COIMBRA BUSINESS SCHOOL

Plano de Continuidade de Negócio no Setor Público

Joana Rita Coelho Rodrigues

ISCAC | 2025

COIMBRA BUSINESS SCHOOL

iscac Politécnico de Coimbra

100 ANOS

Joana Rita Coelho Rodrigues

Dissertação

Plano de Continuidade de Negócio no Setor Público

Coimbra, abril de 2025

Joana Rita Coelho Rodrigues

Plano de Continuidade de Negócio no Setor Público

Dissertação submetida ao Instituto Superior de Contabilidade e Administração de Coimbra para cumprimento dos requisitos necessários à obtenção do grau de **Mestre em Sistemas de Informação de Gestão**, realizada sob a orientação do Professor Doutor Flávio Costa Romão (ISEG, Universidade de Lisboa) e coorientação da Professora Doutora Isabel Mendes Pedrosa.

Coimbra, abril de 2025

TERMO DE RESPONSABILIDADE

Declaro ser a autora desta dissertação, que constitui um trabalho original e inédito, que nunca foi submetido a outra Instituição de Ensino Superior para obtenção de um grau académico ou outra habilitação. Atesto ainda que todas as citações estão devidamente identificadas e que tenho consciência de que o plágio constitui uma grave falta de ética, que poderá resultar na anulação do presente projeto.

PENSAMENTO

"Quem desiste nunca vence e só vence quem nunca desiste"
Napoleon Hill

DEDICATÓRIA

Todos os dias enfrentamos novos desafios e temos de encontrar formas de os superar. Cada desafio é uma nova oportunidade de evolução, para nos tornarmos cada vez mais resilientes, fortes e sábios.

Dedico este trabalho à minha filha Rita, para que não se esqueça que nunca é tarde demais para lutar pelos seus sonhos e que o principal compromisso é ser melhor do que ontem, não melhor do que ninguém.

AGRADECIMENTOS

Em primeiro lugar, um agradecimento muitíssimo especial à minha família, pois sem o apoio incondicional e entreajuda, nada disto seria possível.

À minha mãe, principalmente, pois foi quem teve a maior disponibilidade para me apoiar e ajudar na tomada de decisões, bem como sugerir coisas essenciais para o desenvolvimento da presente dissertação.

Por outro lado, e não menos importante, agradeço aos professores que sempre me cativaram e motivaram, tanto no decorrer desta dissertação, como no percurso até então.

Ao Professor Doutor Flávio Costa Romão pela fantástica orientação. E à Professora Doutora Isabel Mendes Pedrosa, que desde início da minha licenciatura sempre teve um cuidado especial no que toca a motivação e grande disponibilidade em ajudar no que fosse necessário.

Um agradecimento especial a ambos por toda a ajuda, tempo despendido e paciência para comigo. Muito obrigada pela vossa fantástica e essencial colaboração.

RESUMO

As organizações dependem cada vez mais dos Sistemas de Informação e estão constantemente sujeitas a interrupções inesperadas, como desastres naturais e outras situações que causam indisponibilidade nos seus negócios. Por esta razão, ter um Plano de Continuidade de Negócio (PCN) é crucial para que as organizações sejam resilientes e reduzam os danos causados por eventos disruptivos. Empregando uma metodologia de *Action-Research*, este estudo investiga o método de implementação de um PCN, num organismo da Administração Pública, seguindo *standards* internacionais e boas práticas de gestão de serviços de Tecnologias de Informação e *Governance*. Neste contexto, o setor da Justiça, enquanto um dos pilares fundamentais do Estado de Direito, assegura o cumprimento da lei e a resolução de conflitos na sociedade. Os principais resultados sublinham a importância de um PCN atualizado, evidenciando a sua relevância para garantir a resiliência organizacional. Adicionalmente, esta pesquisa proporciona contributos práticos relevantes para a compreensão de como assegurar a recuperação de desastres neste setor, ao mesmo tempo que reforça e expande o corpo de conhecimento teórico existente sobre a temática.

Palavras-chave: Plano de Continuidade de Negócio; Administração Pública; Setor da Justiça; Canonical Action Research; Plano de Recuperação de Desastres

ABSTRACT

Organizations increasingly rely on Information Systems and are constantly subject to unexpected disruptions, such as natural disasters and other situations that cause downtime in their businesses. For this reason, having a Business Continuity Plan (BCP) is crucial for organizations to be resilient and reduce the damage caused by disruptive events. Using an Action-Research methodology, this study investigates the method of implementing a BCP in a Public Administration body, following international standards and good practices in Information Technology and Governance service management. In this context, the Justice sector, one of the fundamental pillars of the rule of law, ensures compliance with the law and resolves conflicts in society. The main results highlight the importance of an updated BCP, highlighting its relevance to guarantee organizational resilience. Additionally, this research provides relevant practical contributions to the understanding of how to ensure disaster recovery in this sector, while reinforcing and expanding the existing body of theoretical knowledge on the subject.

Keywords: Business Continuity Plan; Public Administration; Justice Sector; Canonical Action Research; Disaster Recovery Plan

ÍNDICE GERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

Lista de abreviaturas, acrónimos e siglas

AP – Administração Pública

BCM – *Business Continuity Management*

BCP – *Business Continuity Plan*

BIA – *Business Impact Analysis*

CAR – *Canonical Action Research*

CD – Conselho Diretivo

CMD – *Change Management Database*

COBIT – *Control Objectives for Information and Related Technology*

DRP – *Disaster Recovery Plan*

ERD – Equipa de Recuperação de Desastre

ERI – Equipa de Resposta a Incidentes

GCN – Gestão de Continuidade de Negócio

GL – *Grey Literature* (Literatura Cinza)

IAM – *Indentity Access Management*

IRM – *Institute of Risk Management*

ISACA – *Information Systems Audit and Control Association*

ISO – *International Organization for Standardization*

IT – *Information Technology*

ITAM – *IT Asset Management*

ITIL – *Information Technology Infrastructure Library*

KPIs – *Key Performance Indicators*

MJ – Ministério da Justiça

MLR – *Multivocal Literature Review* (Revisão Multivocal de Literatura)

MTD – *Maximum Tolerable Downtime*

PCN – Plano de Continuidade de Negócio

PDCA – *Plan, Do, Check, Act/Adjust*

RA – *Risk Analysis*

RPO – *Recovery Point Objective*

RTO – *Recovery Time Objective*

SI – Sistemas de Informação

SLA – *Service Level Agreement*

TI – Tecnologias da Informação

2. Introdução

Vivemos atualmente numa realidade onde a tecnologia e o mundo digital estão enraizados no dia-a-dia e cotidiano da maioria das pessoas, acabando mesmo por definirem certos aspetos das suas vidas.

O grande e rápido avanço tecnológico que estamos a presenciar já há algumas décadas, apresenta agora um fator crítico, principalmente a nível da proteção de dados devido a ciberataques, que estão cada vez mais sofisticados. Por outro lado, a tecnologia é um pilar na sociedade, sendo que as interrupções e falhas nas suas normais operações podem causar repercussões irremediáveis de grande impacto (Hilbert, 2020).

Acompanhando a mencionada realidade da simbiose entre a tecnologia e inovação das sociedades, foi inevitável que as organizações se tornassem fortemente dependentes de Sistemas de Informação (SI) (Roztocki et al., 2020). Com o recurso aos SI, as organizações passaram a ter um suporte para os processos de tomada de decisão e melhoraram a sua eficiência operacional, e também contribuírem em grande escala para a memória organizacional, facilitarem o acesso a dados históricos e, por sua vez, apoiarem as tomadas de decisão (Boghossian et al., 2019).

Os SI assentam num conjunto de procedimentos com a finalidade de assegurar a existência de informação imprescindível às diferentes funções e níveis da organização, bem como à sua envolvente externa (Silva, 2016), sendo assim cada vez mais relevante e necessário assegurar o seu constante e normal funcionamento.

Conforme Laudon & Laudon (2007), é necessário entender as dimensões dos SI, para que sejam empregues com eficiência. As organizações apoiam-se nos processos organizacionais, em pessoas com diferentes tipos de conhecimentos e em ferramentas tecnológicas para a possível execução e coordenação do trabalho, conforme representado na Figura 1.

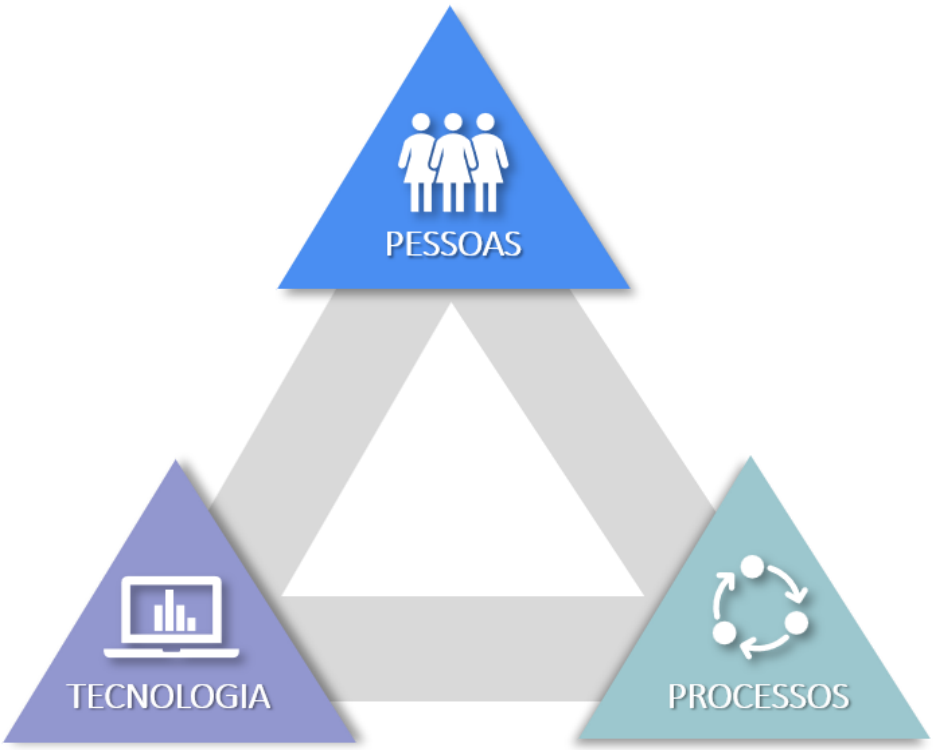

Figura 1 – Teoria dos Sistemas de Informação (adaptado de Laudon & Laudon, 2007).

Análises sobre interrupções e catástrofes em SI destacam a importância da gestão do conhecimento na análise e prevenção de falhas (Almeida et al., 2006). É por este motivo que organizações e instituições devem proteger-se contra os diversos tipos de ameaças às quais estão expostas que podem interromper as suas normais operações. Estas ameaças são diversas e podem ser desde desastres naturais até ciberataques.

Seguindo a inovação tecnológica organizacional empresarial, de implementação de SI e Tecnologias da Informação (TI), a Administração Pública (AP) não é exceção.

Segundo MacLean e Titah (2021), os governos têm vindo a investir tecnologicamente, podendo gerar valor público diretamente para os clientes dos novos sistemas, bem como para os contribuintes interessados no uso eficaz dos recursos governamentais e para os cidadãos que têm objetivos sociais mais amplos, incluindo o desenvolvimento da confiança, da comunicação e do envolvimento com o governo.

Por sua vez, acabam também por enfrentar ameaças da preservação de informação e até no próprio funcionamento dos seus SI.

A AP, em comparação com o setor privado, sofre de obstáculos específicos e concretos que derivam da sua natureza institucional. Estes incluem fatores técnicos, políticos e organizacionais (Souza & Reinhard, 2015). No setor público existem, além das normais ameaças de catástrofes naturais e ciberataques, desafios acrescentados devido às estruturas lentas e desatualizadas, que frequentemente levam à prestação inadequada de serviços e ao envolvimento ineficiente dos cidadãos (Souza & Reinhard, 2015).

Sendo o bem-estar do cidadão uma prioridade da AP, esta deverá ser capaz de corresponder às expectativas de cada indivíduo. Assim, torna-se fundamental que as autoridades competentes assegurem a capacidade de todos os setores e organismos de atuarem numa base contínua e evitarem situações que causem disrupções e indisponibilidade na sua atividade (Decreto-Lei n.º 135/99, 1999). Abordar essas lacunas é crucial para melhorar a transparência, a eficiência e a integridade nos SI do setor público, contribuindo, assim, para um desenvolvimento económico e social mais amplo, rápido e eficaz.

Tendo como referência as atuais práticas, a abordagem para instituir melhoria, resiliência e continuidade dos SI, essencial para garantir a sustentabilidade das organizações, passa fundamentalmente pela implementação da Gestão de Continuidade de Negócio (GCN), conhecida como *Business Continuity Management* (BCM), imprescindível para que as organizações mitiguem interrupções de serviços e mantenham as operações ativas e consistentes (Becerra Acevedo et al., 2021).

A GCN consiste num processo para garantir que as organizações possam continuar com os seus próprios negócios apesar das ameaças (Hecht, 2002). Deste modo, conseguem entregar os seus produtos e/ou serviços com a maior brevidade possível e com níveis de qualidade normais, mesmo durante um evento disruptivo.

A implementação de um sistema de GCN envolve avaliação de impacto, valorização de riscos e desenvolvimento de planos de continuidade de negócio para garantir a disponibilidade de recursos e situações críticas (Becerra Acevedo et al., 2021).

Os modelos de implementação de GCN têm vindo a evoluir de forma a irem ao encontro das necessidades específicas das empresas/organizações, incorporando

abordagens como o ciclo *Plan-Do-Check-Act* (PDCA), ou seja, planear, fazer, verificar e agir (Becerra Acevedo et al., 2021), *Frameworks* de boas práticas, como ISO 22301 e *Control Objectives for Information and Related Technology* (COBIT), bem como *Disaster Recovery Plan* (DRP), que são utilizados para alinhar a GCN com a gestão de TI e os objetivos estratégicos (Gatto et al., 2023).

Um PCN é uma ferramenta essencial na GCN, orientado à recuperação da infraestrutura tecnológica. Através de mecanismos de redundância, como a migração de dados ou a replicação dos vários ambientes, permite a recuperação dos processos de negócio e dos dados na sua totalidade e, claro, no menor período temporal possível (Huapaya-Ruiz & Meneses-Claudio, 2024).

Possuindo estas características, o PCN auxilia as organizações na gestão, prevenção e mitigação adequadas de possíveis riscos. Por sua vez, este plano deve ser dinâmico e nele devem ser executados testes e atualizações consistentes e regulares, abrangendo estratégias de contingência para que as empresas sejam capazes de atuar com a maior brevidade possível quando estão perante eventos disruptivos ou incidentes (da Silveira, 2009; de Oliveira et al., 2024).

Atualmente existem ainda muitas organizações que não ponderam a existência de um PCN, por várias razões, sejam elas por falta de informação ou conhecimento, ou até mesmo questões financeiras. No entanto, tendo em conta que a continuidade de negócio está interligada com a gestão de risco, acaba por ser um desafio com o qual qualquer organização tem de lidar (Silva, 2016).

Por conseguinte, é essencial que as organizações realizem uma GCN com criação, implementação e atualizações constantes de um PCN.

3. Objetivos

Qualquer tipo de organização deve estabelecer políticas e procedimentos que assegurem o funcionamento contínuo da sua atividade, bem como a recuperação atempada sempre que se verifiquem eventos disruptivos, sendo que, em caso de desastre, é o órgão de administração que deve ser o responsável por ativar os procedimentos de continuidade de negócio.

Uma vez que as organizações dependem, cada vez mais, dos SI, e seguido o âmbito da justificação deste trabalho, o principal objetivo no desenvolvimento da presente Dissertação passa por sistematizar o conhecimento sobre o PCN, procedendo à sua elaboração numa entidade da AP, mais propriamente do setor da Justiça.

Segundo o relatório da Organização para a Cooperação e Desenvolvimento Económico, OECD (2024), Portugal continua a desenvolver o seu quadro jurídico com base em iniciativas, que têm como objetivo tornar a Justiça mais acessível às pessoas, tais como o programa Justiça + e o Plano de Recuperação e Resiliência (PRR).

É crucial, para o sistema de Justiça, ter a capacidade de proporcionar o acesso a mais e melhor informação e consentir maior proximidade e facilidade, bem como um elevado nível de transparência e simplificação da linguagem na comunicação para com os cidadãos.

Na última década, conforme relatório da OECD (2024:3), "*Portugal adotou uma reforma abrangente do seu sistema de justiça para torná-lo mais inclusivo e eficiente*". É, no entanto, fundamental existir neste setor um PCN para mitigar possíveis falhas no sistema.

Um PCN desatualizado ou elaborado incorretamente faz com que as organizações comprometam a segurança e integridade e confiabilidade da informação, bem como o serviço prestado, tornando-se crucial o desenvolvimento de um plano, devendo ser dinâmico, envolvendo a realização de testes e atualizações constantes e regulares, abrangendo aspetos como objetivos, recuperação de desastres e continuidade operacional.

Por puro desconhecimento ou, até mesmo, por questões financeiras, muitas organizações subestimam a existência desses planos, no entanto a GCN está interligada com a gestão do risco, gerando um desafio com o qual têm de lidar, antecipando e prevenindo, assim, acontecimentos inesperados e mitigando possíveis riscos associados (Silva, 2016).

Existem diversos exemplos bem-sucedidos aquando da aplicação de um PCN, pelo que, confirma-se que esta cultura organizacional evidencia um fator essencial para que o setor da Justiça garanta a continuidade do negócio em caso de uma disrupção, melhorando a qualidade dos serviços prestados.

A grande motivação para o desenvolvimento da presente Dissertação passa, conforme referido anteriormente, pela idealização e criação de um PCN para um organismo da AP, seguindo *standards* internacionais e boas práticas de gestão de serviços das TI e de *Governance.* É também objetivo, sistematizar a teoria existente em relação ao tema e identificar boas práticas que facilitem implementações futuras de planos desta natureza, em particular num contexto de AP, contribuindo-se, assim, para o corpo de conhecimento teórico que existe sobre o tema.

Com base na literatura atual, os objetos de investigação que guiam este trabalho visam a identificação do que existe no momento do levantamento de informação e, em seguida, de que forma será possível implementar um PCN no setor da Justiça, seguindo as boas práticas.

Consequentemente, a principal questão estrutura-se da seguinte forma:

> Questão 1: Como implementar um Plano de Continuidade de Negócio no setor da Justiça, seguindo *standards* internacionais e boas práticas de gestão de serviços de TI e Governance?

Este estudo também aborda uma questão secundária. Visa obter uma melhor compreensão das implicações da implementação de ações que procuram garantir a recuperação de serviços em casos de eventos disruptivos. Assim, a questão é articulada da seguinte forma:

> Questão 2: Como garantir a recuperação de desastres no setor da Justiça?

4. Revisão da Literatura

Num contexto organizacional em que existe uma constante mudança e evolução, a capacidade de uma organização se adaptar a desafios e incertezas é fundamental para a sobrevivência e o sucesso da mesma.

As organizações que implementam GCN e um PCN, demonstram um objetivo estratégico de terem a capacidade de dar respostas adequadas a incidentes disruptivos que afetam pessoas, ativos, dados ou processos de negócio, dos quais depende o normal funcionamento das mesmas (Becerra Acevedo et al., 2021).

Um PCN é essencial para a sobrevivência e competitividade das empresas, especialmente em situações de crise (de Oliveira et al., 2024), envolvendo a identificação de vulnerabilidades e ameaças.

Componentes importantes de um PCN são a identificação de recursos críticos, definição de estratégias de contingência e elaboração de documentos como o "Plano de Gestão de Incidentes" (da Silveira, 2009). Por sua vez, estes planos de continuidade de negócio são mais eficazes quando fundamentados em normas internacionais e orientadas para os seus objetivos de negócio.

4.1 Normativos para a Continuidade de Negócio

No seguimento de um crescimento tecnológico a um ritmo acelerado e volátil, as organizações não podem correr o risco de terem planos ineficientes e desatualizados. Deste modo, para fins de elaboração e desenvolvimento de um PCN foram identificadas na literatura a ter em conta, as quais serão abordadas em seguida.

4.1.1 Normas ISO 22301 e ISO 27005

A International Organization for Standardization elabora normas de conduta internacionalmente aceites, conhecidas por ISO.

A norma ISO 22301 é a norma internacional para a GCN e foi concebida para ajudar as organizações a prevenir, preparar, responder e recuperar de eventos disruptivos, de forma a mitigar os danos e continuar o seu funcionamento (ISO, 2024).

Fornece também uma visão clara e detalhada de como uma organização atua, oferecendo *insights* valiosos que são úteis para o planeamento estratégico, a gestão de riscos, a transformação de negócios e a gestão de recursos. A Tabela 1 reflete a sua importância e os principais benefícios e elementos da norma.

Tabela 1 – Importância e Benefícios da ISO 22301 (adaptado de ISO 22301:2019).

Categoria	**Detalhe**
Relevância para o negócio	Auxilia as organizações a tornarem-se mais resilientes, minimizando o impacto de incidentes e interrupções
	Garante a continuidade das operações, mesmo em situações hostis
	Protege os ativos da organização
	Demonstra um compromisso com a qualidade e a continuidade dos serviços, garantindo a satisfação dos clientes
	Auxilia no cumprimento de requisitos legais e regulatórios, garantindo a conformidade legal
Principais benefícios para o negócio	Diferencia a organização no mercado, tornando-a competitivamente vantajosa
	Minimiza as perdas financeiras associadas a eventos disruptivos, reduzindo custos
	Fornece uma base sólida para a tomada de decisões
	Demonstra um compromisso com a segurança e a resiliência, aumentando a sua reputação
Principais elementos do negócio	Compreender a organização e respetivos *stakeholders* e o contexto em que atua
	Demonstrar liderança e compromisso
	Desenvolver planos, garantindo a continuidade do negócio
	Garantir os recursos necessários à implementação dos planos
	Implementar e manter a continuidade de negócio de acordo com os planos
	Monitorizar o desempenho da continuidade de negócio
	Implementar ações para melhorar continuamente o negócio

Reunindo as melhores práticas internacionais para ajudar as organizações a responderem e recuperarem interrupções de forma eficaz, esta norma deve ser considerada em qualquer organização da AP.

A norma ISO 22301, à semelhança de outras, segue o ciclo PDCA, demonstrado na Figura 2, que permite a integração com outros sistemas de gestão, nomeadamente:

- ISO 9001 – Sistema de Gestão da Qualidade;
- ISO 14001 – Sistema de Gestão Ambiental;
- ISO 27001 – Sistema de Gestão da Segurança de Informação;
- ISO 20000-1 – Gestão de Serviços de Tecnologias de Informação.

Os requisitos especificados na norma ISO 22301 de planear, estabelecer, implementar, agir, monitorizar, rever, manter e melhorar continuamente um sistema de gestão, são genéricos e aplicáveis a todas as organizações, independentemente da sua dimensão, tipo ou natureza (ISO, 2024).

Figura 2 – Ciclo PDCA ISO 22301 (Marker, 2022).

Para a correta implementação desta norma, é fundamental avaliar os riscos e os impactos de forma abrangente, identificando, assim, as potenciais ameaças que podem afetar a organização, bem como proceder à avaliação do impacto no negócio. Após esta avaliação, a organização deve procurar elaborar um PCN envolvendo todas as partes interessadas no processo da elaboração do mesmo.

Além da ISO 22301, usada para a elaboração do PCN, constata-se o recurso à ISO 27005 - orientação sobre gestão de riscos de segurança da informação - para identificar as ameaças e desenvolver a matriz de avaliação do risco.

A norma ISO 27005, representada na Figura 3, não especifica qualquer método de gestão de risco em concreto, mas estabelece orientações para as metodologias mais apropriadas, bem como suporte à tomada de decisão (ISO, 2024).

Consiste num ciclo contínuo que envolve várias atividades. Inicia-se com a contextualização, no qual é definido o âmbito da análise de riscos, identificando os ativos e os processos por fora a compreender todo o ambiente organizacional.

A identificação dos riscos é a fase seguinte. Aqui reconhecem-se as ameaças que podem comprometer os ativos, bem como as vulnerabilidades existentes e associadas a cada um deles, avaliando as potenciais consequências das mesmas.

Por conseguinte, é então necessário avaliar a probabilidade da ocorrência de cada risco e qual o grau de impacto para o negócio. Para tal, determina-se o nível e a prioridade de cada risco com base nos critérios de cada organização.

Após os processos anteriormente descritos, as organizações devem decidir como lidar com os riscos identificados, optando pela mitigação e aceitação dos mesmos. Para que tal seja possível, podem delegar o risco, por exemplo, recorrendo à subscrição de novos seguros ou até mesmo à alteração de métodos afim de evitar os riscos evidenciados.

Garantir que todos os interessados durante o processo estão cientes dos riscos e das medidas de controlo implementadas, faz parte do ciclo. Para o concluir, são essenciais os processos de monitorização constante e atualização regular da análise de riscos de modo a agir adequadamente às mudanças significativas no ambiente organizacional.

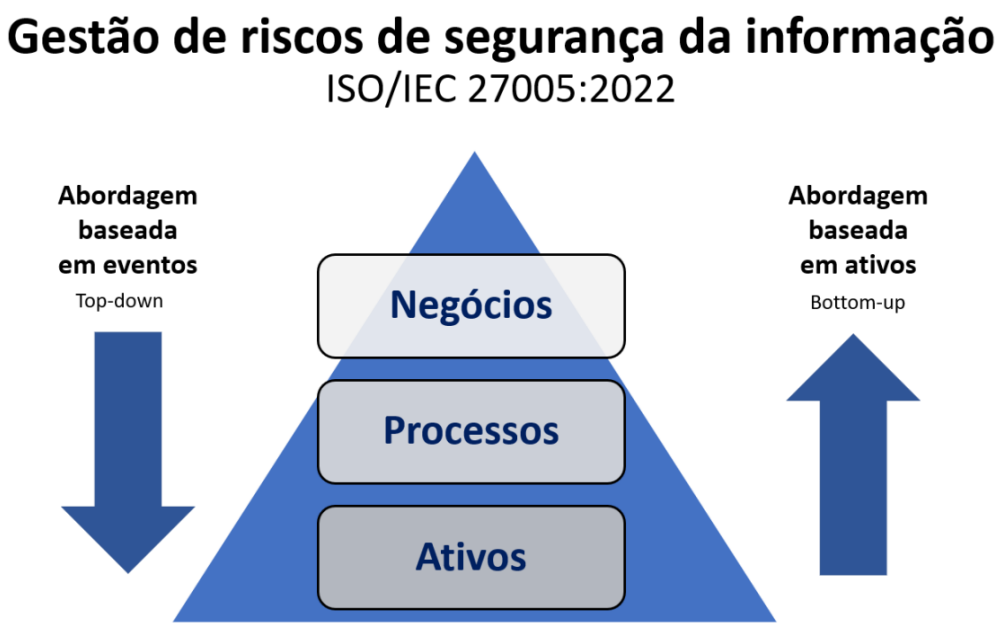

Figura 3 – ISO 27005 (ISO, 2022).

4.1.2 COBIT

O COBIT foi desenvolvido pela *Information Systems Audit and Control Association* (ISACA), como uma estrutura abrangente de diretrizes para a gestão de TI empresarial. Este abrange várias áreas da gestão e de TI, incluindo segurança, gestão de riscos, desenvolvimento de sistemas e controlo interno (de Haes et al., 2013).

O modelo de *governance* COBIT, foca-se nos controlos e nas métricas e releva a importância e o impacto do risco para a organização/empresa/entidade, por definir e quantificar os ativos sujeitos a risco e contabilizar os custos de mitigação ou perdas em caso de incidentes.

O COBIT evoluiu ao longo do tempo e conta atualmente com a sua quinta edição. Expandiu o seu âmbito para abranger áreas tradicionais relacionadas a SI. A estrutura é construída, conforme representa a Figura 4, em cinco princípios básicos que descrevem os requisitos de um sistema de governança de TI eficaz (de Haes et al., 2013), nomeadamente:

1. Responder às necessidades das partes interessadas;
2. Incluir a organização no seu todo;

3. Aplicar um único modelo integrado;
4. Permitir a abordagem holística;
5. Separar a *Governance* de Gestão.

Figura 4 – Princípios COBIT (adaptado de Rodríguez Cruz, M. A. 2025).

O COBIT contribui para as necessidades organizacionais, uma vez que auxilia as organizações a estabelecerem uma ligação com os requisitos do negócio, bem como a organizar as suas atividades de TI. Através deste modelo, as organizações identificam, com maior facilidade, os principais recursos de TI para o seu melhor aproveitamento e definem os objetivos de controlo de gestão que devem ser considerados (da Silveira, 2009).

Unindo as normas e as melhores práticas de TI, o COBIT tem a capacidade de auxiliar as organizações na criação de valor, preservando o equilíbrio entre a realização de benefícios e a otimização dos níveis de risco e da utilização de recursos (Souza, 2022).

Estudos comprovam que recorrendo à sua implementação do COBIT as organizações demonstram resultados positivos, incluindo melhor qualidade de serviço,

redução do tempo de resolução de incidentes e melhor monitorização da própria infraestrutura (Ribeiro & Gomes, 2009).

Desta forma, o COBIT proporciona uma estrutura robusta para que as organizações consigam governar e gerir efetivamente os seus recursos de TI, alinhando-os com os objetivos do negócio, melhorando assim o desempenho geral de toda a organização (de Haes et al., 2013).

Um PCN amplo pressupõe a identificação de recursos críticos, a definição de estratégias de contingência e o desenvolvimento de planos de gestão de incidentes e continuidade (da Silveira, 2009).

Segundo o descrito anteriormente, podemos afirmar que, no contexto do PCN, recorrendo ao COBIT conseguimos assegurar que a gestão de TI fica alinhada com as prioridades das organizações, garantindo que os recursos tecnológicos críticos são identificados, preservados e organizados para uma rápida recuperação. Ajuda as organizações a priorizar e a gerir estes recursos e garante que estes fiquem eficientemente distribuídos e que a redundância é devidamente planeada para evitar possíveis interrupções.

Com a sua estrutura robusta, o COBIT ajuda também na identificação e mitigação dos riscos que podem comprometer a continuidade de negócio, como os ciberataques, as falhas de infraestrutura e até a perda de dados.

A nível de gestão de recursos, o COBIT integra práticas de DRP, permitindo que os sistemas e dados críticos sejam rapidamente restaurados após eventos disruptivos, promovendo ainda o desenvolvimento de políticas de *backups* e testes frequentes de recuperação.

Através deste modelo as organizações têm a capacidade de acompanhar continuamente e com prontidão os riscos associados, recorrendo às métricas que o COBIT fornece para medir a eficácia no contexto da continuidade, como o tempo de recuperação (*Recovery Time Objective* – RTO) e a perda aceitável de dados (*Recovery Point Objective* – RPO), que serão abordados no seguinte capítulo.

O COBIT promove ainda a criação de documentação clara e fluxos de comunicação que são cruciais para um PCN.

Pode-se, desta forma, concluir que o COBIT proporciona o alinhamento das TI com as necessidades das organizações, reduzindo riscos e garantindo a resiliência dos sistemas críticos, sendo por esse razão um modelo a seguir aquando da implementação de um PCN.

4.2 Análise de Impacto de Negócio

A Análise de Impacto de Negócio (*Business Impact Analysis*, BIA) é um processo crítico que avalia os diferentes impactos de potenciais disrupções dos processos de negócio numa organização (Păunescu et al., 2018).

Envolve a análise das potenciais consequências da perda de integridade, confidencialidade e disponibilidade de dados (Bagiński & Rostanski, 2011), permitindo identificar e priorizar os processos críticos da organização e recursos que os suportam através da definição de requisitos de recuperação.

O principal objetivo do BIA passa então por identificar os processos críticos e garantir a continuação dos processos de negócio, sendo que para tal é necessário recorrer a conceitos-chave específicos (Wiboonratr, M., & Kosavisutte, K. 2009), representados na Figura 5:

- MTPD (*Maximum Tolerable Period of Disruption*): Tempo máximo de interrupção tolerável para o qua os impactos não se tornem inaceitáveis para a organização;
- RTO (*Recovery Time Objective*): Período de tempo, inferior ao MTPD, ideal para recuperar as atividades interrompidas com um nível de funcionamento mínimo aceitável;
- RPO (*Recovery Point Objective*): Limite aceitável para a perda de dados, servindo de base à definição da periodicidade mínima de *backups*.

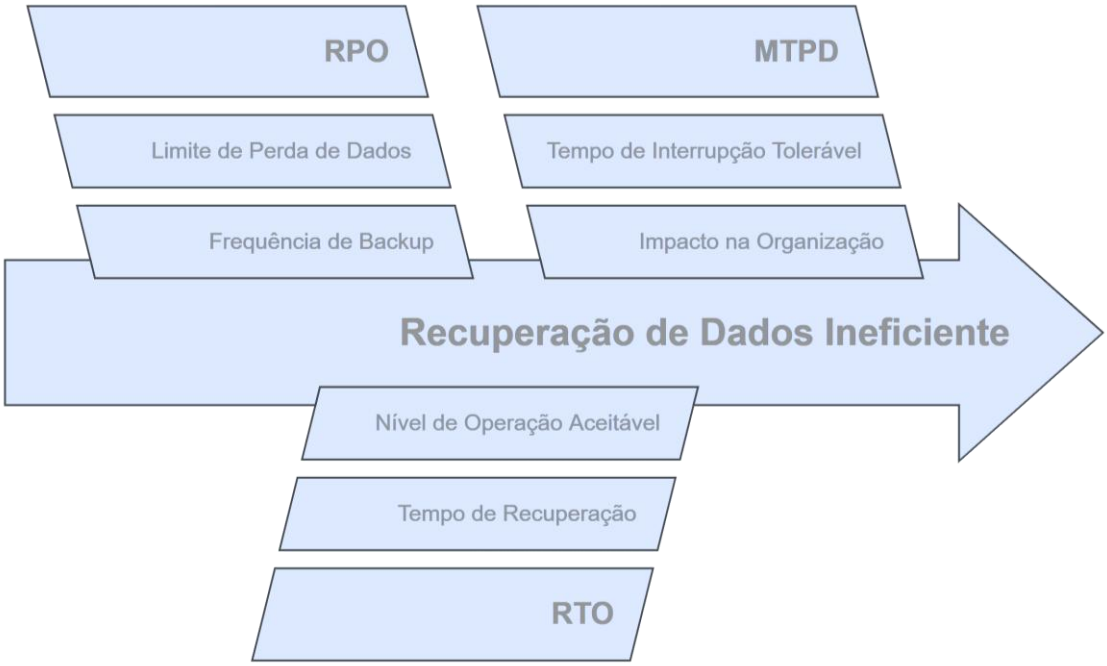

Figura 5 – MTPD/RTO/RPO.

No contexto da análise de impacto no negócio, existe uma ferramenta que ajuda a classificar e a avaliar o impacto que determinada interrupção pode causar nas organizações, sendo ela a escala de impacto.

A escala de impacto deve ser definida em concordância com o perfil de risco da organização e é utilizada para determinar o grau de severidade das consequências de eventos disruptivos ao longo de diferentes períodos de interrupção. Permite, assim, definir uma *baseline* de comparação dos diferentes processos.

As categorias de impacto na Tabela 2 são definidas segundo as boas práticas para implementação de um PCN. Em particular, seguindo a norma ISO 22301 e demais literatura sobre o tema.

Tabela 2 – Categorias de impacto.

Tipo	Descrição
Financeiro	Redução de fundos, lucros perdidos, aumento dos custos operacionais, penalizações ou multas
Reputacional	Afetam a opinião pública da organização e podem manifestar-se através de uma opinião negativa
Operacional	Extensão e duração da interrupção do fluxo das operações de negócio.
Saúde e Segurança	Fatores físicos e/ou ambientais que afetam negativamente a saúde e segurança dos colaboradores
Serviço Público	Atrasos nos serviços prestados
Objetivos de Negócio	Falha em cumprir objetivos ou em tirar vantagem de oportunidades de negócio.

A escala de impacto é geralmente composta por níveis que refletem o grau de impacto que uma interrupção pode causar. De forma a exemplificar esta prática, foram aplicados níveis de 1 (baixo) a 5 (severo) às categorias anteriormente indicadas. O resultado deste cruzamento é apresentado de seguida na Tabela 3.

Tabela 3 – Escala de impacto.

Nível	Financeiro	Reputacional	Operacional	Saúde e Segurança	Serviço Público	Objetivos de Negócio
1. Baixo	Sem impacto significativo no orçamento.	Sem impacto na imagem pública ou interna.	Pequena interrupção.	Sem risco para os colaboradores.	Sem impacto nos cidadãos.	Sem alterações nos objetivos de negócio.
2. Ligeiro	Pequenas perdas financeiras, que são facilmente recuperáveis.	Impacto interno limitado.	Alguma disrupção, onde os processos podem ser retomados com ajustes mínimos.	Sem consequências graves para os colaboradores.	Impacto reduzido, como atrasos pontuais nos serviços prestados ao público.	Ajustes mínimos nos objetivos estratégicos ou prazos.
3. Moderado	Perda financeira relevante, impactando resultados do período.	Danos na reputação da organização, críticas em redes sociais ou media social.	Interrupção de serviços essenciais, exigindo um plano de contingência.	Risco moderado para a saúde e segurança.	Serviços públicos muito afetados, causando reclamações e insatisfação.	Ajustes significativos nos objetivos e prioridades do negócio.
4. Elevado	Grande prejuízo financeiro, com impacto direto na sustentabilidade da organização.	Notícia negativa amplamente divulgada, perda de confiança dos *stakeholders*.	Paralisação total de operações críticas, sem soluções imediatas.	Risco elevado para a saúde e segurança, podendo causar ferimentos graves.	Serviços públicos comprometidos, com impacto direto na vida dos cidadãos.	Metas estratégicas severamente comprometidas, necessidade de reestruturação.
5. Severo	Perdas financeiras massivas, risco de insolvência ou falência.	Danos irreparáveis à reputação, perda de clientes e parceiros estratégicos.	Colapso total das operações, impossibilidade de recuperação a curto prazo.	Risco extremo para a saúde e segurança, com potenciais fatalidades.	Serviços públicos inoperacionais, crise generalizada na população.	Objetivos do negócio inatingíveis, necessidade de redefinição total da estratégia.

4.3 Gestão de Riscos

A gestão dos riscos envolve a identificação e avaliação de riscos que possam afetar a continuidade das operações, com a implementação de medidas de mitigação.

O sistema de gestão de risco deve ser definido de acordo com a maturidade e expectativas que a organização tem do risco (IRM, 2002).

Segundo Silva (2016) e, de acordo com o *standard* de Gestão de Risco do Institute of Risk Management (IRM) a avaliação de cada risco possibilita a sua identificação e categorização, permitindo assim estimar a probabilidade de ocorrência e consequência do seu impacto na organização.

É avaliado de acordo com as categorias estabelecidas pela organização tendo em conta vários fatores, como económicos, sociais, ambientais, restrições legais, interesses das partes interessas, entre outros. Deste modo, a organização fica ciente dos riscos existentes e da forma como cada um desses riscos deve ser tratado ou aceite (Silva, 2016).

Adotar estratégias preventivas, desencadeadas *à priori* e, reativas, *à posteriori* de um evento disruptivo, só é possível através de um planeamento antecipado por parte da organização, permitindo assim a mitigação dos impactos decorrentes de um risco a que se encontra exposta (Silva, 2016).

4.4 Plano de Recuperação de Desastres

Os planos de recuperação de desastres, ou *Disaster Recovery Plan* (DRP), segundo Kesa, D. M. (2023) são um componente crucial da gestão de continuidade de negócio.

Este tipo de planos permite uma resposta estruturada e predefinida para lidar com eventos catastróficos ou desastres que possam interromper as operações das organizações. Esses eventos podem variar entre desastres naturais, ciberataques, falhas de infraestrutura dos sistemas críticos, entre outros (Kesa, 2023).

Os planos de recuperação de desastres envolvem a definição de procedimentos detalhados, a alocação de recursos e a implementação de medidas de restauro, permitindo

que as organizações continuem o seu funcionamento habitual, com o mínimo possível de interrupções.

Segundo Kesa, D. M. (2023), um DRP pode envolver configurar *hardware* de forma redundante, redes e componentes de infraestrutura para assumirem automaticamente o controlo em caso de falha, minimizando o tempo de inatividade e garantindo um serviço ininterrupto.

Já os *backups* e a recuperação de dados requerem bases de dados robustas, devendo existir procedimentos que garantam a proteção de dados críticos e que permitam que os mesmos sejam restaurados em caso de perda ou corrupção de dados. Estes procedimentos devem incluir *backups* regulares, armazenamento externo e testes do processo de recuperação para garantir a integridade e disponibilidade dos dados (Kesa, 2023).

A aplicação dos planos de recuperação de desastres permite às organizações recuperar a funcionalidade dos seus sistemas. É, no entanto, necessário assegurar a disponibilidade das dependências dos diferentes sistemas, de forma a garantir que a recuperação é efetiva e que está assegurada a consistência dos dados.

Em organizações para as quais os vários ativos e infraestruturas são assegurados por fornecedores externos, o envolvimento destes é essencial para a correta implementação de um DRP.

5. Metodologia

Atendendo à necessidade de as organizações manterem os seus planos constantemente atualizados, este trabalho de investigação inicia-se com uma revisão multivocal de literatura uma vez que se pretendem identificar as melhores práticas a elaboração destes mesmos planos.

A abordagem que se propõe seguir assenta na *Action Research* (AR), permitindo ao investigador interagir diretamente com o fenómeno em estudo, por ser flexível ao longo do processo de desenvolvimento (Saunders et al. 2019). Aumenta, igualmente, a probabilidade de aceitação e implementação das soluções propostas. No âmbito do AR, e para efeitos de recolha de dados, para além de se antecipar que será necessário solicitar documentação no decorrer da investigação, irá recorrer-se a entrevistas semiestruturadas para recolher informação junto dos participantes.

A metodologia AR tem vindo a evoluir havendo diferentes versões que são melhor aplicáveis em diferentes contextos. No âmbito do desenvolvimento da presente Dissertação optou-se pela elaboração do ciclo Investigação-ação canónica, CAR, visto ser uma abordagem especialmente útil para o desenvolvimento e a implementação de planos de continuidade de negócio por ser possível combinar diagnóstico, planeamento, ação e avaliação num ciclo iterativo.

5.1 Revisão Multivocal de Literatura

A revisão de literatura é uma etapa fundamental da pesquisa académica, existindo várias metodologias para ir ao encontro desta necessidade, sendo que compreender as particularidades de cada abordagem é essencial não apenas para os investigadores, mas também para revisores e editores.

Para orientar o tema em estudo, irá recorrer-se a uma Revisão Multivocal de Literatura (MLR) que inclui, não só, a Literatura Formal (*Systematic Literature Review*, SLR) como também a Literatura Cinzenta (*Grey Literature* – GL), (Brites, 2022), conforme representado na Figura 6.

A Literatura Cinzenta, representada na Figura 6, refere-se a materiais e pesquisas produzidos fora dos canais tradicionais de publicação académica, abrangendo uma ampla gama de formatos como *blogs*, páginas *web*, teses, dissertações e vídeos.

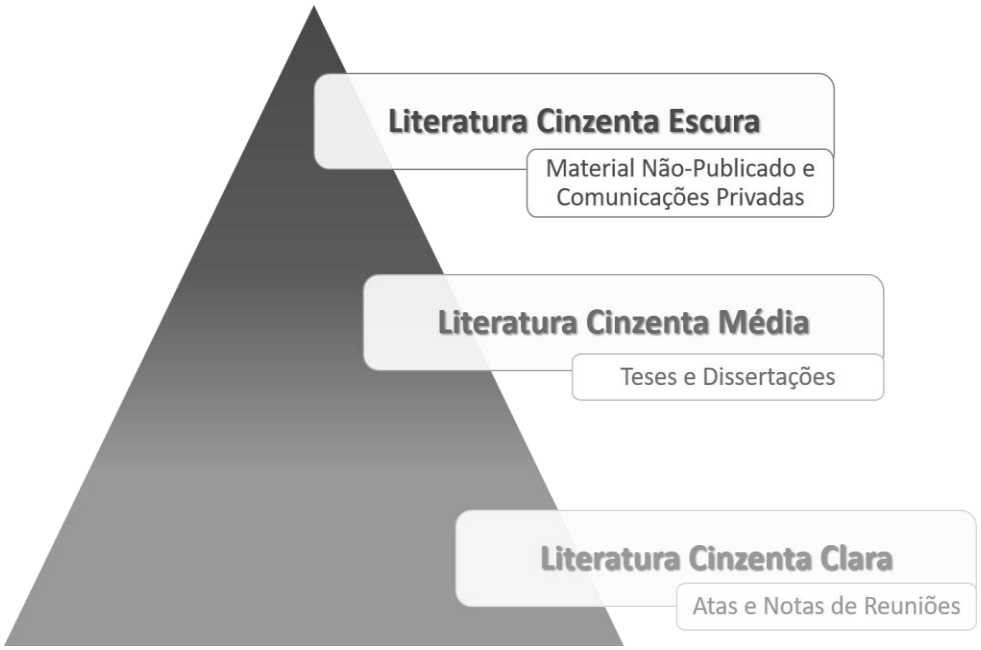

Figura 6 – Literatura Cinzenta (adaptado de Brites, 2022).

As MLRs têm uma importância relevante para a expansão da pesquisa, pois fecham as lacunas entre estudos académicos e de investigação e as atuais práticas profissionais, e até porque a Literatura Cinzenta se tem tornado bastante comum para estudos académicos que tocam nas áreas de Engenharia de Software (Neto et al. 2019).

5.2 Abordagem Metodológica

A abordagem metodológica proposta para a realização desta dissertação passará pelas várias áreas do Ciclo de AR, representado na Figura 7 de "Planear, Atuar, Observar e Refletir".

A essência desta metodologia passa pela Investigação-Ação, sendo um processo emergente e iterativo de investigação que se destina a desenvolver soluções para problemas organizacionais reais através de uma abordagem participativa e colaborativa.

Aqui, são utilizadas diferentes formas de conhecimento que têm implicações tanto para os participantes como para a própria organização (Saunders et al. 2019).

Uma estratégia de AR inicia-se num contexto específico e com uma pergunta de pesquisa. Por sua vez, funciona através de várias etapas ou iterações, pelo que o foco da pergunta pode ser alterado à medida que a pesquisa se vai desenvolvendo.

Cada uma das etapas envolve um processo de diagnóstico ou construção de questões, seguindo-se o planeamento de ações, a tomada de ação e as respetivas avaliações das mesmas. Desta forma, promove-se uma aprendizagem organizacional e resultados práticos através da identificação de problemas (Saunders et al. 2009).

A operacionalização da GCN passa pela identificação das tarefas críticas de uma organização do setor da Justiça e pela definição de critérios para a ativação do PCN.

Figura 7 – Ciclo Action Research (adaptado de Action Research in Teaching and Learning | Western Sydney University, 2025).

Dentro desta abordagem metodológica, são identificadas várias formas de AR, tendo esta dissertação por base a Investigação-ação Canónica (*Canonical Action Research* – CAR).

Davison, R., Martinsons, M. G., & Kock, N. (2004) definem o processo de Investigação-ação Canónica (CAR) como um dos mais praticados dentro das várias formas de AR na literatura dos SI.

Por ser iterativo, rigoroso e colaborativo, envolve foco tanto a nível do desenvolvimento organizacional quanto na conceção de conhecimento.

A sua característica iterativa envolve um processo cíclico, com a realização de um ou mais ciclos de atividades que são projetados para resolver os problemas do meio organizacional.

O rigor do CAR tem dois componentes principais. O primeiro, iterando ciclos de atividades cuidadosamente planeados e executados, para que os investigadores consigam desenvolver uma imagem cada vez mais detalhada da situação crítica e, ao mesmo tempo, definir a melhor solução para o problema identificado.

Em segundo lugar, ao envolver-se num processo contínuo de resolução dos problemas, as atividades planeadas devem ser sempre relevantes para o problema tal como é atualmente compreendido. Esta relevância torna-se assim uma componente essencial do rigor no CAR, representado na Figura 8.

Por fim, a sua característica colaborativa implica que tanto os investigadores como as organizações trabalhem juntos, sendo que não sugere que os investigadores dominem todo o processo.

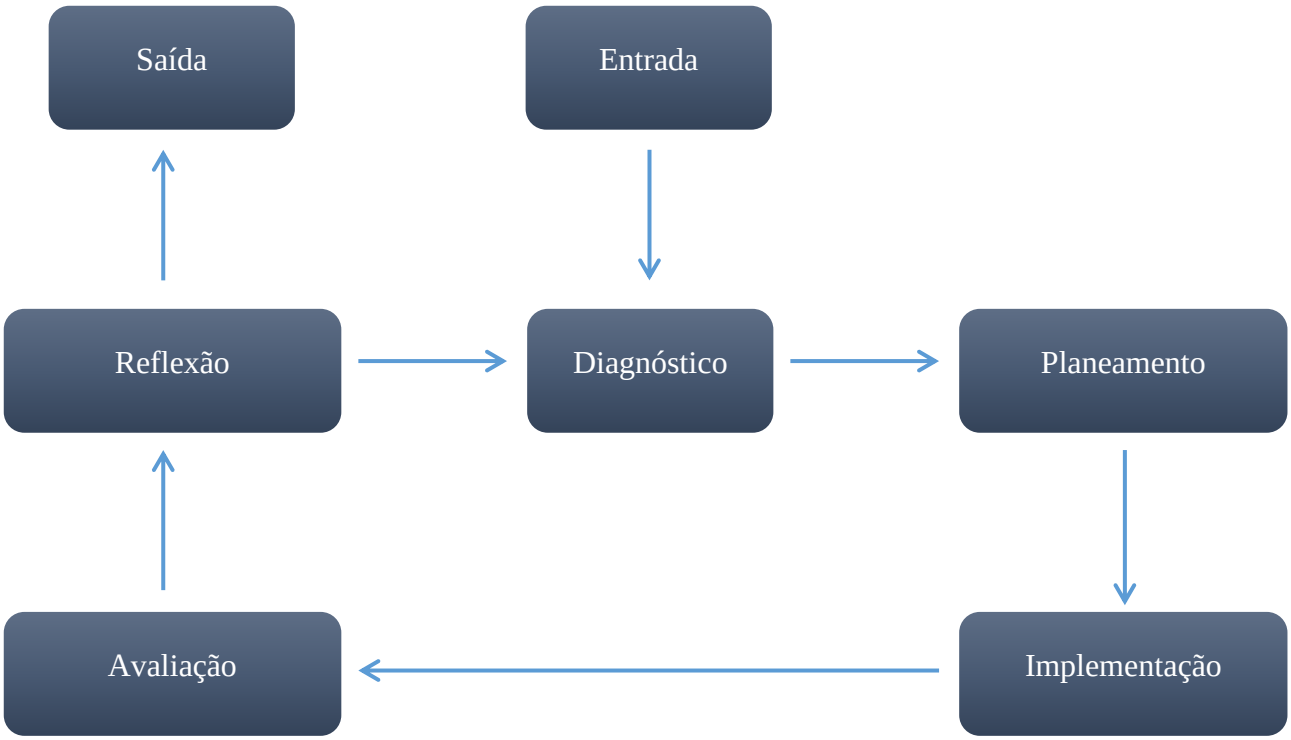

Figura 8 – Canonical Action Research (adaptado de Principles of canonical action research (Davison et al., 2004)).

5.3 Entrevistas semiestruturadas

As entrevistas podem ser classificadas em diferentes tipos, como estruturadas, semiestruturadas e a não estruturadas (Saunders et al., 2019).

Segundo Saunders et al. (2019), as entrevistas estruturadas podem ser realizadas através de questionários preenchidos pelo investigador, enquanto entrevistas semiestruturadas e não estruturadas são "não padronizadas".

Desta forma, enquanto as entrevistas estruturadas se baseiam em questões padrão e as não estruturadas em questões de total liberdade para as conduzir, as entrevistas semiestruturadas assentam na combinação das duas categorias mencionadas. Quem realiza entrevistas semiestruturadas segue uma linha de raciocínio com questões pré-determinadas e, possivelmente, algumas perguntas-chave relacionadas com os temas desejados, para orientar a condução de cada um (Lima, 2016; Saunders et al. 2019).

As entrevistas serão, então, utilizadas para recolher dados que existam à data numa organização enquadrada no setor da Justiça. Será a base para efetuar estudos interpretativos e o principal objetivo passa por recolher informação detalhada sobre o PCN atual existente nessa mesma organização de modo a que seja possível detalhar as maiores lacunas para que o PCN aqui sugerido vá ao encontro de as colmatar.

6. Canonical Action Research

6.1 Entrada

O desenvolvimento da presente Dissertação vem no seguimento de uma dupla motivação: sendo a primeira a de realizar investigação focada na área de Gestão da Continuidade de Negócio, e a segunda, com origem numa entidade no setor público da Justiça, que requer evoluir na forma como aborda o tema da continuidade de negócio.

Relativamente à primeira motivação são de salientar a questões subjacentes à investigação já previamente identificadas, nomeadamente:

> Questão 1: Como implementar um Plano de Continuidade de Negócio no setor da Justiça, seguindo *standards* internacionais e boas práticas de gestão de serviços de TI e *Governance*?

> Questão 2: Como garantir a recuperação de desastres no setor da Justiça?

Tal como mencionado em capítulos anteriores, a GCN preocupa-se em garantir o desempenho sustentado de produtos/serviços críticos a um nível aceitável e em recuperar os processos de negócio dentro de prazos toleráveis, evitando, assim, interrupções que possam resultar em consequências negativas inaceitáveis.

Tendo em conta estes potenciais benefícios, o organismo em causa demonstrou todo o seu interesse em colaborar neste trabalho, sendo o objetivo da entidade em causa estabelecer o sistema de GCN como parte integrante das suas atividades e cultura institucional.

Por forma a dar início ao ciclo mencionado anteriormente, é igualmente importante evidenciar os principais fatores que a entidade identificou como motivação para o desenvolvimento de um processo de GCN, que se encontram representados na Tabela 4. Estes fatores motivacionais foram identificados pelo organismo no decorrer das atividades executadas e análise das mesmas, tendo sido encontradas diversas lacunas que necessitam ser colmatadas.

Tabela 4 – Principais fatores motivacionais para o organismo.

Fatores	Descrição
Melhorar a resiliência do organismo	Reduzindo a probabilidade de interrupção de serviços e processos críticos
Reduzir o tempo de interrupção	Permitindo que o organismo recupere rapidamente e mantenha os serviços mínimos disponíveis
Mitigar os impactos das interrupções	Proteger a reputação e a imagem do organismo, inspirando confiança entre as partes interessadas, bem como possíveis perdas financeiras
Garantir a disponibilidade de recursos	Recursos humanos, tecnologias, instalações e suprimentos para a recuperação
Garantir a segurança e o bem-estar	Colaboradores, fornecedores, clientes e qualquer parte interessada
Garantir a conformidade com as leis	Regulamentos e normas do setor

6.2 Diagnóstico

O principal objetivo da fase de diagnóstico consiste na confirmação dos objetivos que motivam o CAR. Adicionalmente também a identificação dos componentes necessários à elaboração do PCN, bem como para um *Disaster Recovery Plan* (DRP).

Tendo em conta que a estratégia, inserida no Plano de Recuperação e Resiliência (PRR) (Governo Digital, 2024), tem como finalidade tornar a AP mais integrada, funcional e eficiente na realização dos serviços públicos, através das tecnologias digitais, existem cada vez mais riscos associados, principalmente tendo em conta a quantidade de digitalização, bem como a quantidade de serviços prestados ao cidadão por meios eletrónicos.

Por esta razão, foi definido como interveniente da entrevista, o Diretor do Departamento Tecnológico, doravante identificado como DDT, sendo igualmente relevante por inerência das suas funções, considerando-o o ponto de contacto mais importante. A sua contribuição permitiu uma visão multidimensional do que existe atualmente a nível do Plano de Continuidade de Negócio no organismo, que se mantém anónimo.

Para a recolha de dados inicial que suporta a fase de diagnóstico, foi realizada uma entrevista, seguindo um *script* realizado para o efeito, acessível no Apêndice 1, tendo sido essencial para apurar o estado de maturidade do organismo.

O DDT frisou que *"(...) existe constantemente a preocupação das operações do nosso dia-a-dia, mas a principal dificuldade é termos a capacidade de refletir sobre algo que possa vir a acontecer e por essa razão a GCN não pode ficar sempre para segundo plano."*

No decorrer da entrevista, foi também disponibilizada documentação elaborada por uma entidade externa com grande parte do levantamento do plano atualmente em vigor. Deste modo, foi feito o levantamento da documentação existente à data para servir de complemento à entrevista anteriormente realizada.

De acordo com a informação recolhida na entrevista, é objetivo da entidade que o processo da GCN abranja ainda as atividades descritas na Tabela 5:

Tabela 5 – Componentes do processo de GCN relevantes para o organismo.

Componentes	Descrição
Planeamento e controlo operacional	Concentrando os maiores esforços nas áreas que têm o maior impacto na sua operação e garantindo que as medidas de recuperação são adaptadas às necessidades específicas de cada processo
Análise de impacto de negócio	Identificar e avaliar os impactos de possíveis eventos disruptivos nos processos do organismo, priorizando processos críticos e requisitos de recuperação
Avaliação de risco	Identificar e avaliar riscos que possam afetar a continuidade das operações/serviços, com a implementação de medidas de mitigação
Estratégia de continuidade de negócios	Planos de alto nível para manter operações críticas em cenários de risco.
Estabelecer e implementar PCN	Detalhar a aplicação das estratégias, com procedimentos, responsabilidades e recursos
Realização de testes	Simular cenários de crise e avaliam a eficácia dos planos
Avaliação	Avaliar e melhorar continuamente os planos e as estratégias de continuidade

Implementar um PCN neste organismo público exige um esforço coordenado para assegurar que os serviços essenciais continuem a funcionar durante crises, tendo em conta o papel crítico do setor da Justiça na sociedade, já que disponibiliza serviços públicos indispensáveis às necessidades dos cidadãos.

Por essa razão, identificada no decorrer da entrevista inicial, o PCN deve garantir que qualquer tipo de interrupção seja minimizado, garantindo a proteção de acesso à justiça bem como a integridade dos processos legais.

Da análise do plano atual foram identificadas oportunidades de melhoria relevantes e até algumas lacunas a serem corrigidas. Foi elaborado um plano em conjunto com o organismo que foi resumido como consta na Tabela 6.

Tabela 6 – Melhorias e lacunas a colmatar para um PCN de sucesso.

Melhorias	**Descrição**
1.Equipa de continuidade de negócio	Identificar os intervenientes e definir funções e responsabilidades
2.Análise de impacto de negócio (BIA)	Identificar processos críticos, avaliando o impacto de possíveis interrupções para que sejam estabelecidas prioridades
3.Análise de riscos	Identificar as principais ameaças e avaliar o nível de impacto
4.Estratégias de continuidade	Identificar estratégias que garantam a continuidade de serviços aquando da existência de eventos disruptivos
5.Elaborar o plano documentado	Identificar objetivos, definir planos de resposta e estratégias de recuperação de desastres
6.Testar o plano com regularidade	Efetuar simulações para avaliar a eficácia do plano e identificar falhas para que este seja atualizado e reajustado regularmente
7.Sensibilizar e formar	Efetuar ações de sensibilização e formação para todos os colaboradores
8.Monitorizar e atualizar o plano	Avaliar e atualizar o plano de forma contínua

No Anexo 1 é demonstrada a priorização de riscos utilizada à data pelo organismo.

Tanto no decorrer da entrevista como detetado na documentação acedida, foi evidenciada a necessidade de garantir a recuperação de desastres no setor. O DDT salientou a importância da existência de um DRP de modo a permitir que o organismo retome as suas operações com a maior brevidade possível.

Consequentemente, de acordo com o *standard* de Gestão de Risco do *IRM* e em concordância com o DDT por parte do organismo, procedeu-se à identificação de estratégias de continuidade de negócio, representadas na Tabela 7.

Tabela 7 – Estratégias de continuidade de negócio.

Estratégias de continuidade de negócio	
Preventiva	Tratamento dos riscos, que permitam proactivamente minimizar o risco associado ao acontecimento das ameaças identificadas, minimizando a probabilidade de ocorrência ou os próprios impactos originados
Reativa	Estratégias de recuperação que permitam aplicar uma resposta adequada a disrupções e recuperar os seus processos críticos, limitando o impacto temporal

6.3 **Planeamento**

Com base no diagnóstico realizado na fase anterior, foram identificadas as atividades e os intervenientes no horizonte temporal, representado na Figura 9, de forma a que seja implementado o PCN de acordo com os objetivos do organismo.

A primeira atividade pressupõe formar uma Equipa de Continuidade de Negócio, cujos colaboradores serão responsáveis pela elaboração, implementação, manutenção e ativação do PCN.

Com a Identificação de Riscos, o intuito passa por identificar as possíveis ameaças que possam afetar a continuidade de negócio do organismo em causa.

Na terceira atividade, a BIA, o objetivo será avaliar os impactos de possíveis interrupções para definir a criticidade de cada processo, bem como o tempo máximo tolerável de interrupção (RTO/RPO).

De seguida, com a Análise de Riscos pretende-se apurar a probabilidade e o impacto dos riscos identificados na segunda atividade. Esta análise complementa a BIA com foco na vulnerabilidade e nos controles existentes.

Concluindo as atividades anteriormente descritas, é indispensável a definição de ações e soluções que serão adotadas para garantir a continuidade dos processos críticos durante e após uma interrupção, garantindo que o organismo tem as suas próprias Estratégias de Continuidade bem delineadas.

Por fim, e como última atividade para o PCN, serão identificados Possíveis Cenários de Interrupção, com o intuito de simular situações reais ou prováveis de ocorrerem, testando assim a eficácia do plano.

Na Figura 9 destacam-se ainda as atividades para garantir a existência de um plano de recuperação de desastres no setor, em coordenação com o organismo, respondendo aqui à segunda questão mencionada na fase de Entrada do CAR

A lista de ativos é uma atividade fulcral para que sejam identificados e assinalados todos os ativos de TI que precisam ser protegidos e/ou recuperados em caso de cenários desastrosos.

Como segunda atividade para o DRP, será fundamental identificar quais os ativos críticos e respetivos objetivos do organismo, como identificar o RTO (tempo de recuperação) e o RPO (ponto de recuperação) para cada um.

Definir funções e responsabilidades é igualmente importante, dado que garante que todos os colaborados saibam as suas responsabilidades durante a execução do DRP.

Posteriormente, será necessário documentar os procedimentos para que seja criada a sequência das ações técnicas e operacionais que permitirão recuperar os serviços após um incidente disruptivo.

Não menos importante é a criação de um plano de comunicação, por forma a que seja estabelecido de que modo e com que intervenientes o organismo terá de comunicar durante e após um incidente.

A sexta e penúltima atividade para este DRP, passa por assegurar a existência de *backups* atualizados e efetuados de forma segura e acessível, para que sejam restaurados com a maior brevidade possível quando necessário.

Por fim, o plano tem de ser formalizado, com aprovação superior, de modo a garantir que esteja alinhado com as políticas corporativas e seja testado e atualizado regularmente.

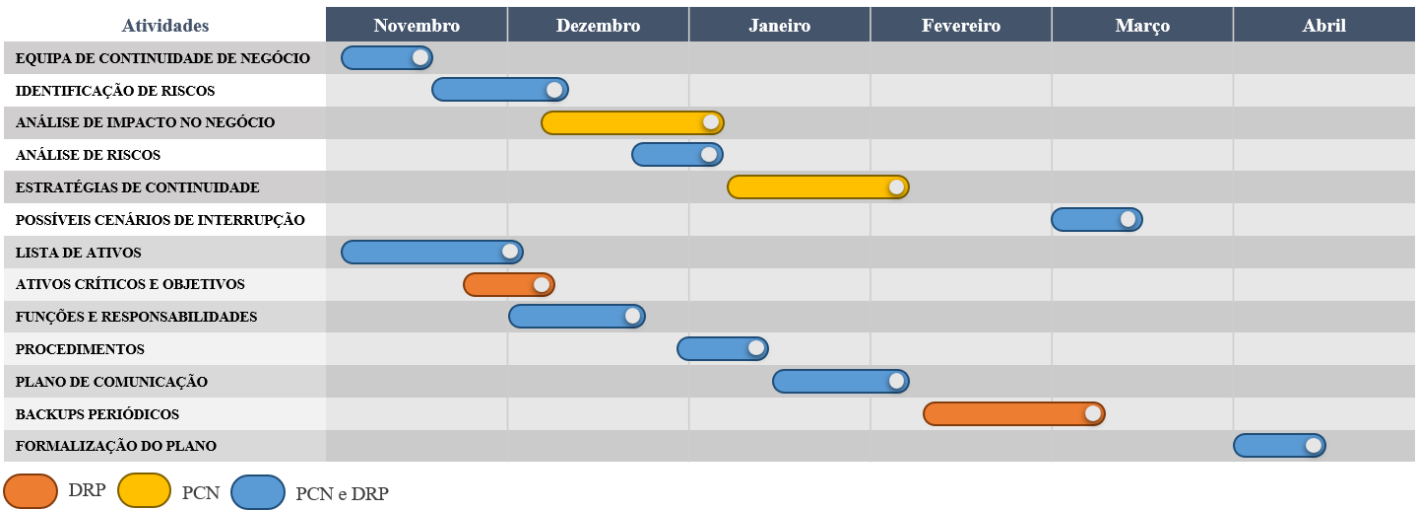

Figura 9 – Plano de atividades para o PCN e o DRP.

6.4 Implementação

6.4.1 Plano de Continuidade de Negócio

De acordo com o planeamento efetuado na fase anterior, o objetivo é implementar um PCN num organismo público, seguindo as boas práticas e indo ao encontro dos objetivos de negócio do mesmo.

6.4.1.1.Equipa de Continuidade de Negócio

No decorrer da entrevista foi evidenciada a extrema necessidade de ser criada uma Equipa de Continuidade de Negócio interna, de forma a garantir que a documentação seja constantemente atualizada, indo ao encontro do descrito anteriormente na Tabela 6.

Para a constituição desta equipa, tornou-se essencial proceder à identificação dos colaboradores detentores de um conhecimento mais abrangente e transversal dos processos de negócio em vigor no organismo. Esta identificação permitiu a atribuição clara de funções e responsabilidades, especificamente delineadas para contextos de disrupção que possam comprometer a continuidade das operações.

Deste modo, foram definidas as seguintes responsabilidades tendo em conta o que o organismo considera crucial os colaboradores da equipa terem e, em particular, seguindo as boas práticas da norma ISO 22301:

1. Colaborar ativamente com as equipas operacionais, gestão de ativos e gestão de infraestruturas de modo a apurar o estado atual do negócio, os seus riscos e respetivas dependências;
2. Definir objetivos e estratégias;
3. Desenvolver e implementar a infraestrutura e as capacidades organizacionais da GCN de acordo com as estratégias definidas;
4. Garantir que a GCN estará alinhada com as necessidades e requisitos do organismo, bem como com as melhores práticas, normas e regulamentos relevantes;
5. Desenvolver e manter atualizada a documentação de suporte à GCN;
6. Sensibilizar e assegurar que a GCN seja desenvolvida e mantida em todas as áreas;

7. Planear e coordenar testes à GCN, garantindo o envolvimento de todos os intervenientes necessários;
8. Incorporar a GCN como parte integral da gestão do risco;
9. Manter-se atualizado sobre as tendências e desenvolvimentos na área de continuidade de negócio, procurando oportunidades de melhoria contínua e inovação.

6.4.1.2.Identificação de Riscos

Através do levantamento e análise detalhada dos processos de negócio existentes no organismo, foi possível identificar um conjunto de riscos com potencial impacto significativo na continuidade das suas operações.

Este diagnóstico permitiu igualmente a definição de categorias de impacto adaptadas à realidade institucional, assim como o cálculo de métricas relevantes para aferir a criticidade dos processos e a respetiva tolerância à interrupção.

No âmbito desta análise, foram identificados os principais riscos associados aos processos de negócio, em coordenação com o organismo, definidos na Tabela 8:

Tabela 8 – Riscos identificados nos processos de negócio.

Riscos
1.Dependência de recursos humanos
2.Inexistência de processos e procedimentos formalizados e desenhados
3.Inexistência de planos de comunicação
4.Ciberataques

No que respeita ao primeiro risco identificado, verificou-se uma elevada dependência de colaboradores detentores de conhecimento técnico e operacional especializado e não documentado (conhecimento tácito versus conhecimento explícito, ou sejam devidamente documentado), o que representa um risco acrescido em caso de ausência prolongada ou saída desses elementos, comprometendo a continuidade operacional a vários níveis.

A inexistência de processos e procedimentos formalizados e desenhados limita a capacidade de resposta estruturada em cenários de disrupção, dificultando a recuperação célere e coerente das atividades essenciais.

A falta de planos de comunicação para situações de crise pode originar falhas na transmissão de informação, tanto internamente como com as restantes partes interessadas, agravando os efeitos de qualquer interrupção significativa.

Por fim, considerando o contexto digital e a crescente dependência de infraestruturas tecnológicas, os ciberataques foram identificados como uma ameaça transversal, com potencial para comprometer a integridade, confidencialidade e disponibilidade dos sistemas de informação e dados institucionais.

A identificação destes riscos constituiu uma etapa fundamental para o desenvolvimento do Plano de Continuidade de Negócio, assegurando que as estratégias de mitigação e os procedimentos de resposta são adequados à realidade e aos desafios específicos do organismo.

6.4.1.3.Análise de Impacto no Negócio

Após a identificação dos ricos, procedeu-se ao desenvolvimento da Análise de Impacto no Negócio (BIA) e da Avaliação de Riscos. Estas etapas permitiram identificar os ativos e processos críticos, bem como os potenciais riscos associados à sua interrupção.

Importa referir que os níveis de impacto foram classificados da seguinte forma:

1. Baixo
2. Ligeiro
3. Moderado
4. Elevado
5. Severo

De acordo com a na Tabela 2, da secção 3.2, foi realizada a BIA referente aos riscos associais, conforme demonstrado na Tabela 9, onde:

- R1 = Risco 1 (Dependência de recursos humanos)

- R2 = Risco 2 (Inexistência de processos e procedimentos formalizados e desenhados)
- R3 = Risco 3 (Inexistência de planos de comunicação)
- R4 = Risco 4 (Ciberataques)

Tabela 9 - Análise de Impacto de Negócio

Categorias de Impacto	**Descrição**	**Nível de Impacto**
Financeiro	R4. Custos com recuperação, sanções ou perdas	Moderado
Reputacional	R1. Perceção de fragilidade organizacional	Ligeiro
	R3. Comunicação ineficaz pode gerar alarme público	Elevado
	R4. Perda de confiança por parte do público	Severo
Operacional	R1. Interrupção de tarefas críticas em caso de ausência prolongada	Elevado
	R2. Desorganização na resposta a incidentes ou falhas	Elevado
	R3. Falhas na coordenação de resposta	Elevado
	R4. Interrupção total ou parcial dos sistemas	Severo
Serviço Público	R1. Atrasos no atendimento e tratamento de processos	Elevado
	R2. Respostas inconsistentes aos cidadãos	Moderado
	R3. Informação desencontrada ou em atraso para utilizadores	Moderado
Político/Legal	R4. Demissões políticas ou incumprimento de obrigações legais	Severo
Objetivos de Negócio	R1. Comprometimento de metas de desempenho	Elevado
	R2. Ineficiência no cumprimento de prazos e metas	Moderado

6.4.1.4.Análise de Riscos

Afetando a continuidade dos processos de negócio do organismo, os quatro principais riscos foram avaliados, em concordância com o próprio organismo, da seguinte forma:

R1 – Dependência de Recursos Humanos

- Probabilidade: Alta
- Impacto: Elevado
- Classificação: Risco Crítico

R2 – Inexistência de Processos e Procedimentos Formalizados e Desenhados

- Probabilidade: Alta
- Impacto: Elevado
- Classificação: Risco Crítico

R3 – Inexistência de Planos de Comunicação

- Probabilidade: Média
- Impacto: Elevado
- Classificação: Risco Alto

R4 – Ciberataques

- Probabilidade: Alta
- Impacto: Severo
- Classificação: Risco Crítico

6.4.1.5.Estratégias de Continuidade

Com o objetivo de assegurar a resiliência organizacional e garantir a continuidade das operações críticas, foram delineadas estratégias específicas para mitigar

os riscos previamente identificados. Foram, portanto, adotadas as seguintes medidas de mitigação considerando os riscos identificados:

R1 – Dependência de Recursos Humanos

- Documentação de processos críticos, permitindo que o conhecimento organizacional seja preservado e acessível;
- Definir planos de sucessão para funções indispensáveis, assegurando a substituição eficaz de recursos em caso de ausência;
- Optar pela capacitação cruzada entre as equipas, de forma a distribuir competências entre colaboradores e reduzir vulnerabilidades relacionadas com a centralização do conhecimento.

R2 – Inexistência de Processos e Procedimentos Formalizados e Desenhados

- Elaborar manuais operacionais, abrangendo as tarefas cruciais referentes aos principais serviços prestados;
- Desenhar um plano de formação contínua, assegurando que todos os colaboradores compreendem e aplicam corretamente os procedimentos estabelecidos.

R3 – Inexistência de Planos de Comunicação

- Criar um plano de comunicação de crise, que definirá os fluxos de informação interna e externa, os canais a utilizar e os responsáveis pela sua ativação;
- Definir canais oficiais;
- Realizar treinos de forma a garantir mensagens claras, coerentes e atempadas em cenários de crise.

R4 – Ciberataques

- Implementação de *firewalls* robustas;
- Realização de *backups* periódicos;

- Criação de um plano de resposta a incidentes de cibersegurança;
- Criação de um plano de sensibilização e formação em cibersegurança, direcionado a todos os colaboradores, promovendo uma cultura de segurança digital.

6.4.1.6.Possíveis Cenários de Interrupção

No seguimento dos pontos acima elencados, foram então identificados potenciais cenários de interrupção, representados na Tabela 10.

Tabela 10 – Potenciais cenários de interrupção.

Potenciais cenários de interrupção
1. Interrupção de tarefas críticas em caso de ausência prolongada
2. Desorganização na resposta a incidentes ou falhas
3. Falhas na coordenação de resposta
4. Interrupção total ou parcial dos sistemas

Deste modo, evidenciam-se todos os processos da fase de implementação na Figura 10

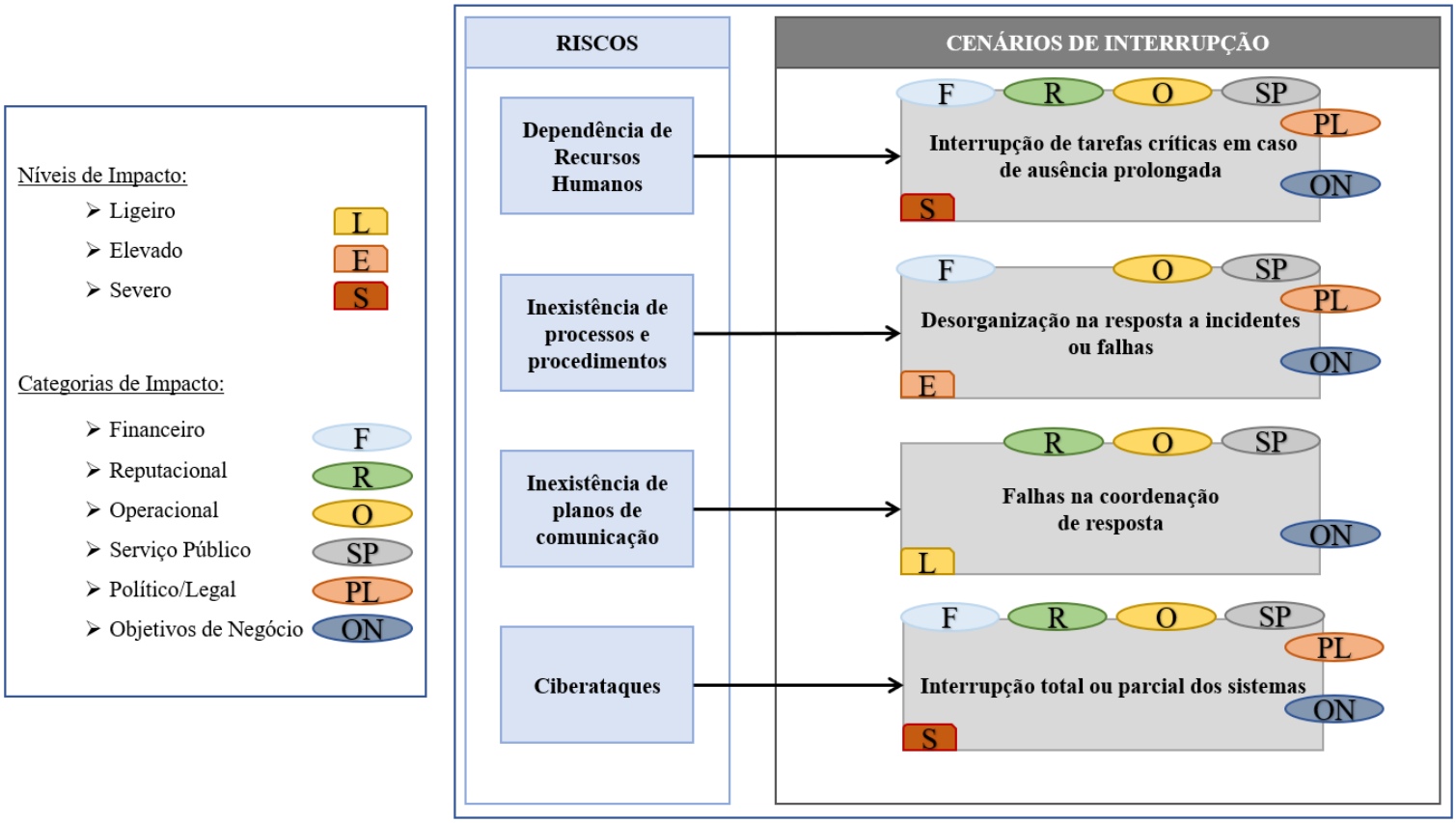

Figura 10 - Fase de implementação do PCN.

6.4.2 Plano de Recuperação de Desastres

No seguimento da implementação do PCN, resta-nos clarificar de que forma o organismo consegue garantir a recuperação de desastres. Para tal, procedeu-se à elaboração de um DRP com base numa das necessidades identificadas pelo mesmo.

Um exemplo identificado no decorrer das entrevistas, pelo DDT, foca a importância e dificuldade, devido ao enquadramento legal atualmente existente, no que respeita à possibilidade de existirem vários fornecedores para o mesmo contrato.

Isto significa que no atual contexto legal não é possível ter mais que um fornecedor contratualizado, o que resulta que se, por alguma eventualidade, ficar impossibilitado de dar continuidade, não existe garantia externa que outro fornecedor possa assegurar o serviço.

6.4.2.1 Lista de Ativos

Com base na revisão de literatura e sendo essencial conjugar o relacionamento entre os ativos e os serviços prestados para o organismo em questão, foi criada a lista dos seus ativos, implementando-se um *IT Asset Management* (ITAM) normalizado, organizando-os de acordo com a importância de acordo com as necessidades do mesmo.

Neste caso, sem a identificação dos ativos, o organismo não poderia mapear as dependências entre eles. Para cada ativo e para cada relação foram identificados os vários responsáveis e os seus respetivos papéis. Este levantamento é relevante para a criação do *Indentity Access Management* (IAM) que permite aumentar a resiliência e operação do PCN.

Para cada ativo, foi igualmente necessário identificar os fornecedores e respetivas condições de contrato, tendo-se procedido à classificação dos recursos de acordo com os sistemas que seriam afetados em caso de diferentes tipos de desastres, como a indisponibilidade de recursos, de energia e até mesmo de incêndios nos edifícios afetos ao organismo.

6.4.2.2 Apuramento de Ativos Críticos e Objetivos

Com base no levantamento dos ativos e respetivas dependências é possível classificá-los de acordo com os sistemas que seriam afetados, garantido, assim, que sejam estabelecidas as métricas de recuperação, nomeadamente o RTO, o RPO e o MTPD.

6.4.2.3 Funções e Responsabilidades

A partir da identificação dos responsáveis e respetivos papéis, foi elaborada a lista dos intervenientes envolvidos nas operações de recuperação de desastres. Este ponto, elaborado no decorrer do diagnóstico, foi crucial para dar seguimento à definição das suas funções e responsabilidades.

Esta informação foi compartilhada para todo o organismo, seguindo o modelo COBIT, dado ser essencial para garantir que o plano de recuperação de desastres funcione de forma eficiente, já que todos os colaboradores passaram a ter o conhecimento das funções e responsabilidade de cada um.

Contudo, identificaram-se processos com número insuficiente de colaboradores definidos, aumentando o risco em caso de indisponibilidade dos existentes.

Foram, portanto, identificados colaboradores substitutos, garantindo que sempre que determinado colaborador responsável se ausente, exista um colaborador com a mesma formação, documentação e perfil de acesso que seja capaz de executar as suas funções e assumir a responsabilidade de executar o PCN na sua integra, reduzindo o tempo de indisponibilidade e contribuindo para as metas de recuperação definidas.

6.4.2.4 Procedimentos

Para a presente fase do plano, foi elaborada uma lista das infraestruturas e aplicações e as suas dependências para garantir o normal funcionamento do negócio. Esta lista foi criada com base nos resultados da Análise de Impacto nos Negócios (BIA).

A lista foi alimentada consoante a respetiva prioridade, ou seja, tendo em conta quais os ativos que devem ser recuperados em primeiro lugar, detalhando os processos e procedimentos necessários para recuperar cada um deles.

Deste modo, existindo interdependências entre ativos, conseguiram identificar-se, por exemplo, quais os que requeriam que a infraestrutura de rede fosse primeiramente disponibilizada antes de ser possível disponibilizá-los para o exterior.

6.4.2.5 Plano de Comunicação

Considerou-se como requisito obrigatório que, durante um desastre, a comunicação fosse frequentemente efetuada, pelo que foi essencial estabelecer um plano de comunicação e um método alternativo de comunicação em caso de algum tipo de evento disruptivo que impossibilitasse o normal procedimento entre os intervenientes do PCN.

Um plano de comunicação eficaz deve também incluir métodos de contato com as outras partes interessadas, como fornecedores e clientes, pelo que exercícios a este nível são um bom método de testar a precisão do plano de comunicação e manter os colaboradores alerta em caso de situações emergentes.

6.4.2.6 Backups periódicos

Nesta fase, foi evidenciada a importância da existência de soluções alternativas para a continuidade dos serviços, como *backups* a nível da infraestrutura, dos ativos e da comunicação para com os fornecedores, clientes e colaboradores.

Em colaboração com o organismo, o qual referiu que existe uma estratégia de *Cloud* para a Administração Pública portuguesa, aprovada em 2020, com a visão assente na "Adoção da *Cloud* pública, sempre que possível, em modelo inteligente, seguro e eficiente", concluiu-se que a realização de *backups* apenas num local é uma potencial falha e, portanto, desaconselhado.

Consequentemente, será possível efetuarem *backups* tanto localmente como recorrendo a servidores alojados em sites remotos e/ou na nuvem. Assim, os *backups* a terem em consideração incluíram *backups* internos, multi-site, e externos, na *cloud*.

6.4.2.7 Formalização do plano

Após a elaboração do plano de recuperação de desastres, este foi submetido a aprovação superior. Após a validação por parte dos responsáveis, não foram sugeridas retificações ao mesmo, pelo que foi possível avançar para a fase de testes.

Com o PCN e o DRP criados, nos seguintes capítulos serão desenvolvidas as atividades de validação e devida reflexão.

6.5 Avaliação

Após o planeamento e implementação, torna-se crucial apurar a eficácia das ações que foram implementadas, identificando pontos de melhoria ou até mesmo alterações que sejam necessárias aos planos.

6.5.1 Plano de Continuidade de Negócio

No decorrer da implementação do PCN foi obtido o feedback das partes interessadas, no qual indicaram que o PCN em questão segue uma abordagem metodologicamente coerente no que toca às normas nele incluídas.

Está alinhado com os princípios da ISO 22301, no que respeita à Continuidade de Negócio, da ISO 27005, englobando a Gestão de Riscos, e da COBIT, no que toca à Governança de TI, conforme demonstrado na Tabela 11.

Tabela 11 - Enquadramento com normas standard internacionais

Norma	Objetivo	Relevância no PCN
ISO 22301	Gestão da Continuidade de Negócio	Definição de processos críticos e definição de responsabilidades
ISO 27005	Gestão de Riscos	Identificação, avaliação e tratamento dos riscos
COBIT	Governança de IT	Controlo de processos

Vários dos intervenientes, envolvidos na avaliação do plano, indicaram que o PCN segue uma sequência lógica que se inicia com a constituição da equipa de continuidade de negócio, dando seguimento à identificação de riscos, análise de impacto de negócio, avaliação de riscos e definição de estratégias de continuidade, garantindo uma visão integrada de continuidade de negócio.

Na opinião do DDT, a identificação da necessidade de uma equipa de gestão de continuidade interna, bem como a definição das suas responsabilidades, estão bem fundamentadas.

No entanto, referiu que não pode estar limitada apenas à área tecnológica dado que existem diversos departamentos no mesmo organismo e só desta forma será possível garantir que todo o organismo segue uma abordagem de continuidade de negócio.

No que toca aos riscos identificados (R1 – dependência de recursos humanos, R2 – inexistência de processos e procedimentos formalizados e desenhados, R3 – inexistência de planos de comunicação e R4 – Ciberataques), o organismo refletiu a realidade do setor da justiça, com destaque para cada um deles:

- R1: Trata-se de uma questão crítica no setor público, pelo facto da idade avançada dos colaboradores. pela morosidade dos processos de recrutamento de novos colaboradores ou de mobilidade interna e devido à falta de atratividade da progressão nas carreiras;
- R2: A informalidade na execução de tarefas é uma preocupação recorrente à resposta em situações de crise;
- R3: É uma lacuna comum nos organismos públicos, com impacto direto na reputação;
- R4: Uma questão que não passa despercebida dada a crescente incidência de ataques a entidades estatais.

Relativamente à análise de impacto, foi indicado pelos vários intervenientes que os níveis de impacto (de Baixo a Severo) estão estruturados de acordo com os objetivos e serviços prestados.

O DDT referiu que a inclusão da categoria Político/Legal é particularmente relevante no setor da Justiça. Justifica-o com o facto de que as decisões tomadas podem ter implicações jurídicas e institucionais sérias.

Já as restantes categorias são comuns aos sectores público e privado, sendo que a Reputação é mais evidenciada no público, na ótica do organismo em causa.

Por fim, indicaram que as estratégias de continuidade definidas vão ao encontro do que pretendem, principalmente por respeitarem os requisitos normativos, nomeadamente:

- ISO 22301: Planeamento, documentação, testes e comunicação;

- ISO 27005: Riscos cibernéticos e continuidade de TI;
- COBIT: Controlo de ativos, gestão de recursos humanos, governação e comunicação de riscos.

6.5.2 **Plano de Recuperação de Desastres**

Analisando o plano DR, tendo em conta que a lista de ativos já estava definida e devidamente atualizada, os intervenientes envolvidos afirmaram que a implementação de um sistema de ITAM seria uma boa estratégia para capacitar o organismo de ter controlo a nível operacional e garantir a rastreabilidade.

Desta forma, conseguem atingir a articulação entre os seus ativos e serviços, bem como as respetivas dependências.

Por conseguinte, indicaram que seria uma mais-valia se o ITAM integrasse com o IAM, já que contribuiria para a melhorar a segurança da informação.

No que toca à definição dos objetivos de recuperação (RTO, RPO, MTPD) com base na criticidade dos ativos, referiram que está de acordo com os objetivos do organismo pela questão de cumprir a norma ISO 22301, permitindo priorizar os possíveis cenários de desastre.

Uma das preocupações do organismo foi colmada aquando da identificação dos responsáveis, tendo sido identificada como ponto fulcral a atribuição de colaboradores substitutos. Deste modo, conseguirão garantir a redundância organizacional, evidenciando o alinhamento com o referencial COBIT.

Consideraram que a lista das infraestruturas e aplicações foi um passo fundamental, uma vez que foi priorizada segundo as criticidades e interdependências. No entanto, não deixaram de mencionar que numa fase posterior, será necessário avaliar as demais aplicações dos outros organismos do setor, para que sejam concretamente definidas as prioridades para todo o MJ.

Outra evidência demonstrada pelos intervenientes do organismo, refletiu-se na existência de um plano de comunicação em caso de cenários de desastre, pois reflete boas práticas da ISO 22301 e da gestão de crises no setor público.

Afirmaram, até, que a inclusão de canais alternativos é crítica num cenário de falha de comunicações e, por essa razão, será importante avaliar quais as melhores opções para estes canais no caso de necessidade.

A equipa responsável pelos *backups* indicou também que a diversificação dos locais de backup (internos, *multi-site*, *cloud*) faz todo o sentido por seguir uma abordagem que garante a resiliência. O alinhamento com a estratégia nacional da *Cloud* mostra uma clara integração com políticas públicas.

Finalizando a avaliação do plano DR, o facto de ter sido aprovado pelo DDT, demostrou que o trabalho foi bem estruturado. Por sua vez, a fase de testes acabou por não se iniciar por questões de janela temporal, não tendo sido possível avaliar no âmbito deste trabalho.

6.6 **Reflexão**

A presente fase tem como principal objetivo refletir sobre o que se aprendeu com os resultados das fases anteriormente descritas, bem como identificar dificuldades e melhorias a considerar como estratégias de melhoria contínua.

Estas aprendizagens constituem uma base valiosa para a melhoria contínua do plano e para o reforço da resiliência da organização.

Sempre antecipámos que seria criado o plano de comunicação, mas não foram consideradas todas as identificações das equipas e essa deverá ser uma lacuna a ser corrigida.

Por outro lado, conforme indicado na fase da avaliação, por motivos de planeamento, não foram efetuados testes a nível do plano de recuperação de desastres, pelo que será também algo a desenvolver.

Assim, em conjunto com vários intervenientes do organismo, evidencia-se a necessidade de desenvolver e testar mecanismos de resposta adequados à sua realidade, pelo que são salientadas algumas melhorias a ter em consideração, nomeadamente:

- Consciencializar os colaboradores e outros responsáveis sobre a importância da GCN e a responsabilidade de cada um, para identificarem e partilharem riscos para o negócio e estarem apto a responder e seguir os planos definidos;
- Garantir a alocação de recursos necessários para manter a disponibilidade de processos críticos;
- Incluir um cronograma de implementação das medidas de mitigação;
- Adotar as normas ISO 22301, ISO 27005 e COBIT;
- Antecipar um plano de auditoria e, consequentemente, de revisão anual do PCN;
- Planear e realizar exercícios e testes de forma a garantir a resiliência e a capacidade de recuperação em caso de desastre são adequadas.

Deste modo, como trabalhos futuros, para que o organismo atinja os seus objetivos, será necessário dar continuidade às sugestões também por eles indicadas:

- Priorizar intervenções com base numa matriz de criticidade e custo-benefício;
- Recorrer a financiamentos externos, como o PRR ou o Portugal 2030;
- Implementar um repositório digital centralizado, com atualização sistemática de documentação crítica por cada unidade orgânica;
- Realizar ações de sensibilização interna, envolvendo a gestão de topo;
- Integrar a continuidade de negócio nos programas de formação obrigatória e incluir igualmente nos planos direcionados aos dirigentes.

Finalizando a fase de reflexão, importa referir que alguns dos colaboradores envolvidos referem que, no projeto em questão, deveriam ter sido definidos indicadores de desempenho (KPIs) desde o início, com o intuito de acompanhar a implementação das medidas propostas como a quantidade de processos documentados ou a percentagem de colaboradores formados.

Não obstante, reforçam a importância de formalizar os calendários de testes, formações e atualizações do PCN, bem como a promoção de formações interdepartamentais para envolver todos os departamentos do organismo.

7. Conclusão

7.1 Contribuições teóricas e metodológicas

Numa perspetiva teórica, esta Dissertação contribui para o corpo de conhecimento sobre GCN demonstrando a aplicabilidade da utilização de CAR como metodologia para esse efeito. Em particular, a aplicabilidade foi demonstrada num organismo público do setor da Justiça, um domínio ainda pouco explorado na literatura científica (Davison et al., 2004; Becerra Acevedo et al., 2021). Através desta abordagem, foi possível adaptar e operacionalizar normas de referência como a ISO 22301 e a ISO 27005, bem como o referencial COBIT, validando empiricamente a sua aplicabilidade num contexto público nacional.

Este trabalho também amplia o entendimento da literatura sobre BIA, ao aplicar as orientações normativas à realidade de um organismo com constrangimentos operacionais e culturais próprios. Alinhando-se com investigações recentes (Păunescu et al., 2018; Gatto et al., 2023), demonstra-se que a BIA não é um processo meramente técnico, mas profundamente contextual e dependente do envolvimento dos diversos *stakeholders*, o que aponta a necessidade de uma crescente melhoria metodológica que permita o envolvimento e alinhamento destes.

Finalmente, o trabalho reforça a importância da integração entre a gestão de risco e a continuidade de negócio, um tema crescente na investigação sobre resiliência organizacional (Huapaya-Ruiz & Meneses-Claudio, 2024), evidenciando a necessidade de um alinhamento contínuo entre objetivos estratégicos, infraestrutura tecnológica e capacitação dos colaboradores.

7.2 Contribuições na perspetiva prática

Num contexto prático, todo o processo deve ser iniciado com o entendimento do contexto da organização, pelo que é necessário avaliar o estado de maturidade da mesma, identificar a sua missão, os processos de negócio e o meio em que se encontra.

De seguida torna-se indispensável a criação de uma lista com todos os ativos existentes e respetivas dependências, tanto internas e como externas.

Somente efetuando primeiramente este levantamento e identificação, se consegue definir o propósito do PCN e do DRP a implementar à organização. Se será apenas na unidade orgânica de TI ou no seu todo.

Nesta fase é crucial que a organização defina os seus objetivos de forma clara, seja proteger os seus dados, manter uma boa reputação ou minimizar o tempo de interrupção em caso de situações catastróficas, sempre com a respetiva aprovação superior.

Definir uma equipa de continuidade de negócio, as funções de cada um e as suas responsabilidades faz igualmente parte de ambos os planos, pelo que é indispensável a criação desta equipa na organização.

Para os ativos anteriormente identificados, devem ser associados os respetivos processos. Só assim será possível proceder à análise de impacto no negócio, estabelecendo o tempo máximo de inatividade aceitável (RTO), o limite aceitável de perda de dados (RPO), bem como a identificação dos riscos, a sua priorização, probabilidade de ocorrer e qual o impacto que advém para a organização.

A definição de estratégias de continuidade e recuperação permitem à organização ter alternativas que as garantam. Exemplos destas estratégias são a definição de procedimentos para recuperar os dados/sistemas, planear estratégias de mitigação de riscos possíveis de ocorrerem e garantirem a redundância, como o caso dos *backups* em vários locais, por exemplo.

Tanto para o PCN como para o DRP, é necessário existir um plano de comunicação, onde são identificados os *stakeholders* e definidos os colaboradores que serão responsáveis pela comunicação em cenários de crise e quais os canais que devem ser utilizados para o efeito.

Também a validação da existência e confiabilidade de *backups* e simulações têm um papel fundamental para que a organização colmate as lacunas ainda existentes e efetue as alterações necessárias aos planos para estarem de acordo com a sua realidade.

É importante redigir os planos de forma clara e acessível para que sejam aprovados e validados formalmente pelos superiores.

Aprovados os planos, a organização deverá realizar testes periódicos e, consequentemente, rever e atualizar o plano semestral ou anualmente ou após mudanças relevantes que impactem de forma direta com a mesma.

7.3 Limitações e Trabalhos futuros

No decorrer da pesquisa em causa foram evidenciadas algumas limitações que são importantes mencionar, já que a colaboração com o organismo e respetivos participantes foi crucial, mas apresentou vários desafios.

Apesar do envolvimento de intervenientes-chave, foi notório que algumas das áreas operacionais demonstraram alguma resistência e pouca disponibilidade para colaborar nas entrevistas.

Não obstando, também na fase de avaliação este facto acabou por comprometer de certa forma uma visão completa do que foi definido para o organismo.

Por outro lado, foi notória a inexistência de uma cultura institucional consolidada de gestão do risco e continuidade de negócio, revelando que normas como as ISO e o referencial COBIT eram, em parte, desconhecidas.

Enquanto investigadora na área, considero que, futuramente, seria importante alargar este trabalho a outras áreas, não restringindo somente o setor público da Justiça.

Seria uma mais-valia, conseguir garantir que também o setor da Saúde ou da Educação têm um PCN e um DRP adaptado às suas necessidades.

Referências Bibliográficas

Acevedo, R. B., Muñoz, J. R. B., Camacho, H. C., & Obando, C. J. (2021). Evolución y modelos de implementación de sistemas de gestión de continuidad del negocio. SIGNOS-Investigación en sistemas de gestión, 13(2).

Action Research in Teaching and Learning | Western Sydney University. (2025). https://www.westernsydney.edu.au/learning_futures/home/professional_learning/evidencing_your_practice/action_research

Almeida, D. A. D., Leal, F., Pinho, A. F. D., & Fagundes, L. D. (2006). Gestão do Conhecimento na análise de falhas: mapeamento de falhas através de sistema de informação. Production, 16, 171-188.

Bagiński, J., & Rostanski, M. (2011). The modeling of business impact analysis for the loss of integrity, confidentiality and availability in business processes and data. *Theoretical and Applied Informatics*, *23*, 73-82.

Bastos, A. (2022, 16 de novembro). Como definir sua abordagem de gestão de riscos . https://pt.linkedin.com/pulse/como-definir-sua-abordagem-de-gest%C3%A3o-riscos-alberto-bastos

Boghossian, R. G., Perez, G., Cesar, A. M. R. V. C., & Barbosa, E. D. E. (2019). A Memória organizacional e os sistemas de informação suportando a tomada de decisão. Prisma. com, (38), 102-125.

Brites, A. P. (2022). Risks of Robotic Process Automation: A Multivocal Literature Review. PQDT-Global.

da Silveira, P. M. (2009). Plano de Continuidade de Negócios para a empresa ALFA: uma proposta com base na NBR 15999, no ITIL e no COBIT. Revista da Graduação, 2(2).

Davison, R., Martinsons, M. G., & Kock, N. (2004). Principles of canonical action research. Information systems journal, 14(1), 65-86.

de Haes, S., Van Grembergen, W., & Debreceny, R. S. COBIT 5 e governança corporativa de tecnologia da informação: blocos de construção e oportunidades de pesquisa.

de Oliveira Gatto, D. D., Possamai, M. E., & Sassi, R. J. (2023). MaPO: modelo de gestão de continuidade de negócios baseado em boas práticas de governança de TI. Revista de Gestão e Secretariado, 14(3), 2963-2981.

de Oliveira, A. B., Fernandes, G. H. M., Luzia, B. B., & Júnior, E. S. (2024). Mortalidade das micro e pequenas empresas: a importância de um plano de continuidade de negócios. Revista de Gestão e Secretariado, 15(7), e3879-e3879.

de Souza, E. G., & Reinhard, N. (2015). Uma revisão bibliográfica dos fatores ambientais que influenciam a gestão de projetos de sistemas de informação no setor público. Revista de Gestão e Projetos, 6(2), 27-41.

Diário da República — I Série-A – Decreto-Lei n.º 135/99, 1999

Governo Digital (2024, dezembro). A Cloud na Administração Pública. https://digital.gov.pt/areas-tematicas/cloud

Hecht, J. A. (2002). Business continuity management. Communications of the Association for Information Systems, 8(1), 30.

Hilbert, M. (2020). Digital technology and social change: the digital transformation of society from a historical perspective. Dialogues in clinical neuroscience, 22(2), 189-194.

Huapaya-Ruiz, R., & Meneses-Claudio, B. (2024). Applicable methodologies for business continuity management in IT services: A systematic literature review. Data and Metadata, 3, 182-182.

ISO - Organização Internacional para Padronização. (2024, 14 de outubro). ISO. https://www.iso.org/home.html

Kesa, D. M. (2023). Ensuring resilience: Integrating IT disaster recovery planning and business continuity for sustainable information technology operations. World Journal of Advanced Research and Reviews, 18(3), 970-992.

Laudon, K. C., Laudon, J. P., Hall, P. P., & Education, P. (2007). Management Information Systems: Managing the Digital Firm–9th Edition. Studies in Informatics and Control, 16(1), 147.

Lima, M. (2016). O uso da entrevista na pesquisa empírica. Métodos de pesquisa em Ciências Sociais: bloco qualitativo, 24-41.

MacLean, D., & Titah, R. (2021). A Systematic Literature Review of Empirical research on the Impacts of e-Government: A Public Value Perspective. *Public Administration Review*, *82*(1), 23–38. https://doi.org/10.1111/puar.13413

Marker, A. (2022, 15 de setembro). ISO 22301 Business Continuity Simplified: Fortaleça seu negócio contra interrupções. Smartsheet. https://www.smartsheet.com/content/iso-22301-business-continuity-guide

Neto, G. T. G., Santos, W. B., Endo, P. T., & Fagundes, R. A. (2019, September). Multivocal literature reviews in software engineering: Preliminary findings from a tertiary study. In 2019 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM) (pp. 1-6). IEEE.

OECD (2024), Modernisation of the Justice Sector in Portugal, OECD Publishing, Paris, https://doi.org/10.1787/cbde9a7a-en.

Păunescu, C., Popescu, M. C., & Blid, L. (2018). Business impact analysis for business continuity: Evidence from Romanian enterprises on critical functions. Management & Marketing, 13(3), 1035-1050.

Publicações da estrutura COBIT 5 | ISACA. (nd-b). ISACA. https://www.isaca.org/resources/cobit/cobit-5

Rodríguez Cruz, M. A. (2025). Diseño de plan estratégico para el área de TI en cooperativas de transportes bajo COBIT 5.0 (Bachelor's thesis, La Libertad: Universidad Estatal Península de Santa Elena, 2025.).

Ribeiro, J., & Gomes, R. (2009, June). IT governance using COBIT implemented in a high public educational institution: a case study. In Proceedings of the 3rd international conference on European computing conference (pp. 41-52).

Roztocki, N., Strzelczyk, W., & Weistroffer, H. R. (2020). Sustaining Organizational Operations during an Outbreak: Problems, Needs, and Opportunities for Information

Systems. Information Systems Management, 37(4), 348–356. https://doi.org/10.1080/10580530.2020.1821133

Saunders, M., Lewis, P., & Thornhill, A. (2019). Research methods for business students. Pearson education.

Silva, P. M. S. D. (2016). Diretrizes para a elaboração de um plano de continuidade de negócio: estudo de caso (Master dissertation, Instituto Politécnico de Setúbal. Escola Superior de Ciências Empresariais).

Souza, T. (2022, August 10). COBIT 5: Princípios, exemplos de uso, domínios, processos de TI e níveis de capacidade. Tiago Souza. https://tiagosouza.com/cobit-principios-exemplos-uso-dominios-processos-ti-niveis-capacidade/

Wiboonratr, M., & Kosavisutte, K. (2009). Optimal strategic decision for disaster recovery. International Journal of Management Science and Engineering Management, 4(4), 260-269.

Yin, R. K. (2018). *Case study research and applications: Design and Methods* (6th ed.). Thousand Oaks: Sage.

APÊNDICES

APÊNDICE 1. *Script* de Entrevista | Ciclo CAR

Introdução

(investigador)

- Contextualização da pesquisa
- Esclarecimento de anonimato

(entrevistado)

- Formação profissional
- Função e responsabilidades associadas

Questões iniciais:

1. Quais os responsáveis de cada área?
2. As funções de cada responsável estão claras e detalhadas?
3. Existe uma equipa responsável pela continuidade de negócio?

Questões relacionadas com continuidade de negócio:

1. Que documentação possuem relativa ao PCN existente?
2. Essa documentação, tem vindo a ser devidamente atualizada? Se sim, por quem?
3. São realizados exercícios e simulações para avaliar a eficácia do PCN existente?
4. Existe uma lista de processos de negócio com as áreas responsáveis e respetivas dependências? Se sim, quem é responsável pela manutenção/atualização?
5. Lista de ativos, onde sejam evidentes o mapeamento com os processos de negócio e a sua localização exata? Se sim, quem é responsável pela manutenção/atualização?
6. Os riscos do negócio estão devidamente identificados?

Questões relacionadas com segurança:

1. Possuem uma lista de estratégias de suporte ao PCN?
2. Estão implementados processos de recuperação de desastres?
3. São efetuados testes e sessões de consciencialização aos colaboradores?

ANEXOS

ANEXO 1 – Priorização de riscos

Priorização de Riscos

1. Identificação de ativos de informação

   São designados ativos de informação, sistemas, portais, servidores, bases de dados, equipamentos de comunicação, serviços de eletricidade, refrigeração, iluminação e contratos que devem ser identificados no âmbito da segurança de informação com o respetivo *owner* associado.

2. Determinação do valor da informação

   Para cada ativo de informação identificado, é efetuada a classificação no que refere à confidencialidade, integridade e disponibilidade (Tabela 12).

Tabela 12 – Classificação de risco

	Baixa	Média	Alta
Confidencialidade Assegurar que a informação apenas está acessível a quem está autorizado	O acesso não autorizado à informação tem um efeito adverso **limitado** nas operações, bens ou pessoas da organização	O acesso não autorizado à informação tem um efeito adverso **significativo** nas operações, bens ou pessoas da organização	O acesso não autorizado à informação tem um efeito adverso **catastrófico** nas operações, bens ou pessoas da organização
Integridade Salvaguardar que a informação (e o método de processamento) é exata e completa	Uma alteração não autorizada à informação ou destruição da mesma tem um efeito adverso **limitado** nas operações, bens ou pessoas da organização	Uma alteração não autorizada à informação ou destruição da mesma tem um efeito adverso **significativo** nas operações, bens ou pessoas da organização.	Uma alteração não autorizada à informação ou destruição da mesma tem um efeito adverso **catastrófico** nas operações, bens ou pessoas da organização
Disponibilidade Assegurar que os utilizadores autorizados têm acesso à informação quando necessário	O não acesso ou impossibilidade de utilização da informação ou sistema de informação tem um efeito adverso **limitado** nas operações, bens ou pessoas da organização	O não acesso ou impossibilidade de utilização da informação ou sistema de informação tem um efeito adverso **significativo** nas operações, bens ou pessoas da organização.	O não acesso ou impossibilidade de utilização da informação ou sistema de informação tem um efeito adverso **catastrófico** nas operações, bens ou pessoas da organização

   É determinado o valor do ativo da informação que caracterize o impacto da perda para cada prioridade (confidencialidade, integridade e disponibilidade):

   - Alto – sempre que combinação seja "alta/alta" ou "alta/alta/alta"
   - Médio – sempre que combinação seja "média", "média/média" ou "média/média/média"
   - Baixo – sempre que combinação seja "baixa/baixa" ou "baixa/baixa/baixa"

3. Determinação da probabilidade de ocorrência

   Para cada ativo de informação identificado, devem ser identificadas as vulnerabilidades e possíveis ameaças, de acordo com os seguintes critérios:

- Vulnerabilidade – condição ou conjunto de condições que permitem que ameaças afetem os ativos
- Ameaça – origina incidentes disruptivos que podem resultar em danos ou perdas de um ativo.
- Probabilidade de ocorrência – probabilidade que uma ameaça tem de explorar inerentes ao ativo.

Critérios para a probabilidade de ocorrência de ameaças:

- Alta – ocorrência frequente (diária/semanal)
- Média – ocorrência repetitiva (mensal/anual)
- Baixa – ocorrência pouco frequente (últimos 3 a 5 anos)

4. Determinação do risco:

   O risco é determinado pela combinação do valor com a probabilidade de ocorrência, de acordo com a matriz disponível em Tabela 13.

Tabela 13 – Matriz de Risco

RISCO		Valor		
		Alta	Média	Baixa
Probabilidade	Alta	Elevado	Alto	Médio
	Média	Alto	Médio	Baixo
	Baixa	Médio	Baixo	Desprezável

5. Identificação de controlos a aplicar:

   O risco associado às meaças identificadas pode ser eliminado ou reduzido por implementação das estratégias de controlo.

6. Plano de ação de mitigação:

   Para cada controlo com necessidade de implementação de um plano de ação, devem ser estabelecidas um conjunto de ações, responsabilidades e prazosd que permitam assegurar a execução dos controlos definidos.

7. Revisão da avaliação de riscos:

   É aconselhável a reavaliação dos riscos de forma a:

   - Incluir alterações nos ativos de informação;
   - Incorporar alterações das prioridades e necessidades;

- Considerar novas ameaças e vulnerabilidades;
- Verificar se os controlos permanecem eficazes e apropriados.