processo de digitalização e a possibilidade de gerenciamento dos documentos criados em meio eletrônico.

O GED, incorpora os conceitos relativos às regras de tramitação, uso e segurança contra adulteração de acessos não autorizados aos documentos criados em meio eletrônico ou não. Evoluindo de um mero software de digitalização e acesso para tornar-se

um instrumento de apoio dentro de sistema de gerenciamento de documentos (eletrônicos ou convencionais) e controles de fluxo de trabalho (workflow). De acordo com Paulo Nascimento [39], "GED é o conjunto de tecnologias utilizadas para organização da informação não estruturada de um órgão ou entidade, que pode ser dividido nas seguintes funcionalidades: captura, gerenciamento, armazenamento e distribuição."

Ainda de acordo com Paulo Nascimento [39], "Um GED se caracteriza pela automação de um processo de forma desestruturada, sem considerar as especificidades arquivísticas da classificação e avaliação dos prazos de guarda."

2.5.1 Sistema eletrônico de informação - SEI

Antigamente, muitas instituições funcionavam totalmente em um ambiente baseado no papel. O surgimento da tecnologia foi facilitando e ao mesmo tempo dificultando a adaptação para a área de tecnologia das organizações, já que necessita de recursos financeiro para investir em equipamentos de infraestrutura de TI para armazenamento de informações. Esse avanço gerou grandes volumes de informação digital, complicando o gerenciamento da informação, o seu armazenamento, a busca e consequentemente sua localização.

Neste contexto, o SEI foi introduzido na Universidade de Brasília com o intuito de revolucionar a forma de produzir e tramitar documentos no ambiente administrativo e, com isso, resolver vários problemas de localização e armazenamento de processos. Desta forma, foi estabelecido o objetivo de modernizar processos e aumentar a eficiência das rotinas produtivas da UnB.

O Sistema eletrônico de informações é um software que permite a produção, edição, assinatura e trâmite de documentos dentro do próprio sistema. Proporciona a visualização de processos e documentos e permite acesso simultâneo de várias unidades ao mesmo tempo em um mesmo processo, ainda que distante fisicamente, reduzindo o tempo de realização das atividades.

O SEI foi implantado na UnB com a promessa de solucionar todos os problemas relacionados ao acúmulo de documentos físicos, ou seja, falta de espaço nos setores de trabalho para armazenamento, extravio de documentos, perda de tempo para localizar documentos físicos, desperdício de papel e retirada não autorizada de peças de processos. Com essa promessa, o sistema traria agilidade na difusão da informação e segurança na recuperação de toda documentação produzida no SEI.

Sobre a visão de segurança de dados, o sistema implementou o controle de nível de acesso em documentos sigilosos, em atenção a Lei nº 12.527, de 2011: Lei de acesso a informação (LAI). O sistema procura seguir as diretrizes da lei, inovando no âmbito da Universidade propondo uma perspectiva diferente para o acesso às informações de caráter público, o qual passa a ser a regram enquanto o sigilo, a exceção.

2.6 ITIL

Nas últimas décadas, o setor de tecnologia vem assumindo um papel determinante para o desenvolvimento econômico, o aumento da produtividade e a difusão tecnológica nas organizações públicas. A biblioteca ITIL é um conjunto de boas práticas de serviços de TI, apesar de ser confundida muitas vezes com uma metodologia. Segundo Esteves [40] para definir melhor o que é ITIL, é interessante começar dizendo o que ele não é, não sendo uma metodologia, e sim uma estrutura flexível que pode ser adaptada às necessidades de cada organização, não sendo também um manual de instruções, sendo uma metologia a ser consultada que contém as melhores práticas na gestão de serviços de tecnologia.

A abordagem de processos da ITIL ultrapassa a estrutura hierárquica de departamentos. A estrutura baseada em processos faz o vínculo entre os departamentos e estabelece um fluxo de trabalho e comunicação entre áreas, evitando assim a criação de atividades não coordenadas. Atualmente a ITIL está em fase de implementação na STI, sendo utilizada principalmente na central de serviços e processos de gestão de projetos.

Um processo é um conjunto de atividades inter-relacionadas com objetivos definidos. Os processos da ITIL variam de acordo com sua biblioteca, ou seja, eles estão divididos por um conjunto de livros, estes livros são: Estratégia de serviço, designer de serviço, transição de serviço, operação de serviço e melhoria contínua de serviço. Conforme imagem 2.6 abaixo.

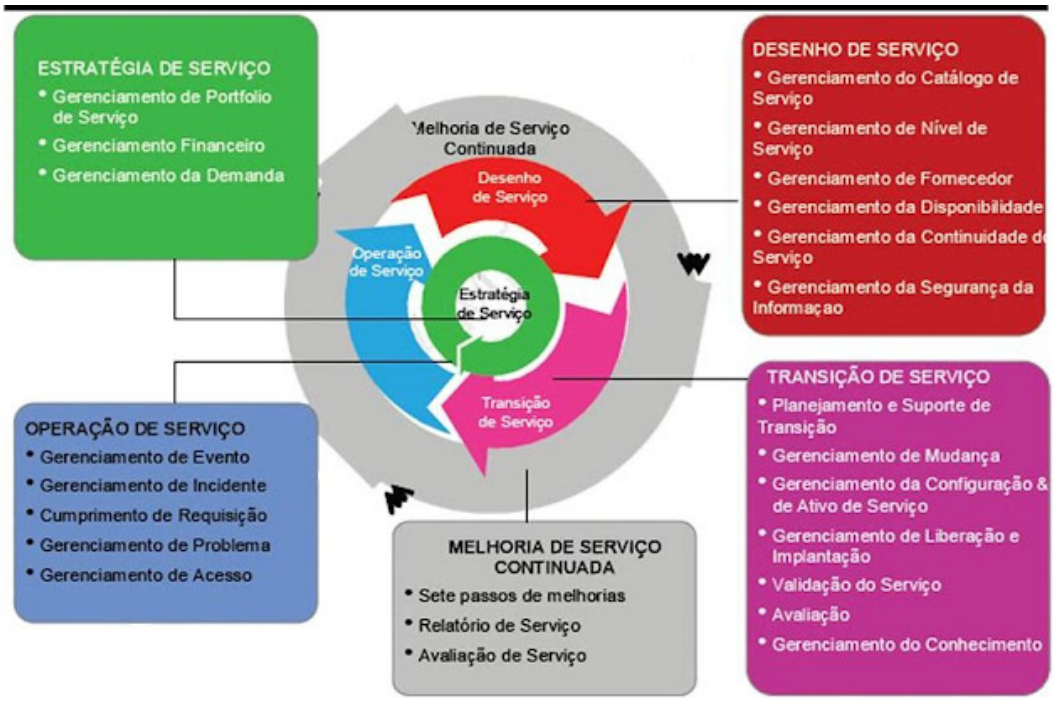

Figura 2.5: Ciclo de vida processos ITIL Versão 3

Nesta pesquisa serão abordados 2 processos do ciclo de vida da ITIL. O processo de operação de serviços especificamente o subprocesso de gerenciamento de incidentes e o processo de desenho de serviços nos processos de gerenciamento de disponibilidade e gerenciamento da continuidade de serviços.

2.6.1 Gerenciamento de incidentes

Os incidentes podem ser definidos como uma interrupção ou redução da qualidade dos serviços de TI [41]. Mesmo os problemas mais simples como por exemplo um erro inicial em uma configuração de sistema pode ser caracterizado como um incidente. Desta forma, de acordo com a cartilha de segurança da informação do CERT.BR [42], um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de rede de computadores.

O gerenciamento de incidentes, conforme descrito na ITIL [43], é o processo cujo propósito é restaurar a operação normal do serviço o mais rápido possível de modo a minimizar o impacto adverso nas operações de negócio, garantindo que os níveis acordados de qualidade do serviço sejam mantidos. Desta forma, o gerenciamento de incidentes visa contribuir para melhorar a satisfação dos usuários com a qualidade dos serviços de TI.

Ainda de acordo com a ITIL [43], o gerenciamento de incidentes é o processo responsável por gerenciar o ciclo de vida de todos os incidentes. O gerenciamento de incidentes garante que a operação normal de um serviço seja restaurada tão rapidamente quando possível e que o impacto no negócio seja minimizado [44].

A POSIC da UnB [33] deixa claro que a STI deverá criar e manter uma Equipe de Tratamento de Resposta a Incidentes (ETIR), instituída pelo comitê de TI, com a responsabilidade de coordenar as atividades relacionadas a incidentes de segurança nos serviços prestados pela secretaria, e informa que:

> "Os eventos de incidentes devem seguir o Plano de gerenciamento de incidentes específico, no qual se definirá as responsabilidades e procedimentos para assegurar respostas tempestivas, efetivas e ordenadas perante incidentes de segurança da informação e comunicação de forma a contribuir para garantir a continuidade das atividades vistas a não intervenção no alcance dos objetivos estratégicos da UnB".

Incidentes podem ser reportados à central de serviços pelos usuários, pelo próprio pessoal de TI ou, automaticamente, pelas ferramentas de monitoramento. Neste contexto, vale ressaltar que não faz parte do escopo do gerenciamento de incidentes investigar a causa raiz dos incidentes. O objetivo do Gerenciamento de Incidentes é restaurar a operação do serviço o mais rápido possível [44]. Para tanto, deverá utilizar as soluções de contorno disponíveis na base de erros conhecidos e bases de conhecimento da organização.

A central de serviços é o ponto de contato entre o provedor de serviços e os usuários. Uma central de serviços gerencia incidentes, requisições de serviços e também a comunicação com os usuários, sendo o primeiro nível no atendimento do incidente [45]. No contexto dos serviços prestados pela STI, quem é responsável pelo primeiro atendimento a requisições e incidentes é a empresa CentralIT.

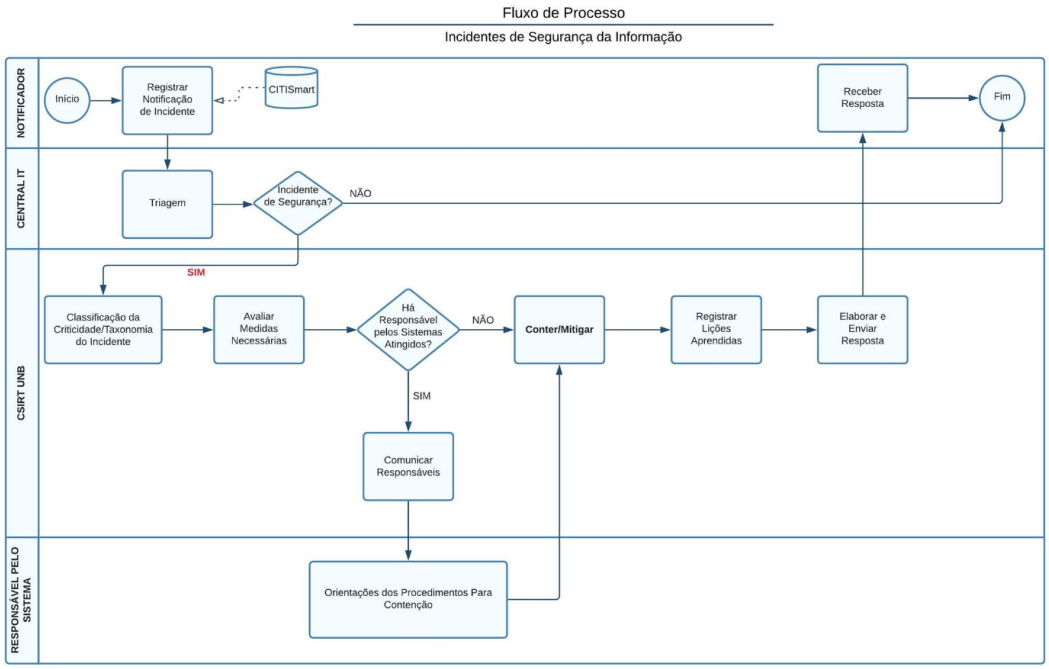

Figura 2.6: Fluxo de Processo de Incidentes de Segurança da Informação - UnB

A central de serviços que hoje é de responsabilidade da empresa prestadora de serviços CentralIT, utiliza ferramentas de auxilio na monitoração do ambiente tecnológico da UnB. Uma das ferramentas utilizadas pela central de serviços é o Zabbix que segundo Benício [46] é um software de nível empresarial projetado para disponibilidade e desempenho de componentes de uma infraestrutura de TI. Outra ferramenta utilizada por essa central identificada na figura 2.7 responsável pela triagem das requisições é o Citsmart que é um software de gestão de TI, que implementa conceitos e técnicas de governança, tendo como objetivo manter a eficiência nos processos de prestação de serviços e promover melhorias.

2.6.2 Desenho do serviço

Gerenciamento da disponibilidade

Gerenciamento de disponibilidade é o processo que visa aperfeiçoar a capacidade da infraestrutura de TI, serviços e suporte para prover, a custo efetivo, um nível de disponibilidade que permita ao negócio atender a seus objetivos [43]. Esse processo é responsável por defi-

nir, analisar, planejar, medir e melhorar todos os aspectos da disponibilidade dos serviços de TI.

Para otimizar continuamente e melhorar a disponibilidade dos serviços de TI, o Gerenciamento de Disponibilidade deve ocorrer em dois níveis inter-relacionados:

- Atividades reativas: monitoramento, medição, análise e gerenciamento de eventos, incidentes e problemas envolvendo a indisponibilidade do serviço;
- Atividades proativas: planejamento proativo, desenho, recomendação e melhoria de disponibilidade.

Gerenciamento da continuidade de serviço

A continuidade de serviços é crucial para a sobrevivência de qualquer negócio. Reduzir riscos e obter e planejar soluções recuperação são medidas eficaz para a manutenção contínua da continuidade de serviços.

O PCN define as etapas necessárias para recupera os processo de negócio logo após um desastre, identificando os fatores que causam o desastre e a forma de comunicação com as pessoas envolvidas no processo de recuperação de serviços.

2.7 Revisão do Estado da Arte

A revisão do estado da arte tem como perspectiva a descoberta do conhecimento, da análise de qualidade e apuração de desempenho. A grande quantidade de informação científica gerada tem o benefício de contribuir para a melhoria contínua de diversas áreas do conhecimento, dando suporte tanto ao processo de pesquisa e desenvolvimento quanto às propostas de solução de problemas de diferentes naturezas. Consequentemente, quando se estabelece um trabalho de pesquisa, é fundamental garantir a relevância do tema estudado, bem como considerar os trabalhos mais relevantes já desenvolvidos, para evitar aplicar esforços que não apresentem contribuição para a ciência.

Com a geração de grande volume de dados, necessita-se de utilização de um método que auxilie o pesquisador na estruturação e análise dos trabalhos científicos. Para satisfazer esta finalidade, a revisão do estado da arte foi realizada utilizando a TEMAC [47], que possui método estruturado considerando os esforços de sua aplicação frente aos benefícios alcançados com o processo.

2.7.1 Método da Teoria do Enfoque Meta Analítico Consolidado

Conforme Mariano e Rocha [47], a aplicação da TEMAC atende aos princípios do enfoque Meta Analítico, que utiliza os critérios de impacto de revistas, citações e autores e artigos

e frequência de palavras-chaves, mas com o benefício de integrar ao processo ferramentas tecnológicas de acesso gratuito que facilitam as análises e reduzem o trabalho manual.

O TEMAC conta com três etapas principais:

1. Preparação da pesquisa: consiste na definição de palavras-chave relacionadas ao tema de pesquisa, a definição do período de análise, as bases de dados utilizadas e as áreas de conhecimento que serão consideradas.
2. Apresentação e inter-relação dos dados: consiste em relacionar inúmeras fontes de informações, a critério do pesquisador, com a evolução do tema ano a ano, os autores mais citados, periódicos que mais publicam, entre outros.
3. Detalhamento, modelo integrador e validação por evidências: nesta etapa são identificados os principais autores, abordagens e linhas de pesquisa referentes ao tema, utilizando técnicas de co-citação e acoplamento.

2.7.2 Preparação da Pesquisa

A preparação da pesquisa consiste em estabelecer os parâmetros da busca. Foi utilizada a base de dados Web Of Science (WoS), por representar uma base sólida e internacional da ciência com a finalidade de integrar não apenas os melhores resultados, como também os mais valiosos.

Base de dados

O WoS é uma plataforma referencial de citações científicas projetada para apoiar pesquisas científicas e acadêmicas. A plataforma inclui mais de 20.000 revistas acadêmicas de alta qualidade revisadas por pares e publicadas em todo o mundo, e mais de 190.000 processos de conferências [48].

A base de artigos acadêmicos WoS foi utilizada como referência para este estudo, em razão de sua reconhecida qualidade na plataforma. Possui disponibilidade de artigos a partir de 1945, o que garante maior cobertura do tema pesquisado. A limitação do tempo de pesquisa foi necessário para atender as documentações e técnicas mais atuais, limitando-se aos últimos de 10 anos.

Termos de pesquisa

Os seguintes termos em inglês e português foram selecionados para esta pesquisa: "Business Continuity plan/ Plano de continuidade de negócios", "Disaster Recovery Plan/ Plano de recuperação de desastres", "Operacion Risks/ Risco Operacional"e "Risk Management/ Gerenciamento de riscos". A estratégia de pesquisa aplicada foi TITLE-ABS-KEY (("Risk

management"OR risk) AND ("Business Continuity Plan"OR "Disaster Recovery Plan"OR "Operacion Risks")).

As palavras-chave serão apresentadas tal qual foram utilizadas nas buscas, considerando facilitadores de pesquisa, como a utilização de aspas duplas para termos compostos, conectores and e or, e o uso do asterisco para indicar que daquele ponto em diante a palavra pode apresentar qualquer letra e em qualquer quantidade, evitando a perda de variações da palavra causadas por prefixos ou sufixos.

Com o objetivo de identificar as principais referências compatíveis com o objetivo dessa pesquisa, foram selecionadas as combinações com todos os termos. Para buscar resultados que atendam a pesquisa, foram correlacionados os termos, onde se obteve os seguintes resultados, conforme tabela 2.4:

Termos	**Quantidade de registros**
"Business Continuity Plan"	2.122
"Risk Management"and "Business Continuity Plan"	332
"Business Continuity Plan"and "Disaster Recovery Plan"	338
"Risk Management"and "Disaster Recovery Plan"	383
"Business strategy"and "Contingency Planning"	263

Tabela 2.4: Termos das pesquisas na base de dados
Fonte: Base de Dados - Web of Science

Dos resultados encontrados e eliminadas as duplicidades foram acrescentados a uma lista marcada na plataforma WoS que permite salvar os dados da pesquisa em listas e extrair informações detalhadas posteriormente.

Consolidação e tratamento de dados para análise

De posse da base de dados com os resultados das buscas individuais consolidadas, foi realizado os refinamentos, conforme detalhamento abaixo:

Categoria Web Of Science: O WoS realiza classificação dos documentos em categorias relacionadas às áreas de pesquisa. Ao analisar os dados obtidos, foram identificados resultados das áreas de Finanças Empresariais, Saúde, Economia, Pesquisa Operacional, Gerenciamento, Engenharia Elétrica, Engenharia industrial, Negócios, Combustíveis, Ciência da computação, Estatística, Engenharia química, Geologia, Engenharia civil, Inteligencia artificial e outros.

Muitas publicações referentes a continuidade de negócios não são ligadas a ciência da computação, conforme mostra a figura 2.7. Nesta pesquisa, foram selecionados os artigos relacionados a ciência da computação, negócios e gerenciamento.

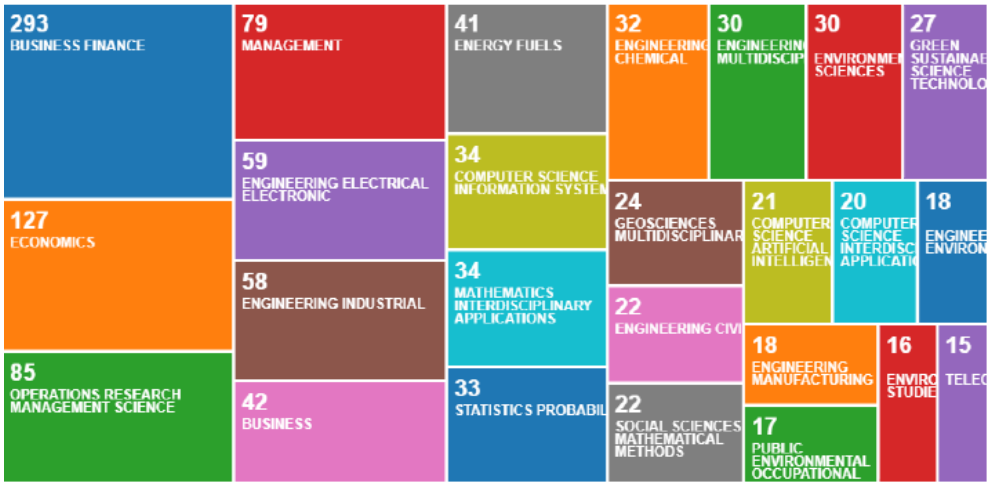

Figura 2.7: Publicações relacionadas ao tema de pesquisa
Fonte: WoS

Palavras-Chave: Utilizando os dados obtidos na base WoS, adotou-se referências ligadas a "Plano de Continuidade de negócios"ou "Plano de recuperação de desastres"e "Gestão de Riscos".

A busca por palavras-chave é importante pela variação de publicações e áreas de pesquisas encontradas. Os termos de pesquisa Gerenciamento, Custo, Modelo, Método, Continuidade, organização e desastres estão entre as palavras mais encontradas nos artigos de pesquisa. A figura 2.8 mostra o mapa de calor com os termos ou palavras mais encontradas no contexto da pesquisa.

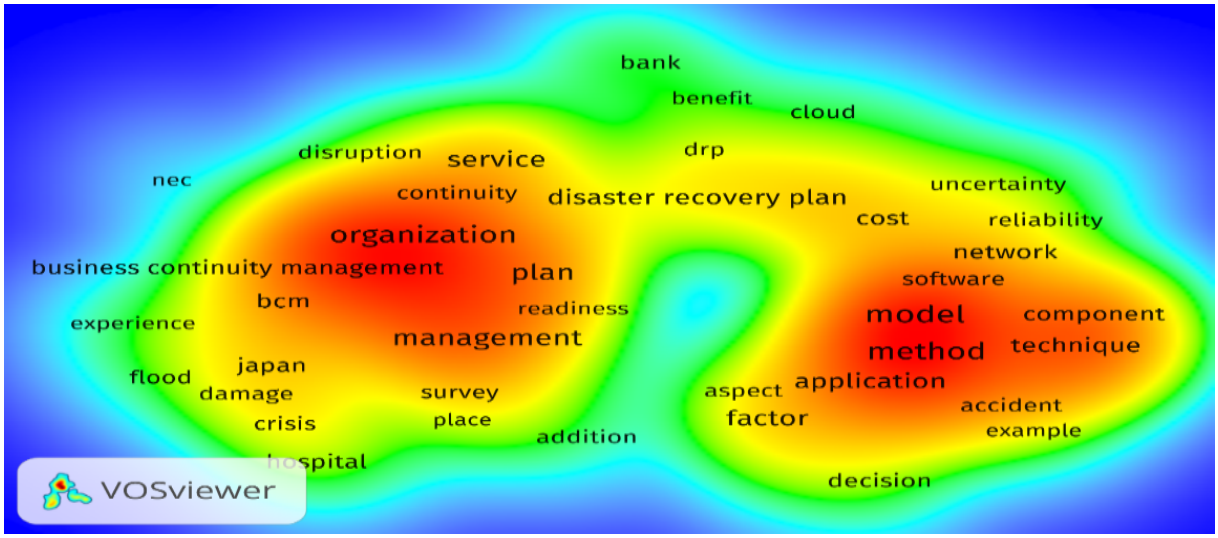

Figura 2.8: Mapa de Calor palavras chave de pesquisa
Fonte: Base de dados - WoS

Os países que mais publicaram sobre o tema nos últimos 10 anos foram, Estados Unidos, seguidos de Japão e China. Os países se destacam em publicações relacionadas

a continuidade de negócios nos últimos dois anos, principalmente em se tratando de empresas ou estados afetados pela pandemia de covid-19 com publicações referentes a área de saúde e segurança e os riscos e soluções para continuidade de atividades durantes este período. Visualizamos o Brasil com 2 publicações relacionadas ao tema no ano de 2015 e 3 artigos relacionados a área de saúde no ano de 2016.

Um dos trabalhos mais citados é o de Jhon, Lindstrom nominado Business Continuity Planning Methodology [49], sendo citado por 16 vezes. Alguns outros artigos foram utilizados para o desenvolvimento desta pesquisa, a exemplo o artigo do ano de 2019 de Miller e Engemann, Business Continuity Management in Data Center Environments [50], este apontando vários pontos semelhantes aos objetivos dessa pesquisa.

Nesta pesquisa, optou-se pela delimitação na busca pela base para os últimos 10 anos (de 2011 a 2021) e área de relevância para ciência da computação. Do total de artigos encontrados com as delimitações de período e área, foram selecionados 78 artigos para auxiliar na produção desta pesquisa. Desta forma, obteve-se a tabela 2.5 com informações referentes a alguns artigos, livros ou trabalhos utilizados nesta pesquisa.

Título	**Autor(s)**	**Ano**
Adaptive Planning for Disaster Recovery and Resiliency: An Evaluation of 87 Local Recovery Plans in Eight States	Philip Berker, John Cooper, Meghan Aminto, Shannon Grabich and Jennifer Horney	2015
Business Continuity Management in Data Center Environments	Holmes E. Miller and Kurt J. Engemann	2019
Business Continuity Plan Using ISO 22301:2012 in it solution company	Ganjar Pramudya W and Ahmad Nurul Fajar	2019
Cobit 5 Domain Delivery, Service and Support mapping for BCP	GAmirul Iqbal, Widyawan and I Wayan Mistika	2016
Contributing factor to business continuity management (bcm) failure – a case of malaysia public sector	Nurul Aisyah Sim Abdullah, Nor Laila Md Noor and Emma Nuraihan Mior Ibrahim	2015
Developing a novel quantitative framework for business continuity planning	Hojat Rezaei Soufi, S. Ali Torabi and Navid Sahebjamnia	2018
Risk Analysis on the development of a Business Continuity Plan	Alexander Setiawan, Adi Wibowo and Andrew Hartanto Susilo	2014

Tabela 2.5: Artigos usados na pesquisa

Dentre os artigos pesquisados, os termos mais encontrados são: incidente, resiliência, impacto, eventos, comunicação, contingência ou recuperação, backup, desastre, indisponibilidade.

2.7.3 Detalhamento, modelo integrador e validação por evidências

A terceira etapa do método TEMAC consiste em analisar as principais contribuições e abordagens presentes na base consolidada, por meio de co-citation e coupling.

De acordo com Melo e Rocha [47], na co-citação, tem-se uma perspectiva das abordagens mais utilizadas por meio da análise de trabalhos que têm literaturas base semelhantes [47]. Por meio do acoplamento, é possível inferir as principais fontes de pesquisa, isto é, os trabalhos que não podem faltar na revisão sistemática. Por oportuno e visando o enriquecimento deste estudo, foi incluso as pesquisas atuais que abordam ou aplicam os temas, técnicas e modelos.

O trabalho de Miller [50], possui uma abordagem de conteúdo para continuidade de negócios em ambientes de data center. Neste artigo o autor menciona que a demanda de disponibilidade em ambientes de data center afeta as expectativas durante a manutenção desses ambientes em momentos de desastes impactantes. A continuidade dos serviços pode ser afetada por ataques hackers que roubam informações ou derrubam serviços com ataques de negação de serviços. Data centers também podem ser afetados por eventos físicos como tornados, furacões e tempestades de inverno, incêndios, terremotos ou quedas de energia. Para o autor, o foco principal do planejamento de continuação de serviços é garantir que a TI seja resiliente. Define um sistema resiliente com capacidade de recuperação quando confrontado com eventos extremos de desastre.

No artigo de Omar [51], que propõe avaliação de alternativas de recuperação de desastres, localmente ou em ambientes de nuvem computacional. O autor informa que, a continuidade de negócios é um requisito vital para muitas empresas, pois uma interrupção repentina do serviço pode impactar diretamente os objetivos do negócio, causando perdas significativas em termos financeiros, de participação de mercado ou de reputação. O autor afirma que, uma organização deve ter um plano de recuperação de desastres que seja aplicável, escalonável e sustentável. Desta forma, o plano deve se atentar as restrições de custo enquanto atinge os objetivos de recuperação e ainda, que as pessoas envolvidas devem identificar eventos prováveis que podem causar desastres e avaliar seu impacto.

O trabalho de Alexander [52], que trás uma análise de risco no desenvolvimento de um plano de continuidade de negócios. O autor diz que à análise de risco pode ajudar as empresas a reconhecerem e evitarem que riscos levantados possam acontecer e evitar

que seja necessário a execução de um plano de continuidade de negócios, de modo que a empresa pode tomar medidas para prevenir ou lidar com os riscos com antecedência.

As diferentes abordagens são um reflexo das áreas de conhecimentos envolvidas, organizações ou profissionais, bem como países. Apesar do número de conceitos é possível verificar que todos partem dos princípios e conceitos de probabilidades, valores esperados, consequências e efeitos indesejáveis ou incertezas nos objetivos ou no valor humano [53]. As definições identificadas apontam pontos fortes e fracos de acordo com as suas disciplinas envolvidas.

Existem outras definições que não foram contempladas, no qual não se pretendeu esgotar esses conceitos, mas demonstrar que a depender da área de interesse existem formas para expressar os riscos envolvidos nos processos ou projetos pelas instituições ou órgãos.

Capítulo 3

METODOLOGIA

Nesta parte são apresentados os procedimentos para alcançar os objetivos propostos, descrevendo a estrutura da pesquisa e as características da metodologia aplicada na busca dos resultados.

3.1 Tipo da pesquisa

De acordo com Lakatos e Marconi [54], método é o conjunto das atividades sistemáticas e racionais que, com maior segurança e economia, permitem alcançar o objetivo e traçar o caminho a ser seguido, além de permitir detectar e auxiliar as decisões do pesquisador.

Pedro Demo, em seu livro Metodologia Científica em Ciências Sociais [55] define que "A pesquisa é entendida tanto como procedimento de fabricação do conhecimento quanto como procedimento de aprendizagem (princípio científico e educativo), sendo parte integrante de todo processo reconstrutivo de conhecimento".

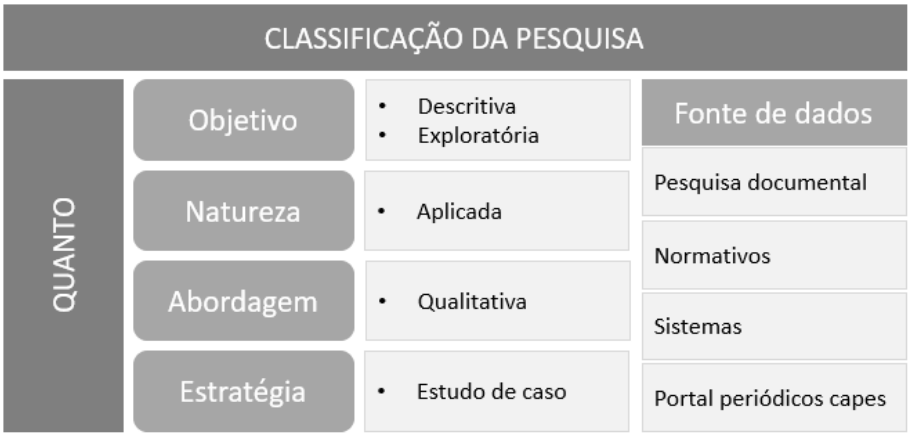

Figura 3.1: Classificação da Pesquisa
Fonte: Adaptado [56]

Vergana [57], entende que a pesquisa exploratória tem a característica de sondagem, sendo realizada em uma área a qual há pouco conhecimento acumulado ou sistematizado. A pesquisa descritiva pode ser utilizada complementarmente à exploratória, visto que esta tem como objetivo descrever as características de determinada população ou fenômeno ou o estabelecimento de relações entre variáveis [58]. Nesta pesquisa, a característica de exploração deu-se pela necessidade de identificar os eventos de indisponibilidade do sistema, ampliar o conhecimento e adequar o pensamento a respeito de tratamento de eventos de indisponibilidade do sistema.

A pesquisa pura tem por objetivo o progresso da ciência e o desenvolvimento dos conhecimentos científicos sem a preocupação direta com suas aplicações e consequências práticas, diferente da pesquisa aplicada, pois esta, apesar de apresentar características de uma pesquisa pura, tem como característica fundamental a sua aplicabilidade [59].

A finalidade da pesquisa, de acordo com Neide e Aidil é "resolver problemas e solucionar dúvidas, mediante a utilização de procedimentos científicos"[60]. Os autores caracterizam que, a partir da formulação de perguntas definidas por meio de pontos ou fatos que permanecem sem respostas e que necessitam de explicações plausíveis, que a pesquisa pode trazer respostas que venham elucidar questionamentos e respostas ao problema em questão. Desta forma, esta pesquisa tem como finalidade ser uma pesquisa aplicada.

A pesquisa apresentada pode ser identificada como qualitativa, pois examina evidências baseadas em dados coletados de ferramentas de monitoramento, documentações técnicas e dados verbais, afim de entender o ambiente com maior profundidade e de forma detalhada. Dentre as técnicas utilizadas para coleta de dados estão as entrevistas em grupo, leitura de documentações técnicas, dados de sistemas de monitoramento e histórico de indisponibilidade do sistema na instituição. Como o objetivo desta pesquisa é avaliar a gestão de riscos e a continuidade de negócios de um sistema crítico específico, esta pesquisa utiliza como cenário para estudo de caso a Secretaria de Tecnologia da Informação da UnB e o ambiente tecnológico que suporta o sistema eletrônico de informações da instituição. Assim, percebe-se que, em alguns momentos é utilizada uma abordagem quantitativa, principalmente na análise dos dados do sistema de monitoramento, porém se fez necessário essa abordagem para poder qualificar a disponibilidade do sistema em relação aos acordos de serviço esperados pela instituição.

Para compreender a capacidade de resposta aos eventos, avaliando se os modelos de gestão de risco e continuidade de negócios são validados e testados, optou-se por um estudo de caso. De acordo com Yin e Eisenhardt [61] [62], "O estudo de caso é um método de pesquisa que utiliza, geralmente, dados qualitativos, coletados a partir de eventos reais, com o objetivo de explicar, explorar ou descrever fenômenos atuais inseridos em seu próprio contexto. Caracteriza-se por ser um estudo detalhado e exaustivo de poucos, ou

mesmo de um único objetivo, fornecendo conhecimentos profundos".

Yin em seu livro sobe planejamento e métodos de pesquisa informa que, "estudo de caso é a estratégia escolhida ao se examinarem acontecimentos contemporâneos, mas quando não se podem manipular comportamentos relevantes"[63]. A figura 3.2 apresenta um esquema de categorização dos tipos de questões conhecidas.

Estratégia	Forma da questão de pesquisa	Exige controle sobre eventos comportamentais?	Focaliza acontecimentos contemporâneos?
Experimento	Como, por que	Sim	Sim
Levantamento	Quem, o que, onde, quantos, quanto	Não	Sim
Análise de arquivos	Quem, o que, onde, quantos, quanto	Não	Sim/não
Pesquisa histórica	Como, por que	Não	Não
Estudo de caso	Como, por que	Não	Sim

Figura 3.2: Situações para diferentes estratégias de pesquisa
Fonte: Estudo de caso: Planejamento e Métodos [63]

Questões do tipo "como"e "por que"são mais exploratórias, e é provável que levem ao uso de estudo de casos, pequisas históricas e experimentos como estratégias de pesquisa escolhidas [63]. Ainda de acordo com Yin, "um estudo de caso é uma investigação empírica que investiga um fenômeno contemporâneo dentro de seu contexto da vida real, especialmente quando os limites entre o fenômeno e o contexto não estão claramente definidos".

3.2 Fonte de dados

Os tipos de dados coletados foram primários (relatos dos profissionais) e secundários (base de dados, documentos técnicos, normas, estudos científicos, entre outros). Os dados primários foram coletados por meio de reuniões, com o consentimento dos participantes, apenas com identificação dos fatos, percepções e experiências que apoiassem o processo de disponibilidade do sistema SEI.

As principais fontes utilizadas para o desenvolvimento do estudo foram distribuídas conforme o tipo de dados. Uma vez que o estudo utiliza dados primários e secundários, as fontes variam e possuem particularidades quanto forma de consulta, trabalho e armazenamento dos mesmos.

As fontes de dados dividiram-se conforme o tipo de dados coletados. As divisões foram:

- Sistemas de monitoramento - consulta registros de indisponibilidade e eventos críticos ou alertas ocorridos no sistema em pesquisa delimitando-se 2 anos de referência,

assim como, todos os eventos de hardware, software, rede e janelas de manutenção do sistema.

- Reuniões - realizadas para entendimento do cenário de sustentação ao sistema SEI, com participação de pessoas que trabalham diretamente com o suporte a plataforma. O roteiro de reuniões está localizado no Apêndice D.
- Normas - consulta a normativos técnicos relacionados a padronizações e normativos internos a STI. A identificação de normas e manuais utilizados nesta pesquisa encontra-se descrita no Apêndice A.
- Documentos técnicos - consulta as áreas envolvidas para levantamento de relatórios, guias, orientações, bem como mapeamento de processos.
- Estudos científicos - bases científicas no Portal Periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) Web Of Science, para a consulta de artigos, trabalhos de conclusão final (monografias, dissertações, teses), trabalhos apresentados, livros se disponíveis.

3.2.1 Coleta de dados

As técnicas utilizadas para coletar os dados foram a análise documental, informações de sistemas de monitoramento e entrevistas com equipe técnica. Pesquisas documentais foram utilizadas para levantar o conjunto de documentos relevantes ao processo e em seguida analisar e selecionar informações importantes para a compreensão dos procedimentos executados, assim como das ferramentas e técnicas utilizadas. Entre os documentos coletados e analisados estão:

- Plano Diretor de Tecnologia da Informação e Comunicação 2019-2022 PDTI;
- Política de Segurança da Informação e Comunicação da Universidade de Brasília POSIC;
- Guia de Gestão de Riscos UnB;
- Relatórios Mensais de monitoramento de sistemas críticos;
- Documentações técnicas.

Também foram criados grupos de discussão com o intuito de entender o ambiente tecnológico que suporta o sistema SEI, assim como pesquisas documentais sobre o tema em ambientes do governo federal, normativos técnicos e referenciais teóricos.

As reuniões com o grupo focal foram conduzidas pelo pesquisador e contaram com a participação de colaboradores responsáveis pela manutenção e administração do sistema SEI. Esses colaboradores tiveram papel fundamental na realização de levantamentos, discussões e validações das informações obtidas e resultados observados. O roteiro de questionamentos realizados na reunião esta localizado no Apêndice C. Foram realizadas 2 reuniões nos dias 07 e 14 de dezembro de 2021. Os entrevistados que participaram das reuniões, assim como sua função e quantitativo foram:

- Administrador de Infraestrutura (2): pessoa responsável pela administração da infraestrutura de tecnologia responsável por suportar a disponibilidade do sistema. Acompanha, Ajusta e Administra a infraestrutura de TI do sistema.
- Administrador de sistema (2): pessoa responsável pelos ajustes na programação do sistema solicitados e autorizados pelo grupo gestor do SEI na UnB;
- Coordenador de Infraestrutura (1): Pessoa responsável pela coordenação de atividades relacionadas a área de sustentação e infraestrutura de sistemas alocados no data center localizado na STI;
- O pesquisador (1): atuou como moderador nos grupos de discussão. Ele possui sólido conhecimento sobre o contexto da pesquisa.

Os dados de eventos críticos relacionados a infraestrutura do sistema SEI foram extraídos de sistemas de monitoramento utilizados na Secretaria de Tecnologia da Informação da Universidade de Brasília. O histórico dos dados encontrados são de 2 anos (2020 e 2021). Para consolidação dos dados extraídos de banco de dados SQL Standard Query Language (SQL), com ajustes, foram utilizadas ferramentas de auxilio para analise de informações a exemplo do Microsoft Excel para elaboração de gráficos, soma de dados e separações. Os chamados abertos no sistema Citsmart a respeito de indisponibilidades e problemas na utilização do sistema SEI, foram recebidos através da extração de dados de banco de dados da ferramenta analisados e contabilizados de acordo com o contexto desta pesquisa. A extração de dados foi realizada nas base de dados dos sistemas de monitoramento e abertura de chamados, para subsidiar a importância das informações para o plano de contingência e avaliação do planejamento. Esses sistemas dispõe de um conjunto amplo de informações a respeito dos sistemas críticos da UnB. Foram utilizados os dados de todos os eventos de indisponibilidade e falhas catalogados no período de janeiro de 2020 a novembro de 2021, totalizando 1.458 registros.

As documentações técnicas referente a implantação, infraestrutura e suporte do sistema SEI, foram coletadas na base de conhecimento administrada pela STI. Para busca de documentações referentes ao contexto desta pesquisa no governo federal, foram utilizados

as páginas web oficiais dos órgãos, documentos compartilhados entre equipes técnicas de TI do governo federal.

3.3 Variáveis

Como afirmado por Vergara [57], a pesquisa descritiva expõe características de determinada população ou de determinado fenômeno e pode estabelecer correlações entre variáveis e definir sua natureza, sem contudo, referir-se às relações causais entre as variáveis.

Castro [64] considera que a pesquisa descritiva apenas captura e mostra cenário de uma situação expressa em números e que a natureza da relação entre variáveis é feita na pesquisa explicativa.

> "Quando se diz que uma pesquisa é descritiva, se está querendo dizer que se limita a uma descrição pura e simples de cada uma das variáveis, isoladamente, sem que sua associação ou interação com as demais sejam examinadas"[64].

As variáveis, sua descrição e seus principais indicadores levantados no ambiente da STI foram organizados no quadro abaixo.

Variáveis/Definição	**Operacionalização das variáveis**	**Indicadores**
Fatores de risco ativos: riscos a que estão sujeitos os ativos da instituição	Identificar os fatores de risco dos ativos da instituição	Fatores de Risco dos Ativos
Tratamento de fatores de risco de ativos: forma de tratamento dos fatores de risco dos ativos	Identificar as formas de tratamento dos fatores de risco dos ativos da instituição	Tratamento dos fatores de risco dos ativos
Impactos de fatores de risco: impactos dos fatores de risco sobre os ativos da instituição	Identificar os impactos produzidos pelos fatores de risco sobre os ativos da instituição	Fatores de risco dos ativos
Fatores de risco ativos de tecnologia: riscos a que estão sujeitos os ativos	Identificar os fatores de risco dos ativos da instituição	Impactos dos fatores de risco dos ativos

Evolução histórica e problemas em relação a tecnologia da instituição	Identificar o comportamento histórico em relação a evolução tecnológica da instituição e problemas relacionados a prestação de serviços à comunidade	Impactos dos fatores de risco dos ativos
Objetivos da instituição quanto aos ativos	Identificar os objetivos relacionados aos ativos	Objetivos dos ativos
Eventos de risco de ativos: eventos de risco a que estão sujeitos os ativos da instituição	Identificar os eventos potenciais causadores de risco para os ativos da instituição	Eventos potenciais causadores de risco dos ativos

Tabela 3.1: Variáveis de estudo

3.4 Ferramentas de Análise

Após concluída a análise documental, executada as reuniões e coletado os dados dos sistemas de monitoramento. Foi utilizada a ferramenta VOSView para análise de dados obtidos da plataforma WoS, gerando mapas de calor de palavras mais encontradas. A modelagem do processo de gestão de incidentes da STI foi realizada por meio da ferramenta Bizagi Modeler. O sistema de monitoramento Zabbix foi utilizado para se extrair informações referentes a eventos críticos de infraestrutura do sistema SEI. Dados relacionados a comunicações de incidentes por parte dos usuários foram obtidos do sistema de abertura de chamados Citsmart. O sistema Zabbix e Citsmart possuem banco de dados Standard Query Language (SQL) onde são armazenadas as informações. Foi utilizado a matriz de probabilidade e impacto durante o processo de análise de risco para compreender as dimensões dos riscos levantados e se estão sendo controlados ou não. Também foi utilizado a ferramenta Microsoft Excel para análise, tratamento e elaboração de gráficos, utilizando-se dos dados coletados da ferramenta de monitoramento.

3.5 Tipos, Fontes, Critério, Técnicas de Coleta, Análise, Apresentação dos Dados

O tópico detalha os dados coletados, os critérios de elegibilidade, as fontes e as técnicas utilizadas, bem como as análises realizadas e forma estabelecida para apresentação dos resultados. Desta forma, elaborou-se um resumo da organização da classificação da pesquisa, coleta de dados, fontes de dados, técnicas, ferramentas, análise dos dados e forma para apresentação dos resultados.

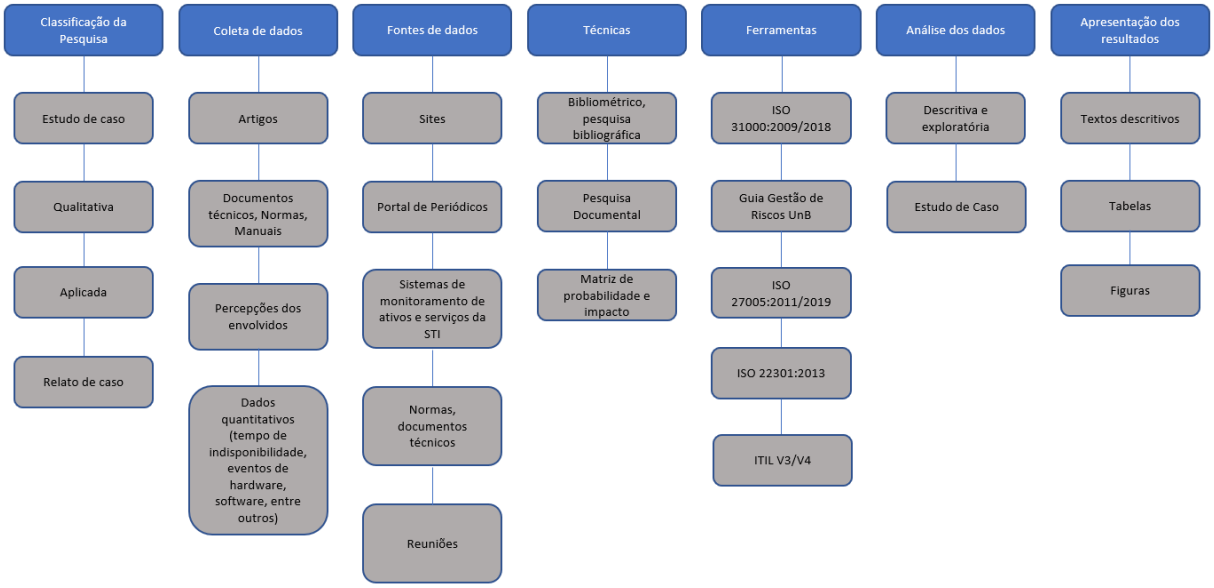

Figura 3.3: Coleta, análise e apresentação dos dados
Fonte: Elaboração própria.

Capítulo 4

ANÁLISE DOS DADOS

Nessa sessão, atendendo aos objetivos específicos 2, 3, 4 e 5, foram coletadas informações sobre o ambiente de tecnologia envolvido na sustentação do sistema SEI, assim como, identificado os ativos primários e de suporte ao sistema suas vulnerabilidades e ameças. Foi realizada a análise de riscos em termos de probabilidade e impacto e discutida a importância e aplicabilidade de um SGCN aplicado ao sistema SEI da instituição.

4.1 A instituição de ensino superior

A Universidade de Brasília foi inaugurada em 21 de abril de 1962. Foi denominada pelo Poder Executivo como Fundação Universidade de Brasília (FUB), sendo uma entidade autônoma, tendo como objetivo criar e manter a Universidade de Brasília, que é uma instituição de ensino superior de pesquisa e estudo em todos os ramos do saber e de divulgação científica, técnica e cultural, conforme lei nº 3.3998 de 15 de Dezembro de 1961 [65].

4.1.1 Secretaria de Tecnologia da Informação - STI

A STI, foi criada em 1991, para suceder o então Centro de Processamento de Dados - CPD, sendo que apenas em 2020 após resolução do Conselho Universitário passou a denominada Secretaria, sendo órgão complementar, com o intuito de desenvolver atividades de caráter permanente de apoio, necessárias ao desenvolvimento do ensino, da pesquisa e da extensão no que se refere a desenvolvimento de sistemas e soluções de tecnologia.

De acordo com o site da Secretaria [66], entre as décadas de 70 e 90 foram desenvolvidos e implementados a maior parte de todos os sistemas corporativos que são necessários aos mais diversos setores da Universidade. Ainda de acordo com o site, o até então denominado CPD desenvolveu o primeiro sistema de informatização para a Biblioteca

Central (BCE) da UnB, que foi a primeira biblioteca universitária informatizada do país, tendo um sistema que pesquisa e atualiza o banco de dados do sistema em tempo real.

Em outubro de 2012 com investimento de cerca de R$ 3,5 milhões de reais, a Universidade de Brasília inaugura o seu data center, planejado e construído em modelo de sala-cofre. Atualmente a sala cofre armazena dados cadastrais, científicos, administrativos e organizacionais de aproximadamente 50.000 discentes de graduação e pós-graduação e cerca de 10.000 prestadores de serviços, servidores públicos técnicos administrativos, estagiários e professores, conforme anuário estatístico da Universidade de Brasília [67].

Missão viabilizar soluções de tecnologia da informação que promovam a disponibilidade, integridade, confiabilidade e autenticidade das informações dos ativos relacionados aos sistemas informativos da Universidade de Brasília.

Visão ser referência nacional, como centro de informática para as Universidades Federais brasileiras e para o Ministério da Educação, reconhecido como um centro sólido pela excelência dos produtos e serviços tecnológicos oferecidos.

Valores

- Transparência no tratamento da informação;
- Busca permanente de atualização em novas tecnologias de informação e comunicação;
- Integridade, confiabilidade e confidencialidade da informação;
- Qualidade na prestação de serviços de TIC;
- Segurança da informação;
- Responsabilidade social;
- Prestação de contas de resultados alcançados;
- Engajamento na participação de seus colaboradores.

4.2 Estabelecimento do contexto organizacional

Como descrito na ISO 31000:2018 [23], ao estabelecer o contexto, a organização articula seus objetivos, define os parâmetros externos e internos a serem levados em consideração ao gerenciar riscos e estabelecer o escopo e os critérios de riscos para o restante do processo.

A Universidade de Brasília possui estatuto e regimento interno geral [68] que orienta a conduta, direitos e deveres, assim como, comportamento do corpo docente, servidores administrativos, prestadores de serviços (Terceirizados ou estagiários) e alunos de graduação e pós-graduação.

4.2.1 Contexto Externo

O contexto externo é o ambiente o qual a organização busca atingir seus objetivos, e é importante entende-lo para assegurar que os objetivos e as preocupações das partes interessadas externas sejam consideradas no desenvolvimento dos critérios de risco [69].

De acordo com a ISO 31000:2018 [23], o contexto externo não está limitado a própria norma, mas pode incluir ambientes culturais, sociais, políticos e outros ambientes, pode incluir também fatores chave que impactam a organização e a relação entre as partes interessadas do processo.

A Universidade de Brasília é órgão subordinado ao Ministério da Educação (MEC). Nos últimos anos, com o advento das crises financeiras que afetaram todos os órgãos do governo federal, teve cortes no repasse a instituição de ensino que afetaram de maneira direta a adequação e modernização do ambiente computacional da instituição. Porém, não limitando a evolução tecnológica da Secretaria de Tecnologia da UnB, que vem atualizando o parque tecnológico da instituição de ensino e proporcionando cada vez mais capacidade computacional de auxilio a pesquisa e ensino na UnB graças aos esforços de investimentos e credibilidade recebida pela área de TI da instituição.

4.2.2 Contexto Interno

A STI é órgão complementar da Universidade de Brasília com responsabilidades pelas atividades de apoio necessárias ao desenvolvimento de ensino, pesquisa e extensão no que se refere a serviços de TI, sendo subordinado ao Decanato de Planejamento, Orçamento e Avaliação Institucional (DPO). Tendo como objetivos estratégicos da área de TIC da UnB descritos no PDTI 2019-2022 [5]:

- Aprimorar o alinhamento, planejamento e a organização dos serviços de TICs prestados à comunidade da UnB, visando o atendimento com excelência das atividades de ensino, pesquisa, extensão, inovação e gestão da Universidade;
- Aprimorar a construção, a aquisição e a implementação de serviços de TICs prestados à comunidade da UnB;
- Aprimorar a entrega, o suporte e a operação de TICs prestados à comunidade da UnB;
- Promover atualização tecnológica dos sistemas e da infraestrutura de TIC da UnB;
- Garantir a conectividade, qualidade e segurança dos serviços de TICs;

- Aprimorar a comunicação das áreas responsáveis da TIC com a comunidade da UnB, visando o atendimento com excelência atividades de ensino, pesquisa, extensão, inovação e gestão da Universidade;
- Promover soluções de TIC com qualidade e de forma tempestiva;
- Atender à legislação pertinente à área de TI;
- Aprimorar o monitoramento, a avaliação e a mensuração dos serviços de TICs;
- Ampliar a participação no ciclo de vida das políticas e serviços públicos, principalmente voltados para o ensino superior público;
- Garantir o efetivo atendimento às demandas de TIC e melhorar a disponibilidade dos sistemas e serviços de TIC.

4.2.3 Escopo

O escopo desta análise de risco é o sistema SEI e seus ativos envolvidos na sustentação e disponibilidade do serviço a comunidade acadêmica.

4.2.4 Critérios

De acordo com a ISO 31000:2018 ao definir os critérios de riscos, convém que os fatores a serem considerados incluam os aspectos de:

- Natureza e tipos de causa e consequência;
- Como a probabilidade será definida;
- A evolução no tempo da probabilidade e/ou consequência;
- Nível de risco a ser determinado.

As documentações técnicas referente ao sistema SEI devem ser o ponto de partida para a coleta de dados, assim como o entendimento geral sobre a gestão de riscos utilizada na sustentação do sistema. Para as reuniões com grupo focal, foram selecionados os servidores que trabalham diretamente na sustentação do sistema SEI. A nível de exclusão, não serão tratados outros sistemas críticos da UnB, assim como não serão analisados dados fora do escopo dessa pesquisa.

Utilizou-se para descrever a probabilidade de riscos e critérios de avaliação e classificação o Guia de gestão de riscos da UnB [18].

4.3 Análise de risco na STI

De acordo com a resolução do conselho de administração nº 0004/2019, há necessidade de promover um tratamento adequado de riscos na UnB. Diante disso, há imprescindibilidade de se inciar ações para se adequar as normas e legislações federais refente a gestão de riscos. Além desta adequação, o monitoramento de riscos realizado pelas áreas de tecnologia facilita o preenchimento de relatórios gerenciais e imposições legais de órgãos de controle.

Os riscos podem ter maior ou menor grau de impacto e probabilidade de ocorrência. Diante disso, se torna necessário priorizá-los a fim de aumentar o desempenho do sistema e evitar possíveis eventos de indisponibilidade. A relevância dos riscos em um ambiente de tecnologia variam bastante possuindo diversos fatores que precisam ser levantados e analisados no ambiente de sustentação do sistema. Desta forma, se torna necessário priorizá-los com o intuito de aumentar o desempenho do sistema ou da produção de uma empresa, assim, de acordo com o impacto de determinado fator de risco, se pode direcionar a priorização ou não daquele evento.

Os resultados obtidos na identificação de riscos tentou evidenciar ao máximo os possíveis riscos que ocorrem ou que podem ocorrer neste processo e posteriormente, classificou-os utilizando a matriz de probabilidade de riscos e matriz de criticidade utilizando modelos em uso na UnB e STI. Essa etapa de classificação se faz importante para que em caso de eventos simultâneos ou indisponibilidade total ou parcial do sistema, se possa priorizar o tratamento dos riscos mais criticos e restauração do sistema em um prazo mais curto de tempo possível.

De acordo com o Guia de gestão de riscos da UnB[18], a probabilidade do risco representa a chance ou a possibilidade do risco se materializar. A probabilidade consiste na medição de o quão provável é a ocorrência do risco, assim, na probabilidade deve-se analisar o quão fácil ou difícil é que determinado risco aconteça. Desta forma, a probabilidade pode ser medida em níveis, ou porcentagens. Na STI a escala de probabilidade é utiliza em níveis descritos na tabela 4.1.

Grau de Probabilidade	**Definição**
1 - Muito baixo	Chance muito rara de acontecer o evento
2 - Baixo	Raramente existe a ocorrência deste tipo de evento
3 - Médio	É comum a ocorrência deste tipo de evento
4 - Alto	São frequentes a ocorrência deste tipo de evento

Tabela 4.1: Grau de probabilidade de risco utilizado na STI
Fonte: Monitoramento de Riscos da STI

A tabela acima demonstra a probabilidade de um evento ocorrer e será utilizada nesta pesquisa com o intuito de definir o grau de ocorrência e a probabilidade do evento ocorrer

no ambiente de produção do sistema SEI. Porém sabe-se que a matriz de riscos é composta pela probabilidade e impacto, sendo necessário apresentar nesta pesquisa a matriz de impacto utilizada na STI para gestão de riscos. Na tabela 4.2 abaixo e apresentada a tabela de grau de impacto a ser utilizada nesta pesquisa.

Grau de Impacto	**Definição**
1 - Muito Baixo	Se o evento ocorrer, não produz impacto na operação. As atividades operacionais continuam sendo realizadas.
2 - Baixo	Se o evento ocorrer, produz um pequeno aumento de custo ou atraso operacional. As atividades operacionais continuam sendo realizadas.
3 - Médio	Se o evento ocorrer, produz um impacto moderado no processo, e as atividades operacionais continuam sendo realizadas, assim como as funções relacionadas ao processo.
4 - Alto	Se o evento ocorrer, produz um grande impacto em um processo, e as atividades operacionais não continuam sendo realizadas na sua totalidade; idem para as funções relacionadas ao processo.

Tabela 4.2: Grau de Impacto de riscos utilizado na STI

De acordo com o guia de gestão de risco da UnB [18], o impacto do risco representa o efeito ou o resultado da materialização dos riscos no processo e nos objetivos que se pretende alcançar.

Dada a matriz de probabilidade e impacto, será calculado o risco inerente, calculado a partir do produto da probabilidade (P) e do impacto (I). Inicialmente, o nível de risco é determinado sem levar em consideração os controles internos que podem reduzir a probabilidade ou impacto dos riscos identificados. Dessa forma, é possível observar o nível de risco inerente ao processo e a mudança do nível de risco após a aplicação dos controles.

A análise de risco realizada para os eventos de ameaça a disponibilidade do sistema SEI estão descritas no Apêndice C desta pesquisa.

Assim, o grau de criticidade do risco é estabelecido pela multiplicação dos fatores de probabilidade e impacto. Na tabela 4.3 temos os níveis da matriz de criticidade utilizada na STI.

Grau de Criticidade	Probabilidade x Impacto
Muito baixo	Valor de 1 a 2
Baixo	Valor de 3 a 4
Médio	Valor de 5 a 9
Alto	Valor de 10 a 16

Tabela 4.3: Grau de criticidade de risco utilizado na STI
Fonte: Monitoramento de Riscos da STI

4.4 Acordo de níveis de serviço estabelecidos na STI

A disponibilidade está relacionada à taxa de ocorrência de falhas nos componentes de um sistema. Uma medida comum de confiabilidade de um componente é o tempo médio entre falhas (MTBF - Mean Time between Failures), que pode ser calculado pela divisão do tempo total de operação do equipamento pelo número de total de falhas MTBF = (Tempo total de operação) / (Número total de falhas). O MTBF de um sistema é obtido pela soma dos tempos de operação de todas as unidades, incluindo as que não falharam, e dividindo pelo somatório de falhas das unidades. Já o tempo de operação é o somatório de horas que as unidades estavam em uso, ou seja, não estavam desligadas. O tempo médio de reparação (MTTR - Mean Time To Repair) caracteriza o espaço de tempo que decorre entre a ocorrência da falha e a total recuperação do sistema em estado operacional.

Desta forma, na tabela 4.4 é identificado o tempo de indisponibilidade aceitável para o sistema SEI da Universidade de Brasília.

Período	SLA aceitável ao ano
Diariamente	4 minutos e 19 segundos
Semanal	30 minutos e 14 segundos
Por mês	2 horas 11 minutos e 29 segundos
Anual	1 dia 2 horas 17 minutos e 50 segundos

Tabela 4.4: Tempo de indisponibilidade aceitável por período

Os prazos acordados de Service Level Agreement (SLA) para os serviços críticos de tecnologia da STI são generalizados não sendo individualizados e divididos de acordo com o grau de criticidade ou aceitação de riscos. Desta forma foi possível levantar o tempo de indisponibilidade do sistema SEI para o prazo de 2 anos (2020 e 2021). De acordo com a tabela 4.5, percebe-se que os acordos de nível de serviços para o sistema SEI foram respeitados durante o período de análise.

SLA	Indisponibilidade
99,92%	14 horas e 38 minutos

Tabela 4.5: Tempo de indisponibilidade do sistema SEI 2020 e 2021

Percebe-se que, mesmo com a grande quantidade de eventos analisados, parte desses eventos não causou a interrupção de disponibilidade do serviço e que as causas de indisponibilidade podem ter surgido de manutenções ou atualizações do sistema, estas possíveis causas serão analisadas nas próximas sessões desta pesquisa.

4.5 Impacto da indisponibilidade ao negócio

A análise de impacto ao negócio faz parte de qualquer plano que tenha como objetivo minimizar os riscos. Auxilia no planejamento da inevitabilidade das consequências e seu custo. Desta forma, pode auxiliar a prever consequências de interrupções e seus processos e sistemas, coletando dados relevantes que podem ser usados para desenvolver estratégias para a empresa utilizar em casos de emergência.

A indisponibilidade do sistema SEI gera impacto ao negócio quando se torna ineficaz na entrega de serviços a comunidade acadêmica e comunicação com outros órgãos do governo federal. Dentre o tempo percorrido de análise não foi identificado impactos relativos a atividades acadêmicas ou relacionadas a perda de informações ou indisponibilidade de realização de atividades no uso do sistema. Também não foram identificados eventos relacionados a perda de informações ou falha de acesso ao sistema durante o período comercial. Desta forma, o tempo de indisponibilidade de 14 horas e 38 minutos não teve impacto ao negócio, visto que não foi identificado até este momento a indisponibilidade por riscos não aceitáveis.

4.6 Coleta de dados e informações

A coleta de dados é um processo que visa reunir os dados para uso secundário por meio de técnicas específicas de pesquisa. A coleta de dados é importante pois observa dados não documentados. A coleta de dados do sistema Zabbix e Citsmart no período de pesquisa de 2 anos (2019 à 2021), com um total de 1.458 eventos ocorridos.

Percebe-se no gráfico da figura 4.1 que os eventos de hardware são grande maioria dos dados levantados, seguidos de eventos de indisponibilidade, eventos de software e eventos de segurança respectivamente. A de se evidenciar que nem todo evento causa indisponibilidade. Alguns eventos desta lista estão relacionados a atividades de rotina para manutenção do sistema ou da infraestrutura de tecnologia que suporta o sistema, como mostra a figura relacionada a eventos de indisponibilidade. Assim, temos a porcentagem descrita na figura 4.1 em relação a indisponibilidade, eventos de hardware, eventos de software e eventos de segurança.

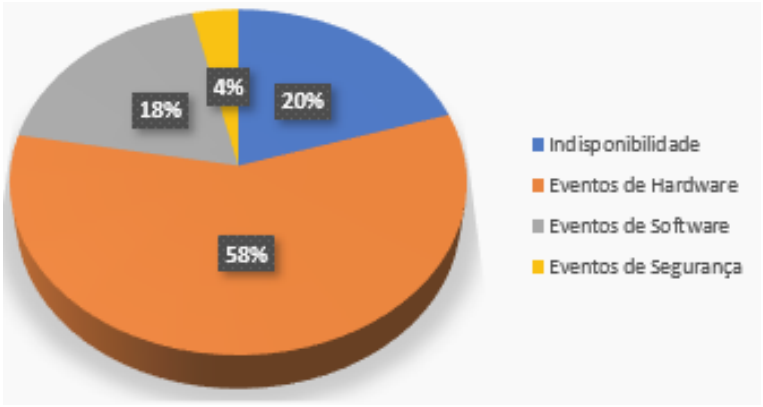

Figura 4.1: Percentual de eventos monitorados
Fonte: Elaboração própria.

O gráfico contido na figura 4.2, demonstra as causas de indisponibilidades ocorridas no período em pesquisa, fragmentando-os em causas encontradas com frequência. É de grande importância entender este gráfico, os principais eventos de indisponibilidade ocorridos e o grau de importância de cada evento em relação a disponibilidade do sistema na instituição. Desta forma, percebe-se que os eventos de manutenção representam mais de 50% dos dados levantados, seguidos de atualização de sistema, indisponibilidade de serviços de rede, banco de dados e correções de falha de segurança do sistema.

Figura 4.2: Eventos de indisponibilidade
Fonte: Elaboração própria.

A quantidade de eventos de manutenção refletem a criticidade que representa o sistema SEI para a Universidade de Brasília. Devido a esta importância o sistema passa por diversas atividades de manutenção, desde a infraestrutura até as melhorias na parte de desenvolvimento do sistema.

4.6.1 Reuniões com equipe de sustentação ao SEI

As reuniões com a equipe de infraestrutura foram realizadas na primeira quinzena de dezembro do ano de 2021, sendo importantes para encontrar informações não documentadas e atividades de rotinas envolvendo a sustentação do ambiente. A duração de cada reunião foi em média 20 minutos. Os participantes da reunião foram: 2 Administradores de infraestrutura 2 Administradores de sistema e 1 coordenador de infraestrutura. Durante as discussões, algumas perguntas e respostas foram obtidas sobre a infraestrutura e sustentação do ambiente. No Apêndice D desta pesquisa encontra-se o roteiro de reuniões realizadas.

Os questionamentos foram formulados de forma a levantar informações relacionadas a sustentação do sistema SEI e foram expostos e conduzidos pelo pesquisador durante os encontros.

Na pergunta 1, foi questionado aos participantes se consideram o serviço SEI um dos serviços críticos fornecidos a comunidade. Neste ponto, todos os participantes concordaram que sim, o sistema SEI é um dos sistemas mais críticos sustentados pela STI atualmente conforme mostra a figura 4.3.

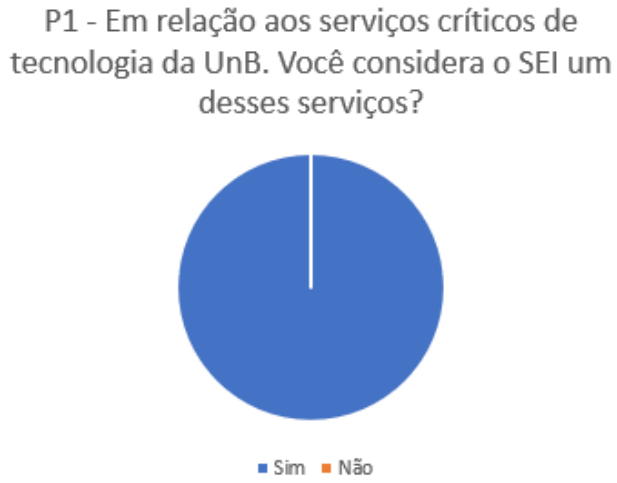

Figura 4.3: Pergunta 1 roteiro de reunião
Fonte: Elaboração própria.

A pergunta 2 é referente aos ativos relacionados ao sistema SEI. Foi questionado aos participantes, caso aconteça algum evento extremos tipo tempestade, queimadas ou desabamentos se os ativos estariam seguros e se o sistema continuaria disponível caso ocorresse algum evento extremo. Neste ponto, 4 dos entrevistados responderam que sim, principalmente pela fato de toda infraestrutura esta alocada na sala cofre, porém levantou-se por parte de 1 participante a alto disponibilidade dos ativos. De acordo com o participante não existe alto disponibilidade dos ativos de suporte ao SEI.

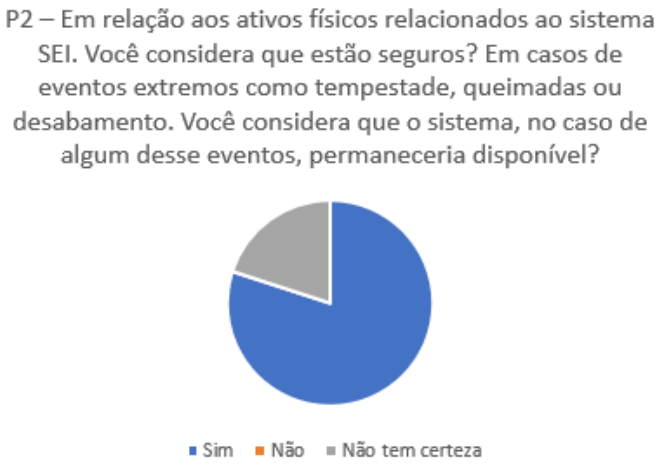

Figura 4.4: Pergunta 2 roteiro de reunião
Fonte: Elaboração própria.

Na pergunta 3 questiona-se a existência de rotinas de backup. Os participantes informam que tem ciência das rotinas de backup mas nem todos conhecem as mídias que são armazenadas, não sabem se o armazenamento é feito apenas em disco ou se existe rotinas de armazenamento em fita magnética. Porém, todos acreditam que as mídias são armazenadas em sala protegida no prédio da STI.

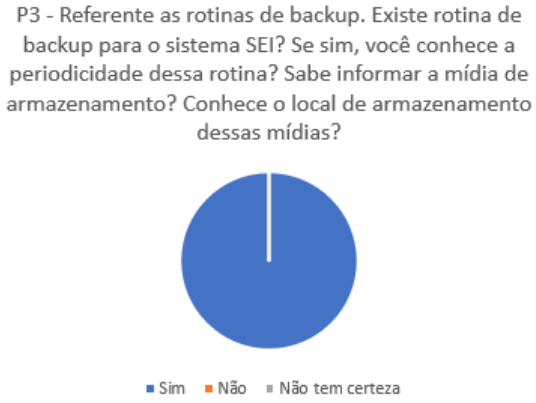

Figura 4.5: Pergunta 3 roteiro de reunião
Fonte: Elaboração própria.

A pergunta 4, ainda está relacionada a realização de backup. Os participantes foram questionados se existe algum processo documentado relacionado a restauração em caso de perda de dados e se nos 2 últimos anos houve indisponibilidade do SEI por conta de perda de dados. Neste caso, a maioria dos participantes informou não conhecer nenhum procedimento relacionado a restauração, porém conhecem os meios de solicitar a restauração de dados em caso de perda. Também informaram que não ocorreu indisponibilidade do SEI por conta de perda de informações.

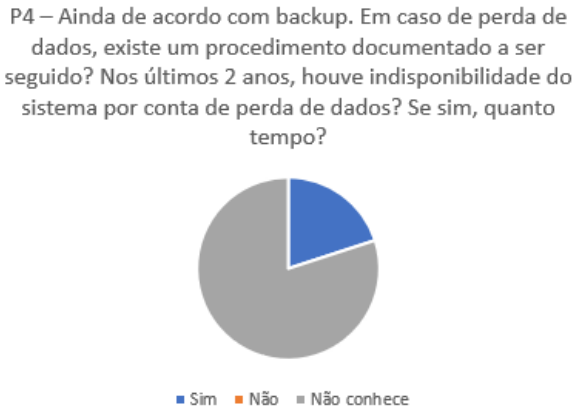

Figura 4.6: Pergunta 4 roteiro de reunião
Fonte: Elaboração própria.

A questão 5 tratou principalmente de plano de contingência. Foram questionados se em caso de falha de um ativo físico, o serviço seria migrado para outro ativo em redundância e se existe ativo algum plano de contingência em caso de falha de ativos. Nesta questão a maioria dos entrevistados informou não ter ciência de ativos em redundância e também não conhecem o plano de contingência ativo na STI para o sistema SEI.

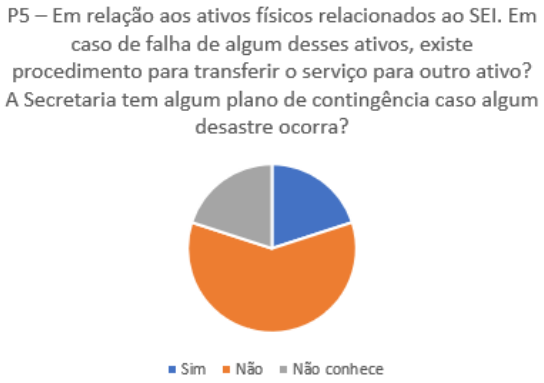

Figura 4.7: Pergunta 5 roteiro de reunião
Fonte: Elaboração própria.

A pergunta 6 esta relacionada a ciclo de gestão de risco em relação ao sistema SEI. Os participantes foram questionados se existe levantamento de riscos na sustentação do sistema SEI e se é possível descrever algum risco relacionado ao serviço. Os participantes informaram que não conhecem a documentação de riscos levantados na sustentação do sistema, porém, podem descrever riscos relacionados a segurança, principalmente relacionados a vulnerabilidade de sistemas, ao levantamento e análise de eventos críticos de sistema, a base de conhecimento relacionada a eventos críticos ocorridos, ao alinhamento nas janelas de manutenção e aplicação de atualizações do sistema e rotinas de backup.

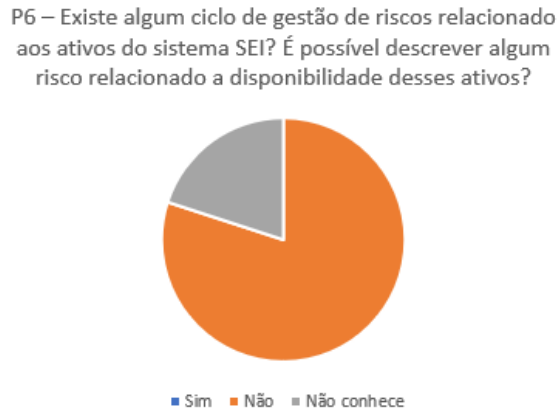

Figura 4.8: Pergunta 6 roteiro de reunião
Fonte: Elaboração própria.

A pergunta 7 está relacionada a aplicação de medidas de segurança relacionados ao sistema. Foram questionados se o sistema possui medidas de análise e melhorias de segurança aplicados ao sistema. Nesta pergunta todos informaram que a rotina de análise de vulnerabilidades do sistema é frequente e que em caso de vulnerabilidades encontradas os processos de homologação e desenvolvimento da solução são aplicados imediatamente. Uma das vulnerabilidades corrigidas sem que houvesse perda de integridade de informações foi a ocorrida em 2019 no modulo de pesquisa pública do sistema que permitia a usuários externos acesso a documentos sigilosos. Esta vulnerabilidade afetou diversas instituições públicas que utilizam o sistema SEI.

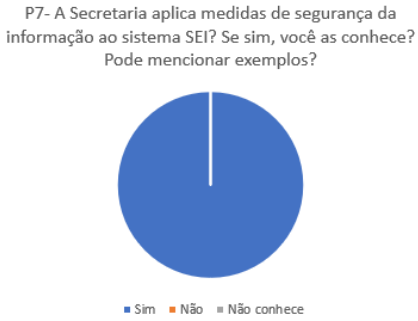

Figura 4.9: Pergunta 7 roteiro de reunião
Fonte: Elaboração própria.

A questão 8 esta relacionada aos impactos e consequências de eventos de indisponibilidade do sistema SEI. Os participantes afirmaram que a indisponibilidade do sistema pode causar, atrasos nos processos com tramite no sistema, indisponibilidade de recursos visto que todas as solicitações são feitas pelo sistema, atraso em pesquisas, atrasos em processos administrativos, falta de pessoal, atraso no lançamento de notas e históricos escolares, dentre outros. Durante a reunião ficou evidente a importância do sistema na ro-

tina administrativa e acadêmica da instituição, devido ao seu gerenciamento de processos relacionados a continuidade de negócio da universidade.

As questões 9 e 10 estão relacionadas aos riscos na sustentação do sistema SEI. Ambas questionam os participantes se a STI levanta riscos relacionados ao sistema e os avalia, afim de entender o real impacto de cada risco levantado. Nesta pergunta os participantes não souberam responder a pergunta porém, acreditam que os riscos relacionados a sustentação do sistema SEI é de conhecimento de todos inclusive dos gestores e que existe dialogo com a alta gestão da Secretaria em relação aos riscos envolvidos e as soluções levantadas pela equipe de sustentação. Lembram também que todas as questões relacionadas ao sistema passam pelo Comitê Gestor do Sistema SEI que caso entenda que o processo a respeito da sustentação do sistema precise ser melhor avaliado, este pode solicitar diretamente a direção da STI tais melhorias.

Na questão 11 ainda relacionada a continuidade de negócios. Os participantes foram questionados se nos 2 últimos anos o sistema SEI sofreu algum evento de indisponibilidade que afetasse a continuidade do negócio da instituição. Neste caso, os participantes não se recordam de nenhum evento de indisponibilidade causado por conta de incidentes de hardware, software ou segurança e caso ocorresse, a comunidade é comunicada através do sistema de e-mail sobre tal fato e divulgação de janela de manutenção do sistema para correção.

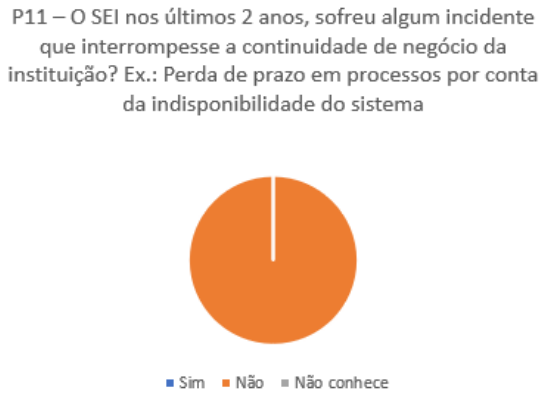

Figura 4.10: Pergunta 11 roteiro de reunião
Fonte: Elaboração própria.

A pergunta 12 é relacionada a existência de um plano de continuidade de negócios relacionado ao sistema SEI, no qual execute no menor tempo possível a disponibilidade do sistema em caso de incidentes ou desastres. Neste questionamento, os participantes informaram que existem procedimentos de restauração do sistema, porém não existe um planejamento de continuidade de negócios diretamente relacionada ao sistema SEI ou serviços críticos da Secretaria.

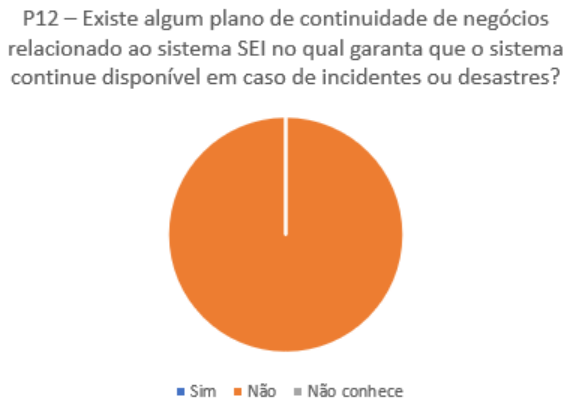

Figura 4.11: Pergunta 12 roteiro de reunião
Fonte: Elaboração própria.

Por fim, os participantes reconheceram a importância do ciclo de gestão de riscos relacionados ao sistema SEI e listaram alguns pontos críticos na sustentação do sistema que pudesse contribuir para esta pesquisa.

- **Janela de homologação e aplicação de atualizações** - Este evento se refere ao tempo alto de homologação necessário para aplicar atualizações e patches de segurança no sistema em produção.
- **Vulnerabilidades** - Parte proativa da equipe em buscar vulnerabilidades no sistema e tratar com antecedência a falha.
- **Ocorrência de eventos** - Monitoramento do ambiente, que estão ocorrendo ou que já ocorreram.
- **Documentação** - Falta de documentação das ocorrências, problemas e soluções executadas durante o evento.

4.6.2 Análise dos dados coletados

Nesta etapa, percebe-se que 90% dos dados coletados foram retirados do sistema Zabbix, as documentações técnicas foram coletadas de órgãos do governo federal e da instituição de pesquisa. As reuniões com a equipe técnica adicionaram informações sobre o processo diário da sustentação do sistema.

Nos dados recebidos do sistema Zabbix, parte dos eventos são relacionados a eventos de hardware. Analisando os eventos, percebe-se que em sua maioria os eventos são relacionadas a paradas do sistema pela realização de backup ou sobrecargas de sistema. Essa parada diária, que ocorre entre às 00:00 até as 03:00, causa indisponibilidade do sistema durante o período da madrugada. A alta gestão da instituição precisa conhecer o risco e

avaliar se é aceitável ou se é possível propor soluções para não acontecer essa indisponibilidade diária. Outros eventos de hardware estão relacionados a paradas no fornecimento de energia e falhas no sistema de virtualização que suportam o sistema.

As falhas no fornecimento de energia são comuns e para estes eventos a Secretaria utiliza um gerador de energia para aumentar a disponibilidade do serviço de energia ao data center. Essa ação por parte da STI é pró-ativa visto que já se conhece o risco e desta forma pode-se tratar o risco pensando na disponibilidade de sistemas ofertados. O gerador de energia passa por rotina de testes bem estabelecidos e conhecidos por todos os funcionários e gestores. O sistema Zabbix é capaz de reconhecer o evento de falta de energia e criar alertas criticos as equipes responsáveis.

Os eventos relacionados a segurança do sistema também foram apontados, porém parte dos eventos de segurança estavam relacionados a aplicação de atualizações e adaptação da infraestrutura de TI para suporte ao sistema. Esses eventos apesar de terem ocasionado indisponibilidade do sistema, foram reportados a comunidade de forma prévia, informando a necessidade de aplicação de correções, assim como o inicio da indisponibilidade e a ativação do sistema como disponível.

Outro percentual importante de eventos que ocorrem são referentes a atualizações de software. O sistema SEI passa por atualizações e melhorias de infraestrutura para comportar a demanda de crescimento de uso do sistema. As atualizações de software do sistema são necessárias, porém, precisam ser implementadas em ambientes de homologação e desenvolvimento, o que pode demorar muito tempo até ser implementadas em ambiente de produção. Esses ambientes existem e são utilizados para validação de funcionalidades do sistema e treinamento de usuários. Toda nova função a ser implementada passa por estes dois ambientes antes de ser aplicada no ambiente de produção.

Desta forma, evidencia-se a importância do registro de eventos para a resiliência do sistema SEI, sua infraestrutura e identificação de rotinas de correção. Os dados coletados dos sistemas de monitoramento, auxiliaram a identificar riscos recorrentes do sistema, analisar possíveis causas e levantar informações sobre rotinas de contingenciamento do sistema em casos de indisponibilidades.

4.7 Ativos primários e suporte

De acordo com o objetivo especifico 3 desta pesquisa, se faz necessário identificar os ativos primários e de apoio ao sistema SEI, assim como suas ameaças e vulnerabilidades no ambiente de produção. De acordo com a norma ISO 27005:2019 [6], convém que o sejam levantados os ativos que podem ser identificados e descritos e que os ativos apresentam vulnerabilidades que podem ser exploradas por ameaças cujo objetivo é comprometer os

ativos primários. Sendo assim, sabe-se que ativos primários são processos e atividades de negócio e as informações relacionadas consideradas críticas pela organização e que ativos de informação dão suporte aos ativos primários.

Todo sistema de gestão de ativos ao ser implementado deve ser esta alinhado com o contexto da organização. De acordo com a Lei geral de proteção de dados (LGPD), o inventário de ativos visa estruturar e manter uma base de dados sobre ativos de informação que sirva de subsídio para os processos de Gestão de Riscos (GR) e da GCN, também no aspecto relativo à privacidade e à proteção dos dados pessoais.

Sabe-se que os ativos críticos do sistema SEI geram valor para a organização. A classificação de um ativo como crítico ou não crítico também pode ser determinada em função da importância destes elementos e das consequências ou de sua ausência ou falha. Desta forma, os ativos físicos levantados nesta pesquisa são considerados como críticos devido a sua importância para sustentação do sistema SEI.

4.7.1 Proteção em divulgação de informações

A proteção dos dados e a forma a qual são armazenados é extremamente importante em ambientes organizacionais. O ambiente tecnológico o qual o sistema SEI está configurado dispõe de segurança física e lógica de dados e equipamentos. Porém, a fim de preservar as informações a qual são armazenadas em sua infraestrutura, algumas informações técnicas e de hardware não podem ser divulgados nesta pesquisa. Sendo assim, limita-se não em sua totalidade a divulgações das informações que não exponham a segurança do ambiente tecnológico da STI.

4.7.2 Ativos primários

São ativos primários (Processos de negócio, sistemas e serviços) considerados críticos pela organização. De acordo com a ISO 27005:2019 [6], os ativos primários normalmente consistem nos principais processos e informações das atividades incluídas no escopo. O levantamento de ativos primários nos ajuda a identificar quais são os processos de negócio e quais são as informações a serem tratadas. Nesta pesquisa os ativos primários estão relacionados ao sistema SEI e listados abaixo:

- Sistema de armazenamento de arquivos
- Sistema de gestão de processos
- Sistema de segurança de acesso
- Sistema de backup

- Processo de acompanhamento de processos
- Processo de distribuição de processos
- Processo gerenciais de sistema
- Processo de acesso a processos
- Processo de controle de processos

O sistema SEI possui diversos sistemas e processos incluídos em suas rotinas. Os processos relacionados a sustentação do sistema, como backup, gerenciamento de acesso e segurança do sistema, foram listados juntamente com processos administrativos do sistema.

4.7.3 Ativos de informação

De acordo com a Política de Segurança da Informação e Cibernética do Banco do Brasil (BB), ativos de informação são os meios de armazenamento, transmissão e processamento da informação, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso. Desta forma, bases de dados e arquivos, contratos e acordos, documentação de sistemas, informações sobre pequisa, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade ou de incidentes, procedimentos de recuperação, sistemas, mídias removíveis devem ser levantados nesta etapa.

De acordo com a norma 27005:2019 [6], ativo de informação é qualquer componente (humano, tecnológico, físico ou lógico) que sustenta um ou mais processos de negócio de uma unidade ou área de negócio e que podem ser classificadas como informação vital, de caráter pessoal, informação estratégica e informação de alto custo. Assim, os ativos de informação encontrados e classificados como informação estratégica são:

- Documentação técnica
- Topologia de rede
- Manuais de utilização do sistema SEI
- Treinamentos
- Procedimentos de restauração do sistema
- Documentações gerais de uso do sistema

Toda a documentação técnica disponibilizada pelo governo federal para implantação, administração e infraestrutura do sistema SEI está disponível no portal do Ministério da Economia [70]. O guia prático do SEI [71] disponível para todo os usuários do sistema na UnB, se faz como manual de uso do sistema no âmbito da Universidade de Brasília. Não foi encontrado na documentação técnica do sistema, plano de continuidade de negócios SEI, exitem procedimentos de recuperação e procedimentos técnicos para backup e restauração do sistema em caso de desastres ou falhas.

4.7.4 Ativos de suporte

O levantamento de todos os equipamentos que fazem sustentação ao sistema SEI são importantes para a gestão de riscos e planejamento de continuidade de negócio do sistema. Na figura 4.12 visualiza-se os ativos de suporte ao sistema e no apêndice B desta pesquisa, os ativos são catalogados de forma individual.

UnB	Tipo do Doc. Documento interno de criticidade de	Doc. Nº 01	Revisão 01
	Data Emissão 10/12/2021	Data Vigência Indefinida	Página 01
	Lista de ativos de informação priorizados sistema SEI		
	Sistema eletrônico de informações - SEI da Universidade de Brasília		
Compilado por: Cristiano Magno de Morais			
Data: 5/12/2021			
Ativo: Sistema Eletrônico de Informações - SEI			
Dono do serviço: Grupo Gestor do Sistema SEI			
Responsável técnico suporte: Coordenação de serviços especializados - CSE			
Contato imediato: 61 3107-0000			
Analisado por: Chefe do setor de redes			
Analisado por: Chefe da divisão de Serviços especializados			
Analisado por: Chefe do setor de segurança			
Analisado por: Chefe da divisão de Data Center - DDC			

Localização	Código Área/Diretoria	Prioridade	Descrição (nome) do ativo	Tipo	Ameaças
Sala cofre	DDC	Alta	Blade G4	Equipamento crítico	Falta de energia, mal funcionamento de peças e conexões de rede, mal configuração, superaquecimento
Sala cofre	DDC	Alta	Storage	Equipamento crítico	Falta de energia, mal funcionamento de peças e conexões de rede, mal configuração, superaquecimento, falta de espaço de armazenamento, furto de informações, vulnerabilidades de sistema
Sala cofre	CSE	Alta	Backup	Equipamento crítico	Falta de energia, mal funcionamento de peças e conexões de rede, falha em robô de backup, falha no sistema de backup, falha de sistema operacional, erro de configuração, falta de fita magnética, furto de informações, ataques externos, ataques internos, fim do suporte com o fabricante, falha de conexão com storage
Sala cofre	CSI	Alta	Firewall	Equipamento crítico	Falta de energia, erro de configuração, falha de rede, ataque externo ou interno, falha de comunicação com o provedor de internet, vulnerabilidade de software
Sala cofre	Redes	Alta	Switch	Equipamento crítico	Falta de energia, erro de configuração, ataque externo ou interno, falha na comunicação de rede, furto de equipamento, equipamento danificado
Sala cofre	DDC	Alta	Sala cofre	Local do equipamento/serviço	Acesso indevido, falta de energia, falha no sistema de refrigeração, falha no sistema de acesso, superaquecimento, falha no sistema de cameras, falha nas conexões de rede, alagamento, queimadas, desmoronamento, falha nas baterias de energia, falha no sistema antifogo, travamento da porta, furto de informações

Figura 4.12: Equipamentos críticos sustentação sistema SEI
Fonte: Elaboração própria.

De acordo com a ISO 27005:2019 [6], as instalações compreendem o lugar onde são encontrados o escopo e os meios físicos necessários para as operações nele contidas, neste caso todos os ativos estão localizados no data center localizado na STI. As maiores ameaças aos ativos físicos, levantados na coleta de dados, estão relacionados a falta de energia, falha no sistema de virtualização, falha no sistema de refrigeração da sala cofre, ataques externos e internos, falhas de hardware ou falha no sistema de backup.

Todos os ativos listados na figura 4.12 foram valorados como prioridade alta, visto que dão suporte a um sistema crítico e possuem aspectos que precisam de atenção por parte da gestão além de servirem de apoio também para outros sistemas disponibilizados pela STI. A avaliação de impacto envolvendo os ativos de suporte, levou em consideração a prioridade do ativo e seu efeito de impacto sendo todos considerados como efeitos imediatos de nível operacional.

4.8 Identificação de riscos ao sistema SEI e infraestrutura

Uma das formas de mitigar riscos é procurar identificar as vulnerabilidades antes que eles sejam explorados por aluma ameaça [72]. Os sistemas de informação das empresas estão vulneráveis a diversas ameaças que podem causar danos aos ativos da empresa como fraudes eletrônicas, espionagem, sabotagem, incêndio, inundação e ataques de crackers. Para que essas vulnerabilidades sejam amenizadas, se faz necessário implementar, monitorar e analisar um conjunto de controles, políticas, processos e procedimentos com o intuito de garantir que os objetivos do negócio e de sua segurança sejam atendidos [73].

Segundo Laudon [74], a maioria das vulnerabilidades e falhas encontradas em softwares têm relação à complexidade e o tamanho das aplicações. No âmbito empresarial, a infraestrutura de TI conta com diversos aplicativos, sistemas operacionais e outros serviços nos diversos ativos existentes, sendo que a manutenção das atualizações e patches são de extrema importância para o correto funcionamento e para a prevenção de vulnerabilidades.

Com base no levantamento obtido na coleta de dados, análise de variáveis de ambiente, levantamento de ativos e vulnerabilidades, a fase de levantamento de ameaças e ações de contingenciamento de ser procedida de identificação, desenvolvimento e a levantamento das ações de contingência, a definição dos respectivos procedimentos de ativação, o estabelecimento de prazos e designação de equipes que ficarão responsáveis pela operacionalização das ações de providência imediata para restauração do sistema, considerando o tempo de espera previsto para restabelecimento da atividade, definidos pelos acordos de níveis de serviço e gestores de informação.

Para a identificação de riscos foi utilizado o método brainstorming com a equipe de especialistas e contou com insumos da coleta de dados, da analise de variáveis de ambiente, do levantamento de ativos e vulnerabilidade e do levantamento das ações de contingenciamento do sistema. A tabela 4.6 demonstra os riscos identificados.

Risco	**Descrição**	**Consequências**
Acesso de pessoas não autorizadas a sala cofre	Acesso de pessoas não autorizadas ao ambiente interno da sala cofre	Furto de informações, equipamentos danificados, furto de equipamentos, violação do sigilo de informações
Ataques externos	Ataques cibernéticos que causam danos ou roubo de informações dos serviços e tem como foco deixar os serviços indisponíveis	Violação do sigilo a informação, perda de dados e informações, indisponibilidade de sistemas, lentidão no acesso aos sistemas, indisponibilidade de dados, indisponibilidade de rede e telefonia, atraso no tramite de processos
Ataques internos	Causados por usuários legítimos da rede, porém, tentando acessar algum serviço ou equipamento para deixa-lo indisponível	Violação do sigilo a informação, perda de dados e informações, indisponibilidade de sistemas, lentidão no acesso aos sistemas, indisponibilidade de dados, indisponibilidade de rede e telefonia, atraso no tramite de processos
Falha humana acidental	Causada pela falta de atenção dos usuários	Indisponibilidade do sistema, indisponibilidade de ativos, lentidão no acesso a sistemas, perda de dados e informações, falhas de segurança de sistema, atraso na distribuição de processos

Falha humana por imperícia	Causada por falta de capacidade técnica ou conhecimento suficiente para dá suporte em algum serviço ou sistema	Indisponibilidade do sistema, indisponibilidade de ativos, lentidão no acesso a sistemas, perda de dados e informações, falhas de segurança de sistema, atraso na distribuição de processos, falha na realização da restauração do sistema, perda de dados de backup
Falta de energia elétrica	Causada por fator externo ou interno à rede elétrica do prédio ou de sua localidade com duração na interrupção superior a 3 horas	Indisponibilidade de sistemas, indisponibilidade de ativos, atraso na distribuição de processos, indisponibilidade de restauração do sistema
Falha na migração e mudanças em aplicações virtuais	Causada na manipulação e instalação de atualizações que possam impactar nas disponibilidades do negócio	Indisponibilidade de sistema, indisponibilidade de informações, falhas na aplicação, falhas de rede, falhas operacionais de sistema
Indisponibilidade de equipamentos	Causado por equipamentos antigos ou equipamentos que por algum motivo precisem de reparo técnico	Indisponibilidade de sistema, indisponibilidade de dados e informações, falhas na distribuição de processos, falha na restauração do sistema
Problema de conexão	Causado principalmente por rompimentos de cabos de rede e fibra óptica ou por problemas de equipamentos de rede (Roteadores ou Switches)	Indisponibilidade do sistema, indisponibilidade de ativos, lentidão no acesso a sistemas, perda de dados e informações, falhas de segurança de sistema, atraso na distribuição de processos, falha na realização da restauração do sistema, perda de dados de backup
Avaliação e identificação de eventos críticos	Causados por falta de pessoal para monitoramento dos eventos no serviço Zabbix	Tempo de solução de problemas elevado, falhas de equipamentos, falhas em conexão de rede, soluções reativas

Perda de capital humano	Causados pela perda de capital humano técnico	Tempo de solução de problemas elevado, falhas de equipamentos, falhas em conexão de rede, soluções reativas
Problemas na sala cofre	Risco que pode comprometer a vida útil dos equipamentos, causando superaquecimento, inundação, incêndios	Indisponibilidade do sistema, indisponibilidade de ativos, lentidão no acesso a sistemas, perda de dados e informações, falhas de segurança de sistema, atraso na distribuição de processos, falha na realização da restauração do sistema, perda de dados de backup, tempo de solução de problemas elevado, falhas de equipamentos, falhas em conexão de rede, soluções reativas

Tabela 4.6: Ameaças, falhas encontradas e ações de contingenciamento

Ao total identificou-se 11 riscos, nos quais esses foram categorizados e levantadas as ações de contingenciamento realizadas em cada risco. Esse é o primeiro passo no processo de GR que orientou a etapa de análise de riscos e as demais, nos quais utilizaram os resultados das causas e consequências apontadas.

4.8.1 Análise de risco

O propósito da análise de riscos é compreender a natureza dos riscos e suas características, incluindo os níveis de riscos [23]. Esse processo envolve o detalhamento de incertezas, fontes de riscos, consequências, probabilidades, eventos, cenários, controles e sua eficácia [23].

O resultado dessa etapa contemplou a utilização da matriz de riscos utilizada na STI. O resultado desse passo detalhou as incertezas, as fontes de riscos, as consequências e as probabilidades de ocorrência dos riscos indesejados identificados previamente no passo de identificação de riscos na tabela 4.6.

Com os riscos e suas consequências coletadas na etapa de identificação de riscos, na análise de risco foi possível identificar a probabilidade de ocorrência daquele evento acontecer, assim como, o seu grau de impacto na organização. Esse levantamento é importante para que se possa avaliar, em caso de indisponibilidade do sistema, as prioridades a serem tratadas dentro de um ambiente geral de sustentação do sistema.

O resultado da análise de riscos sobre o sistema SEI apontou a existência de riscos de alto nível conforme é detalhado nas próximas etapas desta pesquisa, assim como os níveis de probabilidade e impacto conforme mostra a figura 4.15.

Risco	Causa	Consequência	Probabilidade	Impacto
Acesso de pessoas não autorizadas a sala cofre	Acesso de pessoas não autorizadas dentro da sala cofre	Furto de informações, equipamentos danificados, furto de equipamentos, violação do sigilo de informações	Baixo	Alto
Ataques externos	Ataques cibernéticos que causam danos ou roubo de informações dos serviços e tem como foco deixar os serviços indisponíveis	Violação do sigilo a informação,perda de dados e informações, indisponibilidade de sistemas, lentidão no acesso aos sistemas, indisponibilidade de dados, indisponibilidade de rede e telefonia, atraso no tramite de processos	Alto	Alto
Ataques internos	Causados por usuários legítimosda rede, porém, tentando acessaralgum serviço ou equipamentopara deixa-lo indisponível	Violação do sigilo a informação,perda de dados e informações, indisponibilidade de sistemas, lentidão no acesso aos sistemas, indisponibilidade de dados, indisponibilidade de rede e telefonia, atraso no tramite de processos	Médio	Alto
Falha humana acidental ou imperícia	Causada pela falta de atenção dos usuáios ou técnicos	Indisponibilidade do sistema, indisponibilidade de ativos, lentidão no acesso a sistemas, perda de dados e informações, falhas de segurança de sistema, atraso na distribuição de processos no ambiente de desenvolvimento, indisponibilidade no sistema de homologação, indisponibilidade	Baixo	Baixo
Falta de energia elétrica	Causada por fator externo ou interno à rede elétrica do prédio ou de sua localidade com duração na interrupção superior a 3 horas	Indisponibilidade de sistemas, indisponibilidade de ativos, atraso na distribuição de processos, indisponibilidade de restauração do sistema	Médio	Alto
Falha na migração e mudanças em aplicações virtuais	Causada na manipulação e instalação de atualizações que possam impactar nas disponibilidades do negócio	Indisponibilidade de sistema, indisponibilidade de informações, falhas na aplicação, falhas de rede, falhas operacionais de sistema	Muito Baixo	Muito Baixo
Indisponibilidade de equipamentos	Causado por equipamentos antigos ou equipamentos que por algum motivo precisem de reparo técnico	Indisponibilidade de sistema, indisponibilidade de dados e informações, falhas na distribuição de processos, falha na restauração do sistema	Médio	Alto
Problema conexão	Causado principalmente por rompimentos de cabos de rede e fibra óptica ou por problemas de equipamentos de rede (Roteadores ou Switches)	Indisponibilidade do sistema, indisponibilidade de ativos, lentidão no acesso a sistemas, perda dedados e informações, falhas de segurança de sistema, atraso na distribuição de processos, falha na realização da restauração do sistema, perda de dados de backup	Médio	Alto
Riscos na identificação de eventos	Causados por falta de pessoal para monitoramento dos eventos no serviço Zabbix	Tempo de solução de problemas elevado, falhas de equipamentos, falhas em conexão de rede, soluções reativas	Baixo	Baixo
Risco Pessoal	Causados pela perda de capital humano técnico	Tempo de solução de problemas elevado, falhas de equipamentos, falhas em conexão de rede, soluções reativas, perda de conhecimento técnico, perda de credibilidade	Médio	Muito Baixo
Problemas sala cofre	Risco que pode comprometer a vida útil dos equipamentos, causanddo superaquecimento, imundação, incêndios e indisponibilidades	Indisponibilidade do sistema, indisponibilidade de ativos, lentidão no acesso a sistemas, perda de dados e informações, falhas de segurança de sistema, atraso na distribuição de processos, falha na realização da restauração do sistema, perda de dados de backup, tempo de solução de problemas elevado, falhas de equipamentos,falhas em conexão de rede, soluções reativas	Baixo	Alto

Figura 4.13: Matriz de riscos da etapa de Análise de riscos
Fonte: Elaboração própria.

Nesta etapa foi possível identificar eventos com grau de probabilidade baixo, médio e alto e impactos dentro da organização. Percebe-se que ataques externos, falta de energia, problemas com equipamento de hardware e problemas com serviços de comunicação são eventos com maiores probabilidade de ocorre e possuem um nível de impacto alto para organização.

4.8.2 Avaliação de riscos

A avaliação de riscos tem como proposta apoiar as decisões [23], sendo um procedimento que consiste no estudo aprofundado a respeito de determinada atividade realizada dentro de uma organização. Envolve a comparação dos resultados da análise de riscos com os critérios de riscos estabelecidos para determinar onde são necessárias ações adicionais. O resultado obtido da definição dos passos de avaliação de riscos foi a matriz de probabilidade e impacto. A matriz estimula a instituição a imaginar situações futuras, pensando principalmente nas consequências e nos impactos dos riscos identificados na disponibilidade do sistema SEI.

Risco	Causa	Consequência	Probabilidade	Impacto	Criticidade
Acesso de pessoas não autorizadas a sala cofre	Acesso de pessoas não autorizadas dentro da sala cofre	Furto de informações, equipamentos danificados, furto de equipamentos, violação do sigilo de informações	Baixo	Alto	Média
Ataques externos	Ataques cibernéticos que causam danos ou roubo de informações dos serviços e tem como foco deixar os serviços indisponíveis	Violação do sigilo a informação,perda de dados e informações, indisponibilidade de sistemas, lentidão no acesso aos sistemas, indisponibilidade de dados, indisponibilidade de rede e telefonia, atraso no tramite de processos	Alto	Alto	Alta
Ataques internos	Causados por usuários legítimos da rede, porém, tentando acessar algum serviço ou equipamento para deixa-lo indisponível	Violação do sigilo a informação,perda de dados e informações, indisponibilidade de sistemas, lentidão no acesso aos sistemas, indisponibilidade de dados, indisponibilidade de rede e telefonia, atraso no tramite de processos	Médio	Alto	Alta
Falha humana acidental ou imperícia	Causada pela falta de atenção dos usuáios ou técnicos	Indisponibilidade do sistema, indisponibilidade de ativos, lentidão no acesso a sistemas, perda de dados e informações, falhas de segurança de sistema, atraso na distribuição de processos no ambiente de desenvolvimento, indisponibilidade no sistema de homologação, indisponibilidade	Baixo	Baixo	Baixa
Falta de energia elétrica	Causada por fator externo ou interno à rede elétrica do prédio ou de sua localidade com duração na interrupção superior a 3 horas	Indisponibilidade de sistemas, indisponibilidade de ativos, atraso na distribuição de processos, indisponibilidade de restauração do sistema	Médio	Alto	Alta
Falha na migração e mudanças em aplicações virtuais	Causada na manipulação e instalação de atualizações que possam impactar nas disponibilidades do negócio	Indisponibilidade de sistema, indisponibilidade de informações, falhas na aplicação, falhas de rede, falhas operacionais de sistema	Muito Baixo	Muito Baixo	Muito Baixa
Indisponibilidade de equipamentos	Causado por equipamentos antigos ou equipamentos que por algum motivo precisem de reparo técnico	Indisponibilidade de sistema, indisponibilidade de dados e informações, falhas na distribuição de processos, falha na restauração do sistema	Médio	Alto	Alta
Problema conexão	Causado principalmente por rompimentos de cabos de rede e fibra óptica ou por problemas de equipamentos de rede (Roteadores ou Switches)	Indisponibilidade do sistema, indisponibilidade de ativos, lentidão no acesso a sistemas, perda dedados e informações, falhas de segurança de sistema, atraso na distribuição de processos, falha na realização da restauração do sistema, perda de dados de backup	Médio	Alto	Alta
Riscos na identificação de eventos	Causados por falta de pessoal para monitoramento dos eventos no serviço Zabbix	Tempo de solução de problemas elevado, falhas de equipamentos, falhas em conexão de rede, soluções reativas	Baixo	Baixo	Baixa
Risco Pessoal	Causados pela perda de capital humano técnico	Tempo de solução de problemas elevado, falhas de equipamentos, falhas em conexão de rede, soluções reativas, perda de conhecimento técnico, perda de credibilidade	Médio	Muito Baixo	Baixo
Problemas sala cofre	Risco que pode comprometer a vida útil dos equipamentos, causanddo superaquecimento, imundação, incêndios e indisponibilidades	Indisponibilidade do sistema, indisponibilidade de ativos, lentidão no acesso a sistemas, perda de dados e informações, falhas de segurança de sistema, atraso na distribuição de processos, falha na realização da restauração do sistema, perda de dados de backup, tempo de solução de problemas elevado, falhas de equipamentos,falhas em conexão de rede, soluções reativas	Baixo	Alto	Média

Figura 4.14: Matriz de riscos da etapa de Avaliação de riscos
Fonte: Elaboração própria.

A avaliação de riscos parte das informações dos passos de identificação e análise de riscos, desta forma o resultado é expresso, a partir da atualização da matriz de riscos de avaliação de riscos.

A partir do processo de avaliação de riscos demonstrado na figura 4.14, segue-se para a etapa de tratamento de riscos.

4.8.3 Tratamento de riscos

O tratamento de riscos tem como objetivo selecionar e implementar as opções para abordar os riscos [23]. As opções para tratar os riscos podem envolver uma ou mais das seguintes ações previstas na ISO 31000:2018:

- Evitar os riscos - parar de realizar tarefas ou processos se eles geram riscos que são simplesmente muito grandes para mitigar com quaisquer outras opções;
- Compartilhar os riscos - transferir o risco ou gerir em comum com outra parte;
- Assumir ou aumentar os riscos de maneira a perseguir uma oportunidade;
- Mudar as probabilidades ou a consequências - incluir a opção de controles para mitigar riscos;e
- Reter os riscos - aceitar o risco sem fazer nada a respeito.

O controle dos riscos ou tratamento de riscos pode utilizar as seguinte respostas ao risco como evitar, mitigar ou aceitar. O resultado obtido para definição de técnicas de identificação de opções de tratamento de riscos envolvidos na disponibilidade do sistema SEI, foi a matriz de probabilidade e impacto da figura 4.14, que é utilizada para demonstrar visualmente os níveis de tolerância da STI a riscos, permitindo aos gestores a aplicação de tratamento proporcional à criticidade e urgência que cada risco representa.

A etapa de tratamento de risco, foi alinhada com especialistas que dão suporte ao sistema SEI e as informações preenchidas na matriz de risco foram analisadas nas sessões de reunião. Porém é importante lembrar que toda a opção de tratamento irá requerer uma decisão do nível de gestão apropriado para o sistema crítico. No caso o coordenador da área de suporte responsável pelo sistema.

As ações de controle devem ser atribuídas a todos os riscos encontrados nas etapas anteriores e podem sem classificadas como Preventivo onde o objetivo é prevenir falhas ou Corretivo quando o objetivo é detectar falhas que já aconteceram. No caso desta pesquisa, todos os controles implementados são caracterizados por serem preventivos.

Na forma de prevenção de danos se busca agir antecipadamente na diminuição da probabilidade de ocorrência ou indisponibilidades que possam atingir o sistema, caso

tais eventos ocorram. Nestes casos, foi adicionado a matriz de tratamento a coluna de ações de contingência, já iniciando um planejamento de tratamento de incidentes para a implementação de continuidade de negócios para o sistema SEI. A figura 4.15 demonstra as ameaças, controles e ações a serem implementadas aos ativos de suporte ao sistema SEI.

UnB	Revisão 01	Doc. Nº 01	Documento interno de ativos críticos
	Data Emissão 10/12/2021	Data Vigência Indefinida	Página 01
	Lista de ativos de informação priorizados sistema SEI Sistema eletrônico de informações - SEI da Universidade de Brasília		

Compilado por: Cristiano Magno de Morais
Data: 5/12/2021
Ativo: Sistema Eletrônico de Informações - SEI
Dono do serviço: Grupo Gestor do Sistema SEI
Responsável técnico suporte: Coordenação de serviços especializados - CSE
Contato imediato: 61 3107-0000
Analisado por: Chefe do setor de redes
Analisado por: Chefe da divisão de Serviços especializados
Analisado por: Chefe do setor de segurança
Analisado por: Chefe da divisão de Data Center - DDC

Equipamento	Ameaças	Controle	Ação
Blade G4	Falta de energia, mal funcionamento de peças e conexões de rede, mal configuração, superaquecimento	Gerador de energia, redundância de baterias, contrato com fabricante do produto para suporte, gerenciamento de acesso e logs, controle de eventos	Mitigar
Storage	Falta de energia, mal funcionamento de peças e conexões de rede, mal configuração, superaquecimento, falta de espaço de armazenamento, furto de informações, vulnerabilidades de sistema	Gerador de energia, redundância de baterias, contrato com fabricante do produto para suporte, gerenciamento de eventos, controle de acesso	Mitigar
Backup	Falta de energia, mal funcionamento de peças e conexões de rede, falha em robô de backup, falha no sistema de backup, falha de sistema operacional, erro de configuração, falta de fita magnética, furto de informações, ataques externos, ataques	Gerador de energia, redundância de baterias,contrato com fabricante do produto, redundância de robos de backup, controle de acesso e guarda de fitas magnéticas, controle de acesso e eventos de sistema	Mitigar
Firewall	Falta de energia, erro de configuração, falha de rede, ataque externo ou interno, falha de comunicação com o provedor de internet, vulnerabilidade de software	Gerador de energia, redundância de baterias, controle de acesso e eventos, controle de versões e regras, redundância de link de internet, atualização de sistema, analise de regras	Mitigar
Switch	Falta de energia, erro de configuração, ataque externo ou interno, falha na comunicação de rede, furto de equipamento, equipamento danificado	Gerador de energia, redundância de baterias, controle de acesso e eventos, controle de versões e regras, redundância de equipamentos, controle de acesso a salas	Mitigar
Sala cofre	Acesso indevido, falta de energia, falha no sistema de refrigeração, falha no sistema de acesso, superaquecimento, falha no sistema de cameras, falha nas conexões de rede, alagamento, queimadas, desmoronamento, falha nas baterias de energia, falha no sistema antifogo, travamento da porta, furto de informações	Controle de acesso, Gerador de energia, redundância de baterias, controle de temperatura, contrato com empresa terceirizada, redundância de link, sala cofre certificada	Transferir/Compartilhar

Figura 4.15: Equipamentos críticos controles aplicados
Fonte: Elaboração própria.

Os controles são ações que são tomadas para prevenir que as ameaças causem indisponibilidade do ativo, assim como prevenir que outros riscos possam ocorrer.

O tratamento de riscos abrange o planejamento e a execução de ações preventivas, mitigadoras ou contingenciais que resultem na diminuição da probabilidade e/ou impacto dos riscos identificados aconteçam. Dessa forma, a ação de mitigar os riscos, neste caso, serão diminuir os impactos ou a probabilidade de indisponibilidade do sistema com a execução dos controles levantados.

As ações de contingência é um tipo de plano preventivo, preditivo e reativo. Apresenta uma opção estratégica que ajuda a controlar situações emergenciais e a controlar consequências negativas de situações de indisponibilidade. A figura 4.16 mostra o tratamento dos riscos encontrados nas fases de identificação, análise e avaliação dos riscos.

Risco	Causa	Consequência	Probabilidade	Impacto	Criticidade	Tipo de risco	Ações de controle	Resposta ao risco	Ações de contingenciamento
Acesso de pessoas não autorizadas a sala cofre	Acesso de pessoas não autorizadas dentro da sala cofre	Furto de informações, equipamentos danificados, furto de equipamentos, violação do sigilo de informações	Baixo	Alto	Média	Operacional	Verificar registro de acessos a sala cofre	Mitigar	A sala cofre possui monitoramento 24x7x365 e controle de acesso
Ataques externos	Ataques cibernéticos que causam danos ou roubo de informações dos serviços e tem como foco deixar os serviços indisponíveis	Violação do sigilo a informação,perda de dados e informações, indisponibilidade de sistemas, lentidão no acesso aos sistemas, indisponibilidade de dados, indisponibilidade de rede e telefonia, atraso no tramite de processos	Alto	Alto	Alta	Operacional	Verificar registros de log de equipamentos e eventos de sistema	Mitigar	Gerenciamento de eventos e redundância de equipamentos firewall. Equipe de tratamento de incidentes - ETIR
Ataques internos	Causados por usuários legítimos da rede, porém, tentando acessar algum serviço ou equipamento para deixa-lo indisponível	Violação do sigilo a informação,perda de dados e informações, indisponibilidade de sistemas, lentidão no acesso aos sistemas, indisponibilidade de dados, indisponibilidade de rede e telefonia, atraso no tramite de processos	Médio	Alto	Alta	Operacional	Verificar registros de log de equipamentos e eventos de sistema	Mitigar	Gerenciamento de eventos e redundância de equipamentos firewall.
Falha humana acidental ou imperícia	Causada pela falta de atenção dos usuáios ou técnicos	Indisponibilidade do sistema, indisponibilidade de ativos, lentidão no acesso a sistemas, perda de dados e informações, falhas de segurança de sistema, atraso na distribuição de processos no ambiente de desenvolvimento, indisponibilidade no sistema de homologação, indisponibilidade	Baixo	Baixo	Baixa	Operacional	Verificar registros de log de equipamentos e eventos de sistema	Mitigar	Capacitação, treinamento e controle de acesso à serviços e sistemas
Falta de energia elétrica	Causada por fator externo ou interno à rede elétrica do prédio ou de sua localidade com duração na interrupção superior a 3 horas	Indisponibilidade de sistemas, indisponibilidade de ativos, atraso na distribuição de processos, indisponibilidade de restauração do sistema	Médio	Alto	Alta	Operacional	Verificar registros de acionamento de gerador de energia e combustivel	Mitigar	Gerador de tanque interno com capacidade de fornecimento de 25 horas e tanque para funcionamento de 100 horas
Falha na migração e mudanças em aplicações virtuais	Causada na manipulação e instalação de atualizações que possam impactar nas disponibilidades do negócio	Indisponibilidade de sistema, indisponibilidade de informações, falhas na aplicação, falhas de rede, falhas operacionais de sistema	Muito Baixo	Muito Baixo	Muito Baixa	Operacional	Verificar registros de eventos relacionados a alterações de infraestrutura e sistema	Aceitar	Uso de máquina virtuais para migração e aplicação para movimentação ágil de máquinas virtuais
Indisponibilida de de equipamentos	Causado por equipamentos antigos ou equipamentos que por algum motivo precisem de reparo técnico	Indisponibilidade de sistema, indisponibilidade de dados e informações, falhas na distribuição de processos, falha na restauração do sistema	Médio	Alto	Alta	Operacional	Verificar registros de log de equipamentos e eventos de sistema	Mitigar	Contrato com fabricantes de equipamentos para suporte
Problema conexão	Causado principalmente por rompimentos de cabos de rede e fibra óptica ou por problemas de equipamentos de rede (Roteadores ou Switches)	Indisponibilidade do sistema, indisponibilidade de ativos, lentidão no acesso a sistemas, perda dedados e informações, falhas de segurança de sistema, atraso na distribuição de processos, falha na realização da restauração do sistema, perda de dados de backup	Médio	Alto	Alta	Operacional	Verificar registros de log de equipamentos e eventos de sistema	Mitigar	Gerenciamento de eventos e redundância de enlaces
Riscos na identificação de eventos	Causados por falta de pessoal para monitoramento dos eventos no serviço Zabbix	Tempo de solução de problemas elevado, falhas de equipamentos, falhas em conexão de rede, soluções reativas	Baixo	Baixo	Baixa	Operacional	Verificar resitros de responsabilidades e comunicações de incidentes	Eliminar	Contrato com empresa terceirizada para monitoramento de eventos
Risco Pessoal	Causados pela perda de capital humano técnico	Tempo de solução de problemas elevado, falhas de equipamentos, falhas em conexão de rede, soluções reativas, perda de conhecimento técnico, perda de credibilidade	Médio	Muito Baixo	Baixo	Operacional	Verificar escala de responsáveis e gestão de sistema	Aceitar	Plano de capacitação e apoio a educação continuada
Problemas sala cofre	Risco que pode comprometer a vida útil dos equipamentos, causanddo superaquecimento, imundação, incêndios e indisponibilidades	Indisponibilidade do sistema, indisponibilidade de ativos, lentidão no acesso a sistemas, perda de dados e informações, falhas de segurança de sistema, atraso na distribuição de processos, falha na realização da restauração do sistema, perda de dados de backup, tempo de solução de problemas elevado, falhas de equipamentos,falhas em conexão de rede, soluções reativas	Baixo	Alto	Média	Operacional	Verificar registro de eventos, acesso e controle	Transferir	Sala certificada com manutenção em dia e redundância de climatização

Figura 4.16: Matriz de riscos da etapa de Tratamento de riscos
Fonte: Elaboração própria.

Os 11 riscos encontrados na sustentação do sistema SEI, assim como suas causas, consequências, probabilidade, impacto, tipo, controle, resposta e contingência. Através da análise de risco foi possível identificar, pontos atenção que podem mitigar riscos operacionais relacionados ao sistema SEI e podem servir como base inicial para implementação de um plano de continuidade de negócios aplicado a este sistema.

Identificou-se que os procedimentos operacionais padrões (POP) estão sendo implementadas na Secretaria, porém, ainda não voltados especificamente para continuidade de negócio mas sim, para ações reativas. Contudo existem planos de contingência para os serviços críticos disponíveis na STI.

4.9 Aplicabilidade da implementação de um Sistema de Gestão de Continuidade de Negócios ao sistema SEI

A análise das ameaças encontradas leva em consideração os eventos recentes acontecidos e o atual cenário mundial em relação a proteção de dados. Mesmo diante de um cenário que nunca tenha sido ameaçado por qualquer tipo de ocorrência, a implantação de um SGCN é importante, sendo utilizada para mensurar o impacto da contingência e definir processos de negócios cruciais para a instituição. Desta forma é evidente a importância de um sistema de continuidade de negócios aplicado ao SEI da Universidade de Brasília entendendo a expectativa da instituição e implementando estratégias de resiliência, projetando possíveis cenários de crise.

O plano de continuidade de negócios é um dos planos que compõe um SGCN sendo acionado caso riscos residuais ocorram, mesmo quando possuam baixa probabilidade de ocorrem.

A STI precisa se adequar a normas e processos institucionais como o guia de gestão de riscos e a POSIC e de controles federais relacionados a continuidade de negócios e segurança da informação. A UnB normatizou a POSIC e nela informa que precisam ser estabelecidos princípios e diretrizes de segurança da informação [33]. Dentre esses princípios estão a gestão de risco, gestão de ativos e a continuidade de negócios.

O desenvolvimento de um sistema de continuidade de negócios possui diversos fatores positivos para a instituição como:

- Minimiza os efeitos de uma paralisação;
- Possibilita a recuperação de dados e sistemas dentro de um curto espaço de tempo;
- Ajuda a empresa a cumprir com suas obrigações legais e estatutárias;

- Eleva os níveis de confiança dos serviços prestados.

No ano de 2011 e 2019 a UnB passou por experiências de alagamentos, perda de equipamentos e indisponibilidade de serviços de tecnologia. Esses episódios foram amplamente divulgados na impressa, pelo fato de ter causado perda de dados de pesquisa importantes e prejudicado a comunidade acadêmica no acesso a serviços acadêmicos. No ano de 2020 aos arredores das instalações do prédio onde se encontra o data center, fortes queimadas ocorreram, porém neste evento não ocorreram danos a equipamentos e indisponibilidade de serviços. Ainda no ano de 2020, com a pandemia decretada mundialmente, os serviços ofertados pela Secretaria tiveram que expandir a oferta para fora do ambiente controlado da rede interna da instituição e passou a ser disponibilizado a toda a comunidade através da internet. Neste contexto, percebe-se a importância da busca por alternativas que visualizem cenários de risco e planejamentos de contingencia para contornar possíveis eventos de indisponibilidades.

O sistema SEI é um dos sistemas críticos sobre guarda da STI. Atende toda a comunidade acadêmica e realiza comunicação com outros órgãos federais. Possui infraestrutura robusta, segurança e ambientes de desenvolvimento e homologação. Porém, mesmo contando com um cenário aparentemente desfavorável a falhas, a alta gestão de TI precisa implementar ações e cultura de continuidade de negócio em seus sistemas críticos.

O levantamento realizado dos ativos primários e de apoio identificam pontos de atenção na infraestrutura que suporta o sistema SEI. Eventos críticos podem ocorrer mesmo em ambientes seguros de tecnologia causando indisponibilidade de sistema. Foram identificados eventos criticos recorrentes que precisam ser documentados e tratados. Realizar o estudo de riscos, suas possíveis consequências e as formas de tratar esses riscos é importante para qualquer sistema a ser disponibilizado aos usuários. Com as informações coletadas foi possível identificar a necessidade na redundância de equipamentos, porém, sabe-se que nem sempre é possível este ambiente ideal. Desta forma, ter o levantamento de ações de contingência se torna ainda mais fundamental para a disponibilidade do sistema.

Ter um sistema de continuidade melhora a confiabilidade do sistema e auxilia na disponibilidade do sistema para a comunidade. A gestão de continuidade de negócios aplicado ao sistema SEI prepara o ambiente para possíveis indisponibilidade. Porém, durante esta pesquisa percebeu-se que a elaboração de um SGCN é muito complexa, necessita de conhecimento aprofundado do negócio, da organização como um todo, do entendimento do ambiente, dos processos críticos, e dos recursos a serem aplicados, além da vontade da instituição em desenvolver um plano de continuidade de negócios.

Percebe-se também que a gestão de risco tem importante papel na elaboração de um SGCN, pois com ela, a instituição entende melhor os riscos que permeiam o ambiente e pode se proteger de forma pró-ativa. Durante a identificação e análise dos riscos levanta-

dos, percebeu-se que os riscos de ataque externo, problemas de hardware, problemas de equipamento de conexão e falta de energia possuem alto impacto para o negócio e podem ser tratados com planos de continuidade e planejamento de contingência. Porém, para que esse sistema seja efetivo é necessário o empenho da alta gestão em dar importância a cultura de continuidade de negócios não apenas para o sistema SEI, mas para todos os sistemas críticos disponibilizados pela STI.

A cultura de continuidade de negócios deve ter passos a serem implementados desde o inicio da implementação do sistema e perpetua-se durante sua disponibilidade aos usuários. A Secretaria já implementa testes de validação do sistema SEI em todas as etapas, assim como, possui planos de recuperação para casos de desastres extremos do sistema, porém estes processos precisam estar documentados e prontos para serem utilizados em momentos de crise. Entende-se que o sistema SEI não é o único sistema crítico ofertado pela Secretaria e que essa pesquisa de mestrado pode ser o primeiro passo a ser tomado pela Secretaria para implementação da cultura de continuidade de negócios para os sistemas críticos ofertados.

Desta forma, foi possível desenvolver um comparativo com as normas utilizadas nesta pesquisa e o atual cenário de sustentação do sistema SEI na STI, sendo possível chegar a tabela 4.7 abaixo onde são argumentados o benefício da norma, os processos utilizados pela Secretaria e processos que podem ser utilizados para adequação a norma.

Norma	**Benefício da norma**	**Processos da norma utilizados**	**Processos que podem ser implementados de acordo com a norma**

ISO 22301	Auxiliar na diminuição de efeitos de possíveis paralisações adotando atitudes proativa para minimizar o impacto de incidentes mantendo funções críticas em funcionamento durante períodos de crise e contribui para recuperação de dados e sistemas dentro de curso espaço de tempo elevando o nível de confiança dos serviços prestados	Política de backup. Documentações técnicas, Monitoramento de eventos. Definição de pessoas com responsabilidade. Participação da alta gestão.	Levantamento e análise de riscos envolvendo o ambiente de sustentação do sistema SEI. Elaborar planos de continuidade de negócio e recuperação de desastres, assim como a política de continuidade de negócios da STI. Levantamento de ativos. Definir prioridades e estratégias de continuidade de negócios de continuidade de negócios e recuperação para o sistema SEI, assim como a Análise de Impactos em caso de indisponibilidade do serviço. Implementar a cultura de continuidade de negócios a serviços críticos ou serviços ofertados pela STI a comunidade acadêmica.
ISO 31000	Proteger o valor das organizações, gerenciando riscos, tomando decisões, estabelecendo e alcançando objetivos e melhorando o desempenho.	Atribuição de papeis e responsabilidades. Busca de melhoria continua de serviços e sistemas	Desenvolver gestão de risco a cerca de sistemas e serviços de tecnologia. Articular o comprometimento com a gestão de riscos da STI. Implementar processos de identificação, avaliação e tratamento de riscos.

ISO 27005	Processo de gestão de riscos de segurança da informação de uma organização	Equipe específica de tratamento de eventos de segurança da informação, Monitoramento e análise de eventos de segurança da informação, Norma de segurança da Informação	Definir nível de risco e probabilidade de eventos de TI, assim como risco residual relacionados ao sistema SEI. Definir níveis de riscos aceitáveis e análise crítica de riscos relacionados ao SEI. Implementar processo de SGSI relacionado ao SEI. Identificação de ameaças e vulnerabilidades que possam comprometer o sistema SEI. Identificação de controles e consequências para tratamento de riscos. Determinar níveis de riscos identificados. Realizar monitoramento e análise crítica de riscos.
POSIC	Política que tem o propósito de limitar a exposição ao risco a níveis que garantam a disponibilidade, integridade, confidencialidade e a autenticidade das informações no âmbito da Universidade	Equipe definida de ETIR. Resiliência de sistemas, sendo todos pensados a resistir e recuperar-se dos efeitos de desastres. Auditabilidade de sistemas. Controle de acesso físico. Gestão de riscos em contratações de TIC. Plano de contingência. Proteção de ativos de informação.	Gestão de Riscos relacionados a sustentação do sistema SEI. Gestão de Ativos de informação e suporte ao sistema SEI. Gestão de incidentes, assim como o plano de gestão de incidentes. Gestão de Continuidade e conformidade levando em consideração normas, procedimentos e controles relacionados a continuidade de negócios.

Tabela 4.7: Compatibilidades de normas com atual cenário

Como mostra a tabela 4.7 existem processos que podem auxiliar a STI na mitigação de riscos e melhoria da continuidade de negócio aprimorando e incluindo processos no atual ambiente de sustentação do sistema SEI. Estes processos podem servir como apoio em momentos de crise e contribuir para a restauração do sistema a nível funcional no menor tempo possível de indisponibilidade. Para tanto, é necessário que estruture equipes de gestão de riscos e continuidade de negócios que possam, não apenas identificar mas elaborar planos que contribuam para a resiliência do sistema.

Capítulo 5

CONCLUSÕES

O ciclo de gestão de riscos apresentado nesta pesquisa favorece a estruturação de um Sistema de Gestão de Continuidade de Negócios - SGCN aplicado ao Sistema Eletrônico de Informações - SEI utilizado na UnB.

A questão de pesquisa enunciada no inicio desta pesquisa foi respondida demonstrando a importância da implementação de um SGCN aplicado ao sistema SEI proporcionando resiliência através de ações proativas de levantamento de riscos, análise de ameaças e tratamento de incidentes. Foi possível validar a aplicabilidade da implementação de um SGCN que é composto pelos planos de contingência, administração de crises, recuperação de desastres e continuidade operacional. Nessa pesquisa, foi realizado o ciclo de gestão de riscos relacionados a sustentação do sistema SEI, ao final deste ciclo, se algum risco identificado ou não ocorrer, mesmo com probabilidade baixa é possível acionar um plano de continuidade de negócios. Desta forma, foi possível identificar e validar que a cultura de continuidade de negócios deve ter passos a serem implementados desde o início da implementação do sistema e perpetua-se durante sua disponibilidade aos usuários.

Para tanto, a pesquisa baseou-se na análise de riscos e ameaças envolvidas na sustentação do sistema com expectativa de contribuir com a instituição de ensino, apresentando um estudo que visa mitigar falhas e incidentes bem como atenuar o impacto relacionado a eventuais indisponibilidades do sistema SEI.

Através desta pesquisa foi possível compreender os conceitos envolvidos no ciclo de gestão de riscos e um SGCN com conhecimentos advindos de normativos relacionados a gestão de risco e continuidade de negócio e conclusões de pesquisadores das áreas de ciência da computação, gerenciamento e negócios. Assim, com base nos conhecimentos obtidos, elaborar um plano de ação para desenvolver este estudo.

Os normativos e literaturas consultadas demonstram a importância do levantamento de riscos e gestão de continuidade de negócios para serviços críticos. Através da busca de conhecimento da instituição, foi possível analisar documentações técnicas, realizar

entrevistas com pessoas ligadas diretamente com a sustentação do sistema e coletar dados de sistemas de monitoramento e ativos de informação. Desta forma, após analisar as informações coletadas, foi possível concluir que é viável a implementação de um SGCN para mitigar riscos operacionais na sustentação do sistema SEI utilizado na UnB.

Por se tratar de um ambiente complexo e com várias fontes de informação, foi necessário buscar documentos técnicos relacionados ao ambiente de infraestrutura do sistema, assim como manuais de implementação. As reuniões com pessoas que trabalham na sustentação do sistema foram importantes, pois contribuirão com informações não documentadas e entendimento do ambiente. Foi possível identificar documentos técnicos relacionados a particularidade do ambiente de TI da UnB e formas de tratamento de incidentes envolvendo o sistema, assim como a preocupação que a instituição tem com a segurança das informações armazenadas no SEI.

O levantamento de ativos primários e suporte ao sistema evidenciaram a criticidade e a complexabilidade de sua infraestrutura de sustentação. Neste levantamento é possível identificar pontos críticos na análise de risco relacionados a disponibilidade do sistema e que são absorvidos pela STI com o intuito de mitigar eventuais eventos de indisponibilidade.

Em função da criticidade do sistema de pesquisa limitou-se a não divulgação de versão de sistemas operacionais, segmentações de rede, regras de firewall, versões de software ou qualquer outra configuração que possa comprometer a segurança do sistema ou sua infraestrutura.

Foi possível realizar coleta de dados de sistemas de monitoramento relacionados a eventos de hardware, software, rede ou segurança que possam causar indisponibilidade do sistema. Nesta análise ficou claro que grande parte dos eventos ocorridos no sistema estão relacionados a manutenção do sistema ou eventos de hardware que não necessariamente causam indisponibilidade do sistema, porém precisam ser analisados como forma de melhoria continua. Para tanto, foi demonstrado que durante o período de pesquisa o sistema SEI manteve os acordos de nível de serviços acordados em 99,92%, desta forma, respeitando os prazos estabelecidos com a STI.

A análise de riscos das ameaças e vulnerabilidades encontradas foi realizada utilizando a matriz de probabilidade e impacto utilizada na STI, obedecendo as etapas de identificação, análise, avaliação e tratamento de riscos. Nestas etapas foram analisados 11 riscos levantados, assim como as ações de controle e contingencia realizadas atualmente pela equipe de sustentação em caso de evento de indisponibilidade do sistema.

Foi possível identificar que o levantamento de riscos e gestão de continuidade de negócio podem ser positivos no contexto de melhoria continua do sistema, resiliência de infraestrutura operacional e disponibilidade.

Na elaboração desta pesquisa, entende-se que o processo de elaboração de um SGCN é complexo e desafiador e precisa está alinhado com diversos fatores institucionais. Porém, com o advento de novas tecnologias e com a implementação de novas formas de acesso e proteção a dados e informações, principalmente nos últimos anos com o crescimento de tecnologias e armazenamento de dados em instituições públicas, é essencial que estes órgãos e empresas elaborem planos preventivos que contribuam com a resiliência e com a disponibilidade de serviços e sistemas.

Apesar desta pesquisa ser delimitada apenas em relação ao sistema SEI, a cultura organizacional da Secretaria pode utilizar a continuidade de negócios e gestão de riscos para todos os serviços ofertados, não limitando-se apenas a serviços críticos ou essenciais ao funcionamento da instituição mas também a processos e sistemas internos e ou futuros a serem implementados.

A POSIC da UnB diz que a Secretaria precisa implementar procedimentos e controles que estabeleçam a continuidade de negócios e que esses controles minimizem os impactos decorrentes de eventos que causem indisponibilidade, assim como criar e manter equipes de tratamento de incidentes. A mesma política, em relação a gestão de riscos, diz que "a STI precisa estabelecer metodologias que possibilite a identificação, a quantificação, a priorização, o tratamento, a comunicação e a monitoração periódica dos riscos"[33]. Então, entende-se que para se adequar a essa norma e outras normas institucionais, a STI pode utilizar um SGCN para os seus serviços críticos.

Em conclusão, esta pesquisa levanta pontos que podem ser utilizados na implementação de processos que visem a continuidade de negócios e gerenciamento de risco na disponibilidade do sistema SEI. Este sistema que esta no rol de serviços críticos suportados pela Secretaria é de grande importância para a instituição de ensino e precisa ter sua infraestrutura de TI disponível, mesmo em casos de eventos extremos. Desenvolver planejamentos de contingência auxiliam na resiliência do sistema em casos de eventos de indisponibilidade. Os esforços para tratar eventos de forma reativa não podem ser superiores aos esforços no tratamento de eventos de forma pró-ativa. A aplicabilidade de SGCN precisa estar alinhada com um ciclo de gestão de riscos. Os riscos envolvidos na prestação deste serviço a comunidade acadêmica precisam ser levantados e tratados e que, em caso de indisponibilidade, existam processos definidos que possam ser seguidos para retornar o serviço para produção no menor tempo de indisponibilidade possível.

5.1 Trabalhos futuros

Esta pesquisa traz oportunidades de trabalhos futuros a serem explorados pela área de tecnologia da UnB.

O aumento do interesse na aplicação de gestão de riscos e continuidade de negócios após a pandemia de covid-19 é visto como uma oportunidade para melhorar serviços e gerir disponibilidade de sistemas. Expandir a cultura de gestão de riscos e planejamentos relacionados a continuidade de negócio não apenas para os serviços críticos, partindo para uma visão parcial ou total do catalogo de serviços ofertados para a comunidade. A possibilidade de implementar essa iniciativa para outros serviços críticos, seria uma oportunidade para permitir a continuidade deste estudo, promovendo possíveis melhorias nos processos de gestão de tecnologia e podendo servir como modelo a ser implementado em outras instituições de ensino superior.

Referências

[1] UNIVERSIDADE DE BRASÍLIA: *Missão Universidade de Brasília*, 2021. `https://unb.br/a-unb/missao`, acesso em 2021-10-28. 2

[2] RIBEIRO, DARCY: *UnB, invenção e descaminho*, volume 3. Avenir Editora, 1978. 2

[3] SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO DA UNB: *Secretaria de tecnologia da informação*. `https://sti.unb.br`. Acesso em 28-10-2021. 2

[4] UNIVERSIDADE DE BRASÍLIA: *Anuário estátistico unb 2019*. `http://www.dpo.unb.br/index.php?option=com_content&view=article&id=60&Itemid=896`, 2019. Accessed: 21-05-2021. 2

[5] UNIVERSIDADE DE BRASÍLIA: *Plano diretor de tecnologia da informação e comunicação 2019-2022*. `https://unb.br/images/Noticias/2019/Documentos/PDTIC_2019_2022.pdf`. Acesso em 29-10-2021. 3, 43

[6] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS: *Iso:27005 gestão de riscos de segurança da informação*. Iso, International Organization for Standardization, 2019. 4, 15, 16, 17, 18, 19, 20, 56, 57, 58, 60

[7] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS: *Iso:15999-1 gestão de continuidade de negócios parte 1 - código de prática*. Iso, International Organization for Standardization, 2007. 7, 9

[8] BAJGORIC, NIJAZ: *Business continuity management: a systemic framework for implementation*. Kybernetes, 2014. 7

[9] IQBAL, AMIRUL, WIDYAWAN e I WAYAN MUSTIKA: *Cobit 5 domain delivery, service and support mapping for business continuity plan*. Em *AIP Conference Proceedings*, volume 1746, página 020045. AIP Publishing LLC, 2016. 8

[10] GRAHAM, JULIA e DAVID KAYE: *A risk management approach to business continuity: Aligning business continuity and corporate governance*. Rothstein Publishing, 2015. 8

[11] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS: *Iso:22301 sistema de gestão de continuidade de negócios - requisitos*. Iso, International Organization for Standardization, 2013. 9, 10, 11

[12] BURBY, RAYMOND J: *Making plans that matter: Citizen involvement and government action*. Journal of the American Planning Association, 69(1):33–49, 2003. 10

[13] MILETI, DENNIS: *Disasters by design: A reassessment of natural hazards in the United States*. Joseph Henry Press, 1999. 10

[14] ENGEMANN, KURT J, HOLMES E MILLER e RONALD R YAGER: *Disaster management of information resources using fuzzy and attitudinal modelling*. International Journal of Technology, Policy and Management, 5(4):388–406, 2005. 10

[15] MANUELE, FRED A: *Acceptable risk: Time for sh&e professionals to adopt the concept*. Professional safety, 55(05):30–38, 2010. 10

[16] MOORE, BETHANY e ERIC A BONE: *Decision-making in crisis: Applying a healthcare triage methodology to business continuity management*. Journal of business continuity & emergency planning, 11(1):21–26, 2017. 10

[17] FERNANDO, MAHENDRA SAGARA: *It disaster recovery system to ensure the business continuity of an organization*. Em *2017 National Information Technology Conference (NITC)*, páginas 46–48. IEEE, 2017. 11

[18] UNIVERSIDADE DE BRASÍLIA: *Guia de gestão de riscos unb*. `http://dpo.unb.br/images/phocadownload/gestaoriscosintegridade/Guia_de_gest~ao_de_riscos_UnB_07.02.20.pdf`. Acesso em 29-10-2021. 12, 13, 16, 44, 45, 46

[19] FERREIRA, ALBERTINA DA CUNHA COUTO: *A gestão de risco aplicada à auditoria interna*. Universidade de Aveiro, Mestrado em Contabilidade e Auditoria, 2010. 12

[20] FORÇA AÉREA BRASILEIRA: *Manual de metodologia de gestão de riscos em segurança da informação do centro de computação da aeronáutica de brasília*. 2019. 12

[21] TRIBUNAL DE CONTAS DA UNIÃO: *Manual de gestão de riscos do TCU*. 2018. 12

[22] WILDAVSKY, AARON: *Views: No risk is the highest risk of all: A leading political scientist postulates that an overcautious attitude toward new technological developments may paralyze scientific endeavor and end up leaving us less safe than we were before*. American scientist, 67(1):32–37, 1979. 13

[23] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS: *Iso:31000 gestão de riscos - diretrizes*. Iso, International Organization for Standardization, 2018. 13, 16, 42, 43, 63, 65, 66

[24] THEMSEN, TIM NEERUP e PETER SKæRBæK: *The performativity of risk management frameworks and technologies: The translation of uncertainties into pure and impure risks*. Accounting, Organizations and Society, 67:20–33, 2018. 13

[25] DE CICCO, FRANCESCO: *Gestão de riscos-Diretrizes para a implementação da ISO 31000: 2018*. Risk Tecnologia Editora Ltda, 2018. 13

[26] FABRA, MGMC: *Gerenciamento de riscos em projetos de implantação de sistemas erp*, 2006. 15

[27] FERNANDES, JORGE HENRIQUE CABRAL: *Introdução à gestão de riscos de segurança da informação*. Brasília: UNB, 2009. 15

[28] TRIBUNAL DE CONTAS DA UNIÃO - TCU: *Referencial básico de gestão de riscos*. `https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/outros-documentos-externos/tcu_referencial_gestao_riscos.pdf`. Acesso em 2021-11-19. 15

[29] LOPES, ARTUR CESAR SARTORI LOPES: *Gestão de risco: a importância da resiliência em eventos indesejáveis*. Tese de Doutoramento, 2016. 16

[30] INSTITUTO NACIONAL DE PROPRIEDADE NACIONAL: *Manual de gestão de risco do inpi*. `https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2020/01/manual-de-gestao-de-riscos-do-inpi.pdf`, acesso em 2021-11-19. 16, 17

[31] ADRIANA, BEAL: *Segurança da informação: princípios e as melhores práticas para a proteção dos ativos de informações nas organizações*. São Paulo: Atlas, 2008. 18

[32] CÔRTE, KELSON: *Segurança da informação baseada no valor da informação e nos pilares tecnologia, pessoas e processos. 2014. 212 f., il.* Tese de Doutoramento, Tese (Doutorado em Ciência da Informação)—Universidade de Brasília, Brasília, 2014. 18

[33] Universidade de Brasília: *Política de segurança da informação e comunicação da Universidade de Brasília 0 PoSIC/UNB*. 2019. Acesso em 07-02-2022. 19, 24, 69, 77

[34] MACH, ERNST: *The Science of Mechanics: A Critical and Historical Account of Its Development. Supplement*. Open court publishing Company, 1915. 20

[35] ROHLEDER, THOMAS R e EDWARD A SILVER: *A tutorial on business process improvement*. Journal of Operations Management, 15(2):139–154, 1997. 21

[36] DE ALMEIDA, JOÃO FERREIRA, JOSÉ MADUREIRA PINTO e MARIA EDUARDA CRUZEIRO: *A propósito do problema da causalidade em ciências sociais: o modelo de decomposição de proporções de r. boudon*. Análise social, páginas 734–777, 1973. 21

[37] LINETE, BARTALO e MORENO NADIA APARECIDA: *Gestão em arquivologia: Abordagens múltiplas*. Londrina: Eduel, página 188 p., 2008. 21

[38] JARDIM, JOSÉ MARIA: *O conceito e a prática de gestão de documentos*. Acervo, 2(2):35–42, 1987. 21

[39] NASCIMENTO, PAULO ROBERTO DA SILVA: *Impactos da implantação do sistema eletrônico de informação (sei): estudo de caso da universidade de brasília*. 2017. 22

[40] ESTEVES, RUI: *Implementação do processo gestão da configuração da framework ITIL–um estudo de caso*. Tese de Doutoramento, Instituto Politécnico de Bragança, Escola Superior de Tecnologia e Gestão, 2012. 23

[41] POTGIETER, BC, JH BOTHA e C LEW: *Evidence that use of the itil framework is effective*. Em *18th Annual conference of the national advisory committee on computing qualifications, Tauranga, NZ*. Citeseer, 2005. 24

[42] CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES NO BRASIL: *Gerenciamento de incidentes cert.br*. `https://www.cert.br/docs/certbr-faq.html#6`. Acesso em 2021-11-16. 24

[43] ADAMS, SIMON: *ITIL V3 foundation handbook*. The Stationery Office, 2009. 24, 25

[44] KIM, GENE, KEVIN BEHR e GEORGE SPAFFORD: *The visible ops handbook: Starting itil in 4 practical steps*. Information Technology Process Institute, 2004. 24

[45] RUDD, COLIN: *ITIL® V3 guide to software asset management*. TSO, 2009. 25

[46] BENICIO, WASHINGTON ERNANDO PEREIRA: *Monitoramento e gerenciamento de redes utilizando zabbix*. Trabalho apresentado ao Curso de Análise e Desenvolvimento de Sistemas do Instituto Federal como requisito para obtenção do título de Tecnólogo em Análise e Desenvolvimento de Sistemas, 2015. 25

[47] MARIANO, ARI MELO e M ROCHA SANTOS: *Revisão da literatura: Apresentação de uma abordagem integradora structural equations view project service quality view project*. Em *XXVI Congreso Internacional de la Academia Europea de Dirección y Economía de la Empresa (AEDEM), n. September, pv*, volume 26, 2017. 26, 31

[48] BIBLIOTECA CENTRAL - UNB: *Conheça a web of science - bce*. `https://bce.unb.br/2018/06/conheca-a-web-of-science/`. Acesso em 2021-11-19. 27

[49] LINDSTRÖM, JOHN, SÖREN SAMUELSSON e ANN HÄGERFORS: *Business continuity planning methodology*. Disaster Prevention and Management: An International Journal, 2010. 30

[50] MILLER, HOLMES E e KURT J ENGEMANN: *Business continuity management in data center environments*. International Journal of Information Technologies and Systems Approach (IJITSA), 12(1):52–72, 2019. 30, 31

[51] ALHAZMI, OMAR H e YASHWANT K MALAIYA: *Assessing disaster recovery alternatives: On-site, colocation or cloud*. Em *2012 IEEE 23rd International Symposium on Software Reliability Engineering Workshops*, páginas 19–20. IEEE, 2012. 31

[52] SETIAWAN, ALEXANDER, ADI WIBOWO e ADREW HARTANTO SUSILO: *Risk analysis on the development of a business continuity plan*. Em *2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT)*, páginas 1–4. IEEE, 2017. 31

[53] AVEN, TERJE: *Risk assessment and risk management: Review of recent advances on their foundation*. European Journal of Operational Research, 253(1):1–13, 2016. 32

[54] MARCONI, MARINA DE ANDRADE e EVA MARIA LAKATOS: *Fundamentos de metodologia científica*. 5. ed.-São Paulo: Atlas, 2003. 33

[55] DEMO, PEDRO: *Metodologia científica em ciências sociais*. 1995. 33

[56] SANTOS, ORLANDO OLIVEIRA DOS: *Metodologia de diagnóstico e análise de desempenho de processos (mdadp): estudo de caso sobre o processo de atendimento de serviços de ti*. 2016. 33

[57] VERGARA, SYLVIA CONSTANT: *Projetos e relatórios de pesquisa*. São Paulo: Atlas, 2006. 34, 38

[58] GIL, ANTONIO CARLOS: *Métodos e técnicas de pesquisa social. são paulo: Atlas, 2008. gomes, nl a contribuição dos negros para o pensamento educacional brasileiro*. SILVA, Petronilha BG e & BARBOSA M. de Assunção (org.). O Pensamento negro em educação no Brasil: expressões do movimento negro. São Paulo, UFSCar, 19. 34

[59] GIL, ANTÓNIO CARLOS: *Métodos e técnicas de pesquisa social*. 2008. 34

[60] LEHFELD, NEIDE APARECIDA DE SOUZA e AIDIL DE JESUS PAES BARROS: *Projeto de pesquisa: propostas metodológicas*. Petrópolis/RJ: Vozes, 1991. 34

[61] EISENHARDT, KATHLEEN M: *Building theories from case study research*. Academy of management review, 14(4):532–550, 1989. 34

[62] KUMAR, R e R MALHOTRA: *Case study research: Design and methods*, 2011. 34

[63] Yin, Robert K: *Estudo de Caso-: Planejamento e métodos*. Bookman editora, 2015. 35

[64] CASTRO, CLÁUDIO DE MOURA: *Estrutura e apresentação de publicações científicas*, 1976. 38

[65] SENADO FEDERAL: *Criação da fundação universidade de brasília*. `https://noticias.unb.br/images/Noticias/2017/Documentos/lei_3998-61_criacao_fub.pdf`. Acesso em 07-02-2022. 41

[66] SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO DA UNB: *Historia da secretaria de tecnologia da informação - sti da universidade de brasília*. `https://sti.unb.br/index.php/sti-institucional/historia-da-sti`. Acesso em 18-11-2021. 41

[67] DECANO DE PLANEJAMENTO, ORÇAMENTO E AVALIAÇÃO INSTITUCIONAL - DPO: *Anuário estatístico unb 2020*. `https://anuario-estatistico-unb-2020.netlify.app/index.html`. Acesso em 18-11-2021. 42

[68] BRASÍLIA, UNIVERSIDADE DE: *Estatuto e regimento geral universidade de brasília*. https://unb.br/images/Noticias/2016/Documentos/regimento_estatuto_unb.pdf. Acesso em 18-11-2021. 42

[69] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS: *Guia 73 - gestão de riscos - vocabulário - recomendações para uso em normas*, 2009. 43

[70] FEDERAL, MINISTÉRIO DA ECONOMIA GOVERNO: *Documentação sei governo federal*. https://www.gov.br/economia/pt-br/assuntos/processo-eletronico-nacional/servicos/documentacao. Acesso em 02-12-2021. 59

[71] Brasília, Fundação Universidade de: *Guia prático para usuários do sistema sei unb*. http://www.unbdigital.unb.br/index.php?option=com_content&view=article&id=480:guia-pratico-do-sei-na-unb&catid=2&Itemid=162. Acesso em 02-12-2021. 59

[72] SILVA, MARCELO GASPAR RODRIGUES, TAMP GOMEZ e ZAILTON CARDOSO DE MIRANDA: *Ti: mudar e inovar: resolvendo conflitos com itil v3 aplicado a um estudo de caso*. Brasília: Senac DF, 2010. 60

[73] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS: *Iso:17799 tecnologia da informação - código de prática para gestão de segurança da informação*. Iso, International Organization for Standardization, 2001. 60

[74] LAUDON, KENNETH C e JANE P LAUDON: *Sistemas de informação gerenciais. 5ª edição*, 2004. 60

Apêndice A

Identificação de Normas e manuais utilizados na pesquisa

A tabela A.1 abaixo reflete as normas, políticas e manuais pesquisados para auxiliar no contexto de elaboração dessa pesquisa.

Norma	**Origem**	**Descrição**
ISO 31000	Gestão de Riscos	Norma internacional para gestão de riscos que fornece as diretrizes para desenvolvimento do processo de gerenciamento de riscos nas empresas, atuando como um recurso importante do planejamento estratégico
ISO 27005	Gestão de segurança da informação	Define o processo de gestão de risco como atividades coordenadas para dirigir e controlar o risco de uma organização
ISO 22301	Gestão de continuidade de negócios	A norma do sistema de gerenciamento de continuidade de negócios ISO 22301 fornece as melhores práticas internacionais que ajudam você a responder e se recuperar de forma eficaz de interrupções.
ISO 15999-1	Gestão de continuidade de negócios. Parte 1 - Código de prática	Fornece sistema baseado em boas práticas de gestão de continuidade de negócios, fornecendo informações para entender, desenvolver e implementar a continuidade de negócio em uma organização.

Guia UnB	Guia de Gestão de riscos da Universidade de Brasília	Apresentação a estrutura e a metodologia de gestão de riscos da Universidade de Brasília, ressaltando o processo de implantação, aprendizagem e melhoria contínua, adequando a melhores práticas utilizadas no governo federal
Manual TCU	Manual de gestão de riscos do TCU	Gestão de riscos é um dos mais importantes instrumentos de aperfeiçoamento e está intimamente associada ao princípio constitucional da eficiência.
Manual INPI	Manual de gestão de riscos do INPI	O modelo de gestão de riscos do INPI tem como premissa básica a avaliação de riscos dentro dos processos organizacionais, e está apoiado em diretrizes da norma ABNT NBR ISO 31000:2009
POSic	Política de segurança da informação e comunicação da UnB	A PoSIC tem por objetivo instituir princípios e diretrizes de Segurança da Informação e Comunicações - SIC no âmbito da Universidade de Brasília- UnB, com o propósito de limitar a exposição ao risco a níveis que garantam a disponibilidade, a integridade, a confidencialidade e a autencidade das informações e comunicações que suportam os objetivos estratégicos e as atividades precípuas de ensino, pesquisa e extensão desta Universidade

Tabela A.1: Identificação de normas de gestão de risco e continuidade de negócios utilizadas na pesquisa

Apêndice B

Levantamento de ativos críticos de sustentação ao sistema SEI

Este apêndice reflete o levantamento dos ativos primários e de suporte relacionados a sustentação do sistema SEI na UnB.

Cada ativo levantado encontra-se na sala cofre localizado no prédio da STI, o qual para acesso, precisa-se de acesso ao prédio da STI, abertura de chamado junto a empresa terceiro e acesso biométrico de acesso a sala cofre.

As siglas referente aos responsáveis pelos ativos estão listados abaixo:

- DDC - Divisão de Data Center
- CSE - Coordenação de Serviços Especializados
- CSI - Coordenadoria de Segurança da Informação
- CRI - Coordenadoria de Redes e Infraestrutura

As figuras B.1, B.2, B.3 e B.4 demonstra a prioridade do ativo e seu responsável.

Atualmente a guarda, manutenção e monitoramento da sala cofre é de responsabilidade da Divisão de Data Center. O controle de acesso é feito pela empresa parceira CentralIT, que também participa do monitoramento dos equipamentos e serviços disponibilizados pela STI.

UnB	**Tipo do Doc.** **Documento interno de criticidade de ativos**	**Doc. Nº 01**	**Revisão 01**
	Data Emissão **10/12/2021**	**Data Vigência** **Indefinida**	**Página 01**
	Lista de ativos de informação priorizados sistema SEI **Sistema eletrônico de informações - SEI da Universidade de Brasília**		

Compilado por: Cristiano Magno de Morais

Data: 5/12/2021

Ativo: Sistema Eletrônico de Informações - SEI

Dono do serviço: Grupo Gestor do Sistema SEI

Responsável técnico suporte: Coordenação de serviços especializados - CSE

Contato imediato: 61 3107-0000

Analisado por: Chefe do setor de redes

Analisado por: Chefe da divisão de Serviços especializados

Analisado por: Chefe do setor de segurança

Analisado por: Chefe da divisão de Data Center - DDC

Localização	Código Área/Diretoria	Prioridade	Descrição (nome) do ativo	Tipo	Ameaças
Sala cofre	DDC	Alta	Blade G4	Equipamento critíco	Falta de energia, mal funcionamento de peças e conexões de rede, mal configuração, superaquecimento
Sala cofre	DDC	Alta	Storage	Equipamento critíco	Falta de energia, mal funcionamento de peças e conexões de rede, mal configuração, superaquecimento, falta de espaço de armazenamento, furto de informações, vulnerabilidades de sistema
Sala cofre	CSE	Alta	Backup	Equipamento critíco	Falta de energia, mal funcionamento de peças e conexões de rede, falha em robô de backup, falha no sistema de backup, falha de sistema operacional, erro de configuração, falta de fita magnética, furto de informações, ataques externos, ataques internos, fim do suporte com o fabricante, falha de conexão com storage
Sala cofre	CSI	Alta	Firewall	Equipamento critíco	Falta de energia, erro de configuração, falha de rede, ataque externo ou interno, falha de comunicação com o provedor de internet, vulnerabilidade de software
Sala cofre	Redes	Alta	Switch	Equipamento critíco	Falta de energia, erro de configuração, ataque externo ou interno, falha na comunicação de rede, furto de equipamento, equipamento danificado
Sala cofre	DDC	Alta	Sala cofre	Local do equipamento/serviço	Acesso indevido, falta de energia, falha no sistema de refrigeração, falha no sistema de acesso, superaquecimento, falha no sistema de cameras, falha nas conexões de rede, alagamento, queimadas, desmoronamento, falha nas baterias de energia, falha no sistema antifogo, travamento da porta, furto de informações

	Revisão 01	**Doc. Nº 01**	**Documento interno de ativos críticos**
	Data Emissão 10/12/2021	**Data Vigência Indefinida**	**Página 01**
	Lista de ativos de informação priorizados sistema SEI **Sistema eletrônico de informações - SEI da Universidade de Brasília**		

Compilado por: Cristiano Magno de Morais

Data: 5/12/2021

Ativo: Sistema Eletrônico de Informações - SEI

Dono do serviço: Grupo Gestor do Sistema SEI

Responsável técnico suporte: Coordenação de serviços especializados - CSE

Contato imediato: 61 3107-0000

Analisado por: Chefe do setor de redes

Analisado por: Chefe da divisão de Serviços especializados

Analisado por: Chefe do setor de segurança

Analisado por: Chefe da divisão de Data Center - DDC

Equipamento	Ameaças	Controle	Ação
Blade G4	Falta de energia, mal funcionamento de peças e conexões de rede, mal configuração, superaquecimento	Gerador de energia, redundância de baterias, contrato com fabricante do produto para suporte, gerenciamento de acesso e logs, controle de eventos	Mitigar
Storage	Falta de energia, mal funcionamento de peças e conexões de rede, mal configuração, superaquecimento, falta de espaço de armazenamento, furto de informações, vulnerabilidades de sistema	Gerador de energia, redundância de baterias, contrato com fabricante do produto para suporte, gerenciamento de eventos, controle de acesso	Mitigar
Backup	Falta de energia, mal funcionamento de peças e conexões de rede, falha em robô de backup, falha no sistema de backup, falha de sistema operacional, erro de configuração, falta de fita magnética, furto de informações, ataques externos, ataques	Gerador de energia, redundância de baterias,contrato com fabricante do produto, redundância de robos de backup, controle de acesso e guarda de fitas magnéticas, controle de acesso e eventos de sistema	Mitigar
Firewall	Falta de energia, erro de configuração, falha de rede, ataque externo ou interno, falha de comunicação com o provedor de internet, vulnerabilidade de software	Gerador de energia, redundância de baterias, controle de acesso e eventos, controle de versões e regras, redundância de link de internet, atualização de sistema, analise de regras	Mitigar
Switch	Falta de energia, erro de configuração, ataque externo ou interno, falha na comunicação de rede, furto de equipamento, equipamento danificado	Gerador de energia, redundância de baterias, controle de acesso e eventos, controle de versões e regras, redundância de equipamentos, controle de acesso a salas	Mitigar
Sala cofre	Acesso indevido, falta de energia, falha no sistema de refrigeração, falha no sistema de acesso, superaquecimento, falha no sistema de cameras, falha nas conexões de rede, alagamento, queimadas, desmoronamento, falha nas baterias de energia, falha no sistema antifogo, travamento da porta, furto de informações	Controle de acesso, Gerador de energia, redundância de baterias, controle de temperatura, contrato com empresa terceirizada, redundância de link, sala cofre certificada	Transferir/Compartilhar

	Tipo do Doc. Documento interno de criticidade de ativos	Doc. Nº 02	Revisão 01
UnB	Data Emissão 10/12/2021	Data Vigência Indefinida	Página 01
	Lista de ativos de informação priorizados sistema SEI		
	Ativos de informação do sistema SEI		

Compilado por: Cristiano Magno de Morais				
Data: 5/12/2021				
Ativo: Hardware de virtualização				
Dono do ativo: Divisão de Data Center - DDC				
Responsável técnico: Coordenador Divisão de Data Center - DDC				
Contato imediato: 61 3107-0000				
Localização	**Código Área/Diretoria**	**Prioridade**	**Descrição (nome) do ativo**	**Tipo**
Sala Cofre	DDC	Alta	Blade G4	Hardware Crítico
Sala cofre	DDC	Alta	Lâmina 03	Hardware Crítico
Sala Cofre	DDC	Alta	Lâmina 04	Hardware Crítico
Sala Cofre	DDC	Alta	Lâmina 05	Hardware Crítico

Figura B.1: Ativo físico - Servidor de armazenamento da aplicação
Fonte: Elaboração própria.

UnB	Tipo do Doc. Documento interno de criticidade de ativos	Doc. Nº 03	Revisão 01
	Data Emissão 10/12/2021	Data Vigência Indefinida	Página 01
	Lista de ativos de informação priorizados sistema SEI		
	Ativos de informação do sistema SEI		
Compilado por: Cristiano Magno de Morais			
Data: 5/12/2021			
Ativo: Hardware de armazenamento - STORAGE			
Dono do ativo: Divisão de Data Center - DDC			
Responsável técnico: Coordenador Divisão de Data Center - DDC			
Contato imediato: 61 3107-0000			

Localização	Código Área/Diretoria	Prioridade	Descrição (nome) do ativo	Tipo
Sala Cofre	DDC	Alta	Storage 01	Hardware Crítico
Sala cofre	DDC	Alta	Storage 02	Hardware Crítico
CEBRASPE	DDC	Alta	Storage 03	Hardware Crítico

Figura B.2: Ativo físico - Storage de armazenamento de informações
Fonte: Elaboração própria.

UnB	Tipo do Doc. Documento interno de criticidade de ativos	Doc. Nº 03	Revisão 01
	Data Emissão 10/12/2021	Data Vigência Indefinida	Página 01
	Lista de ativos de informação priorizados sistema SEI		
	Ativos de informação do sistema SEI		
Compilado por: Cristiano Magno de Morais			
Data: 5/12/2021			
Ativo: Hardware de armazenamento - Backup			
Dono do ativo: Divisão de Data Center - DDC			
Responsável técnico: Coordenador de serviços especiais - CSE			
Contato imediato: 61 3107-0000			

Localização	Código Área/Diretoria	Prioridade	Descrição (nome) do ativo	Tipo
Sala Cofre	DDC	Alta	Robô 01	Hardware Crítico
Sala cofre	DDC	Alta	Robô 02	Hardware Crítico
Sala Cofre	CSE	Alta	Sistema de Backup	Software
Sala Cofre	CSE	Alta	Robô 03	Hardware Crítico

Figura B.3: Ativo físico - Backup
Fonte: Elaboração própria.

UnB	Tipo do Doc. Documento interno de criticidade de ativos	Doc. Nº 03	Revisão 01
	Data Emissão 10/12/2021	Data Vigência Indefinida	Página 01
	Lista de ativos de informação priorizados sistema SEI		
	Ativos de informação do sistema SEI		
Compilado por: Cristiano Magno de Morais			
Data: 5/12/2021			
Ativo: Hardware de segurança - Firewall e redes			
Dono do ativo: Coordenação de segurança da informação - CSI			
Responsável técnico: Coordenador de segurança da informação - CSI			
Contato imediato: 61 3107-0000			

Localização	Código Área/Diretoria	Prioridade	Descrição (nome) do ativo	Tipo
Sala Cofre	CSI	Alta	Firewall 01	Hardware Crítico
Sala Cofre	CSI	Alta	Firewall 02	Hardware Crítico
Sala Cofre	CRI	Média	Swhitch	Hardware Crítico

Figura B.4: Ativo físico - Firewall e redes
Fonte: Elaboração própria.

Apêndice C

Análise de riscos levantados

Apêndice fornecendo a análise, avaliação e tratamento de riscos relacionados a sustentação do sistema SEI.

Na primeira imagem encontra-se a análise dos 11 riscos encontrados durante essa pesquisa. Foram levantadas as causas, consequências, probabilidade e impacto, tipo do risco, ações de controle, resposta ao risco e ações de contingenciamento relativo a cada risco. As figuras C.1 até C.11 estão relacionadas ao tratamento individual dos riscos identificados.

Risco	Causa	Consequência	Probabilidade	Impacto	Criticidade	Tipo de risco	Ações de controle	Resposta ao risco	Açoes de contingenciam
Acesso de pessoas não autorizadas a sala cofre	Acesso de pessoas não autorizadas dentro da sala cofre	Furto de informações, equipamentos danificados, furto de equipamentos, violação do sigilo de informações	Baixo	Alto	Média	Operacional	Verificar registro de acessos a sala cofre	Mitigar	A sala cofre possui monitoramento 24x7x365 e controle de acesso
Ataques externos	Ataques cibernéticos que causam danos ou roubo de informações dos serviços e tem como foco deixar os serviços indisponíveis	Violação do sigilo a informação,perda de dados e informações, indisponibilidade de sistemas, lentidão no acesso aos sistemas, indisponibilidade de dados, indisponibilidade de rede e telefonia, atraso no tramite de processos	Alto	Alto	Alta	Operacional	Verificar registros de log de equipamentos e eventos de sistema	Mitigar	Gerenciamento de eventos e redundância de equipamentos firewall. Equipe de tratamento de incidentes - ETIR
Ataques internos	Causados por usuários legítimosda rede, porém, tentando acessaralgum serviço ou equipamentopara deixa-lo indisponível	Violação do sigilo a informação,perda de dados e informações, indisponibilidade de sistemas, lentidão no acesso aos sistemas, indisponibilidade de dados, indisponibilidade de rede e telefonia, atraso no tramite de processos	Médio	Alto	Alta	Operacional	Verificar registros de log de equipamentos e eventos de sistema	Mitigar	Gerenciamento de eventos e redundância de equipamentos firewall.
Falha humana acidental ou imperícia	Causada pela falta de atenção dos usuáios ou técnicos	Indisponibilidade do sistema, indisponibilidade de ativos, lentidão no acesso a sistemas, perda de dados e informações, falhas de segurança de sistema, atraso na distribuição de processos no ambiente de desenvolvimento, indisponibilidade no sistema de homologação, indisponibilidade	Baixo	Baixo	Baixa	Operacional	Verificar registros de log de equipamentos e eventos de sistema	Mitigar	Capacitação, treinamento e controle de acesso à serviços e sistemas
Falta de energia elétrica	Causada por fator externo ou interno à rede elétrica do prédio ou de sua localidade com duração na interrupção superior a 3 horas	Indisponibilidade de sistemas, indisponibilidade de ativos, atraso na distribuição de processos, indisponibilidade de restauração do sistema	Médio	Alto	Alta	Operacional	Verificar registros de acionamento de gerador de energia e combustivel	Mitigar	Gerador de tanque interno com capacidade de fornecimento de 25 horas e tanque para funcionamento de 100 horas
Falha na migração e mudanças em aplicações virtuais	Causada na manipulação e instalação de atualizações que possam impactar nas disponibilidades do negócio	Indisponibilidade de sistema, indisponibilidade de informações, falhas na aplicação, falhas de rede, falhas operacionais de sistema	Muito Baixo	Muito Baixo	Muito Baixa	Operacional	Verificar registros de eventos relacionados a alterações de infraestrutura e sistema	Aceitar	Uso de máquina virtuais para migração e aplicação para movimentação ágil de máquinas virtuais
Indisponibilidade de equipamentos	Causado por equipamentos antigos ou equipamentos que por algum motivo precisem de reparo técnico	Indisponibilidade de sistema, indisponibilidade de dados e informações, falhas na distribuição de processos, falha na restauração do sistema	Médio	Alto	Alta	Operacional	Verificar registros de log de equipamentos e eventos de sistema	Mitigar	Contrato com fabricantes de equipamentos para suporte
Problema conexão	Causado principalmente por rompimentos de cabos de rede e fibra óptica ou por problemas de equipamentos de rede (Roteadores ou Switches)	Indisponibilidade do sistema, indisponibilidade de ativos, lentidão no acesso a sistemas, perda dedados e informações, falhas de segurança de sistema, atraso na distribuição de processos, falha na realização da restauração do sistema, perda de dados de backup	Médio	Alto	Alta	Operacional	Verificar registros de log de equipamentos e eventos de sistema	Mitigar	Gerenciamento de eventos e redundância de enlaces
Riscos na identificação de eventos	Causados por falta de pessoal para monitoramento dos eventos no serviço Zabbix	Tempo de solução de problemas elevado, falhas de equipamentos, falhas em conexão de rede, soluções reativas	Baixo	Baixo	Baixa	Operacional	Verificar resitros de responsabilidades e comunicações de incidentes	Eliminar	Contrato com empresa terceirizada para monitoramento de eventos
Risco Pessoal	Causados pela perda de capital humano técnico	Tempo de solução de problemas elevado, falhas de equipamentos, falhas em conexão de rede, soluções reativas, perda de conhecimento técnico, perda de credibilidade	Médio	Muito Baixo	Baixo	Operacional	Verificar escala de responsáveis e gestão de sistema	Aceitar	Plano de capacitação e apoio a educação continuada
Problemas sala cofre	Risco que pode comprometer a vida útil dos equipamentos, causanddo superaquecimento, imundação, incêndios e indisponibilidades	Indisponibilidade do sistema, indisponibilidade de ativos, lentidão no acesso a sistemas, perda de dados e informações, falhas de segurança de sistema, atraso na distribuição de processos, falha na realização da restauração do sistema, perda de dados de backup, tempo de solução de problemas elevado, falhas de equipamentos,falhas em conexão de rede, soluções reativas	Baixo	Alto	Média	Operacional	Verificar registro de eventos, acesso e controle	Mitigar	Sala certificada com manutenção em dia e redundância de climatização

Risco	Acesso à sala cofre	
Probabilidade	2	
Impacto	4	
Criticidade	8	
Tipo de tratamento de risco	Mitigar	
Dano 1	Furto de informações, equipamentos danificados, furto de equipamentos, violação do sigilo de informações	
Dano 2		
Dano 3		
ID	Ação Preventiva	Responsável
	Verificar registros de acesso a sala cofre	DOS/DDC
ID	Ação de Contingência	Responsável
0	A sala cofre possui monitoramento 24x7x365	DOS/DDC
ID	Ação Preventiva	Responsável
ID	Ação de Contingência	Responsável
0		
ID	Ação Preventiva	Responsável
ID	Ação de Contingência	Responsável
0		

Figura C.1: Risco - Acesso a sala cofre
Fonte: Elaboração própria.

Risco	Ataques externos	
Probabilidade	4	
Impacto	4	
Criticidade	16	
Tipo de tratamento de risco	Mitigar	
Dano 1	Violação do sigilo a informação, perda de dados	
Dano 2	indisponibilidade de sistema, indisponibilidade de dados, indisponibilidade de rede e telefonia	
Dano 3	Atraso no tramite de processos	
ID	**Ação Preventiva**	**Responsável**
	Verificar registros de log de equipamentos e sistemas	DOS/CSI
ID	**Ação de Contingência**	**Responsável**
0	Gerenciamento de eventos e redundância de equipamentos e firewall, capacitação de equipe técnica	DOS/CSI
ID	**Ação Preventiva**	**Responsável**
ID	**Ação de Contingência**	**Responsável**
0		
ID	**Ação Preventiva**	**Responsável**
ID	**Ação de Contingência**	**Responsável**
0		

Figura C.2: Risco - Ataques externos
Fonte: Elaboração própria.

Risco	Ataques internos	
Probabilidade	3	
Impacto	4	
Criticidade	12	
Tipo de tratamento de risco	Mitigar	
Dano 1	Violação do sigilo a informação, perda de dados	
Dano 2	indisponibilidade de sistema, indisponibilidade de dados, indisponibilidade de rede e telefonia	
Dano 3	Atraso no tramite de processos	
ID	**Ação Preventiva**	**Responsável**
	Verificar registro de log de equipamento e eventos de sistema	DOS/CSI
ID	**Violação do sigilo a informação, perda de dados**	**Responsável**
0	Gerenciamento de eventos e redundância de equipamentos e firewall, capacitação de equipe técnica	DOS/CSI
ID	**Ação Preventiva**	**Responsável**
ID	**Ação de Contingência**	**Responsável**
0		
ID	**Ação Preventiva**	**Responsável**
ID	**Ação de Contingência**	**Responsável**
0		

Figura C.3: Risco - Ataques Internos
Fonte: Elaboração própria.

Risco	Falha humana acidental ou impericia	
Probabilidade	2	
Impacto	2	
Criticidade	4	
Tipo de tratamento de risco	Mitigar	
Dano 1	Indisponibilidade de sistema, indisponibilidade de ativos, indisponibilidade ambiente de desenv. e homologa.	
Dano 2	Lentidão no acesso, perda de informações, falha de segurança de sistemas, atraso na distribuição de processos	
Dano 3	Instabilidade/indisponibilidade de serviços hospedados no servidor	
ID	Ação Preventiva	Responsável
	Verificar registros de log de equipamentos e eventos de sistema	DOS/CSI
ID	Ação de Contingência	Responsável
0	Capacitação, treinamento e controle de acesso de sistemas e serviços	DOS/CSI
ID	Ação Preventiva	Responsável
ID	Ação de Contingência	Responsável
0		
ID	Ação Preventiva	Responsável
ID	Ação de Contingência	Responsável
0		

Figura C.4: Risco - Falha humana acidental ou imperícia
Fonte: Elaboração própria.

Risco	Falta de energia no ambiente de datacenter	
Probabilidade	3	
Impacto	4	
Criticidade	12	
Tipo de tratamento de risco	Mitigar	
Dano 1	Indisponibilidade de sistemas, ativos e restauração de sistemas	
Dano 2	atraso na distribuição de processos	
Dano 3		
ID	Ação Preventiva	Responsável
	Verificar registros de acionamento de gerador de energia e combustível	DOS/DDC
ID	Ação de Contingência	Responsável
0	Gerador de tanque interno com capacidade de fornecimento de 25 horas + tanque para fornecimento de 100 horas de energia	DOS/DDC
ID	Ação Preventiva	Responsável
ID	Ação de Contingência	Responsável
0		
ID	Ação Preventiva	Responsável
ID	Ação de Contingência	Responsável
0		

Figura C.5: Risco - Falta de energia
Fonte: Elaboração própria.

Risco	Migração e mudança em aplicações virtuais	
Probabilidade	1	
Impacto	1	
Criticidade	1	
Tipo de tratamento de risco	Aceitar	
Dano 1	Indisponibilidade de sistema e informações	
Dano 2	falha no sistema, falha de rede e falhas operacionais	
Dano 3		
ID	Ação Preventiva	Responsável
	Verificar registros de eventos relacionados a alterações de infraestrutura e sistema	DOS/CSI
ID	Ação de Contingência	Responsável
0	Uso de máquinas virtuais para migração e aplicação ágil de máquinas virtuais	DOS/DDC
	Manter ambiente de teste de movimentação de máquinas virtuais	
ID	Ação Preventiva	Responsável
ID	Ação de Contingência	Responsável
0		
ID	Ação Preventiva	Responsável
ID	Ação de Contingência	Responsável
0		

Figura C.6: Risco - Migração e mudança em aplicações virtuais
Fonte: Elaboração própria.

Risco	Problemas de equipamentos de hardware	
Probabilidade	3	
Impacto	4	
Criticidade	12	
Tipo de tratamento de risco	Mitigar	
Dano 1	Indisponibilidade de sistema e ativos	
Dano 2	Lentidão de acesso ao sistema, perda de dados e informações, atraso na distribuição de processos	
Dano 3	Falha de segurança do sistema	
ID	Ação Preventiva	Responsável
	Verificar registro de log de equipamentos e eventos de sistema	DOS/CSE
ID	Ação de Contingência	Responsável
0	Contrato com fabricante de equipamento para suporte	DOS/DDC
ID	Ação Preventiva	Responsável
ID	Ação de Contingência	Responsável
0		
ID	Ação Preventiva	Responsável
ID	Ação de Contingência	Responsável
0		

Figura C.7: Risco - Problemas de equipamento de hardware
Fonte: Elaboração própria.

Risco	Problema de equipamentos de conexão	
Probabilidade	3	
Impacto	4	
Criticidade	12	
Tipo de tratamento de risco	Mitigar	
Dano 1	Indisponibilidade de sistema e ativos	
Dano 2	Lentidão de acesso ao sistema, atraso na distribuição de processos	
Dano 3	Falha na realização de backup e restauração de sistema	
ID	**Ação Preventiva**	**Responsável**
	Verificar registros de log de equipamentos e eventos de sistema	DOS/CSE
ID	**Ação de Contingência**	**Responsável**
0	Gerenciamento de eventos e redundância de enlaces	DOS/CRI
ID	**Ação Preventiva**	**Responsável**
ID	**Ação de Contingência**	**Responsável**
0		
ID	**Ação Preventiva**	**Responsável**
ID	**Ação de Contingência**	**Responsável**
0		

Figura C.8: Risco - Problemas em equipamentos de conexão
Fonte: Elaboração própria.

Risco	Riscos na identificação de eventos	
Probabilidade	2	
Impacto	2	
Criticidade	4	
Tipo de tratamento de risco	Compartilhar/Tranferir	
Dano 1	Tempo de solução de problemas elevado	
Dano 2	Falha de equipamentos	
Dano 3	Falha de sistema de rede de dados	
ID	**Ação Preventiva**	**Responsável**
Dano 1	Verificar registro de responsabilidades e comunicação de incidentes	DOS/CSE
ID	**Ação de Contingência**	**Responsável**
Dano 1	Contrato com empresa terceirizada de monitoramento de eventos críticos	DOS
ID	**Ação Preventiva**	**Responsável**
Dano 1		
ID	**Ação de Contingência**	**Responsável**
Dano 1		
ID	**Ação Preventiva**	**Responsável**
ID	**Ação de Contingência**	**Responsável**
0		

Figura C.9: Risco - Identificação de eventos
Fonte: Elaboração própria.

Risco	Risco pessoal	
Probabilidade	3	
Impacto	1	
Criticidade	3	
Tipo de tratamento de risco	Aceitar	
Dano 1	Tempo de solução de problemas elevado	
Dano 2	Falha de equipamentos e conexões de rede	
Dano 3	Soluções reativas, perda de conhecimento técnico, perda de credibilidade	
ID	Ação Preventiva	Responsável
Dano 1	Verificar escala de responsabilidades e gestão de sistemas	DOS
ID	Ação de Contingência	Responsável
Dano 1	Plano de capacitação e apoio a educação continuada	CIC
ID	Ação Preventiva	Responsável
Dano 1		
ID	Ação de Contingência	Responsável
Dano 1		
ID	Ação Preventiva	Responsável
Dano 1		
ID	Ação de Contingência	Responsável
Dano 1		

Figura C.10: Risco - Pessoal técnico
Fonte: Elaboração própria.

Risco	Sala cofre	
Probabilidade	2	
Impacto	4	
Criticidade	8	
Tipo de tratamento de risco	Mitigar	
Dano 1	Indisponibilidade de serviços de tecnologia	
Dano 2	Tempo de solução de problemas elevado	
Dano 3		
ID	Ação Preventiva	Responsável
Dano 1	Verificar registros de eventos, acesso e controle da sala cofre	DOS/DDC
ID	Ação de Contingência	Responsável
Dano 1	Sala certificada com manutenção em dia e redundância no sistema de climatização	DOS/DDC
ID	Ação Preventiva	Responsável
Dano 2	Duplicidade de armazenamentos críticos do sistema	DOS/CSE
ID	Ação de Contingência	Responsável
Dano 2	Redundância de equipamentos de backup	DOS
ID	Ação Preventiva	Responsável
ID	Ação de Contingência	Responsável
0		

Figura C.11: Risco - Sala cofre
Fonte: Elaboração própria.

Apêndice D

Roteiro de reunião

Agradeço a participação de todos presentes. É importante deixar claro que a reunião esta relacionada ao entendimento da sustentação do sistema SEI na UnB. Pessoa chave foram selecionadas pois possuem atividades ligadas a sustentação do sistema e conhecem ou não as rotinas envolvidas na disponibilidade do SEI a comunidade acadêmica.

É importante ressaltar que as informações levantadas nesta reunião terão caráter confidencial e sua utilização será estritamente para fins acadêmicos, bem como será assegurado o anonimato dos entrevistados.

Desta forma, se iniciam as perguntas.

P1 - Em relação aos serviços críticos de tecnologia da UnB. Você considera o sistema SEI um desses serviços?

P2 - Em relação aos ativos relacionados ao sistema SEI. Você considera que estão seguros? Em casos de eventos extremos como tempestade, queimadas ou desabamento. Você considera que o sistema, no caso de algum desse eventos, permaneceria disponível?

P3 - Referente as rotinas de backup. Existe rotina de backup para o sistema SEI? Se sim, você conhece a periodicidade dessa rotina? Sabe informar a mídia de armazenamento? Conhece o local de armazenamento dessas mídias?

P4 - Ainda de acordo com backup. Em caso de perda de dados, existe um procedimento documentado a ser seguido? Nos últimos 2 anos, houve indisponibilidade do sistema por conta de perda de dados? Se sim, quanto tempo?

P5 - Em relação aos ativos físicos relacionados ao SEI. Em caso de falha de algum desses ativos, existe procedimento para transferir o serviço para outro ativo? A Secretaria tem algum plano de contingência caso algum desastre ocorra?

P6 - Existe algum ciclo de gestão de riscos relacionado aos ativos do sistema SEI? É possível descrever algum risco relacionado a disponibilidade desses ativos?

P7 - A Secretaria aplica medidas de segurança da informação ao sistema SEI? Se sim, você as conhece? Pode mencionar exemplos?

P8 - Quais impactos ou consequências da indisponibilidade do sistema SEI?

P9 - A Secretaria conhece os riscos existentes na sustentação do sistema SEI? Se sim, quais foram levantados?

P10 - A Secretaria conhece os riscos em seu ambiente externo e interno? (Ameaças naturais, físicas e humanas)

P11 - O SEI nos últimos 2 anos, sofreu algum incidente que interrompesse a continuidade de negócio da instituição? Ex.: Perda de prazo em processos por conta da indisponibilidade do sistema

P12 - Existe algum plano de continuidade de negócios relacionado ao sistema SEI no qual garanta que o sistema continue disponível em caso de incidentes ou desastres?

P13 - Tem alguma informação para acrescentar a esta pesquisa? Se sim, pode expor?