LISBON SCHOOL OF ECONOMICS & MANAGEMENT
UNIVERSIDADE DE LISBOA

MESTRADO EM

ECONOMIA E GESTÃO DE CIÊNCIA, TECNOLOGIA E INOVAÇÃO

TRABALHO FINAL DE MESTRADO

TRABALHO DE PROJECTO

RESILIÊNCIA DIGITAL NO SECTOR PÚBLICO FINANCEIRO EM CONTEXTO DE CATÁSTROFE

Carmen Karina Garcia Paiva

JUNHO- 2025

LISBON SCHOOL OF ECONOMICS & MANAGEMENT
UNIVERSIDADE DE LISBOA

TRABALHO FINAL DE MESTRADO

TRABALHO DE PROJECTO

RESILIÊNCIA DIGITAL NO SECTOR PÚBLICO FINANCEIRO

EM CONTEXTO DE CATÁSTROFE

CARMEN KARINA GARCIA PAIVA

Orientador:

Prof. Doutor Manuel Duarte Mendes Monteiro

Laranja

JUNHO- 2025

RESUMO

Este Trabalho Final de Mestrado analisa a resiliência digital no sector público financeiro em contextos de catástrofe, com especial enfoque na inundação de 2024 no estado do Rio Grande do Sul (Brasil), considerada a mais severa da sua história, afectando mais de 2,3 milhões de pessoas e provocando prejuízos estimados entre 110 e 155 mil milhões de reais. A investigação adopta uma abordagem qualitativa, integrando revisão sistemática da literatura, análise documental e estudo de caso. São explorados modelos teóricos com o objectivo de compreender a resposta dos sistemas financeiros públicos a falhas digitais em situações de emergência.

Os resultados evidenciam vulnerabilidades estruturais e institucionais, mas também identificam práticas resilientes susceptíveis de replicação. A investigação oferece contributos para a formulação de políticas públicas e para o aperfeiçoamento de modelos de governação digital resiliente. Num cenário global marcado por guerras, pandemias, alterações climáticas e ciberataques, a resiliência digital afirma-se como um eixo estratégico. Com base no caso empírico do Rio Grande do Sul e em referenciais internacionais (Arup & Resilient Cities Network, 2023), propõe-se um modelo de resiliência digital assente na redundância de sistemas, inclusão social e promoção da literacia tecnológica.

Palavras-chave: resiliência digital, sector público financeiro, catástrofes, continuidade operacional, governação digital, cibersegurança, emergências climáticas.

ABSTRACT

This Master's Final Work analyzes digital resilience in the public financial sector in catastrophe contexts, with a special focus on the 2024 flood in the state of Rio Grande do Sul (Brazil), considered the most severe in its history, affecting more than 2.3 million people and causing losses estimated between 110 and 155 billion reais. The research adopts a qualitative approach, integrating systematic literature review, documentary analysis and case study. Theoretical models are explored with the aim of understanding the response of public financial systems to digital failures in emergency situations.

The results highlight structural and institutional vulnerabilities, but also identify resilient practices susceptible to replication. Research offers contributions to public policy-making and the refinement of resilient digital governance models. In a global scenario marked by wars, pandemics, climate change and cyberattacks, digital resilience asserts itself as a strategic axis. Based on the empirical case of Rio Grande do Sul and international references (Arup & Resilient Cities Network, 2023), a digital resilience model based on systems redundancy, social inclusion and the promotion of technological literacy is proposed.

Keywords: digital resilience, public financial sector, disasters, business continuity, digital governance, cybersecurity, climate emergencies.

Índice

Lista de Abreviaturas

Sigla / Abreviatura	Designação por extenso	Descrição
ANA	Agência Nacional de Águas e Saneamento Básico	Órgão brasileiro responsável pela gestão dos recursos hídricos. Em Portugal, pode ser comparada à Agência Portuguesa do Ambiente.
ANATEL	Agência Nacional de Telecomunicações	Autoridade brasileira de regulação das telecomunicações.
BID	Banco Interamericano de Desenvolvimento	Instituição financeira internacional que apoia o desenvolvimento económico na América Latina e Caraíbas.
CEPAL	Comissão Económica para a América Latina e o Caribe	Agência regional das Nações Unidas para o desenvolvimento económico e social.
CMM	Capability Maturity Model	Modelo de Maturidade de Capacidades — estrutura internacional usada para avaliar o grau de maturidade em processos de segurança ou gestão digital.
COR	Centro de Operações do Rio de Janeiro	Entidade pública municipal brasileira responsável pela coordenação de emergências urbanas.
DANFE	Documento Auxiliar da Nota Fiscal Electrónica	Documento fiscal brasileiro
FAO	*Food and Agriculture Organization*	Organização das Nações Unidas para Alimentação e Agricultura
GNRE	Guia Nacional de Recolhimento de Tributos Estaduais	Documento de pagamento de tributos estaduais no Brasil
IBGE	Instituto Brasileiro de Geografia e Estatística	Órgão oficial de estatísticas e geociências do Brasil.

ICMS	Imposto sobre a Circulação de Mercadorias e Serviços	Tributo estadual brasileiro.
INMET	Instituto Nacional de Meteorologia	Entidade federal brasileira responsável pela meteorologia.
MEI	Microempreendedor Individual	Categoria fiscal brasileira.
MTTR	*Mean Time to Recovery*	Tempo Médio de Recuperação — indicador técnico de desempenho em resiliência digital.
MTTD	*Mean Time to Detection*	Tempo Médio de Deteção — indicador técnico de resposta a incidentes.
OECD	*Organisation for Economic Co-operation and Development*	Organização para a Cooperação e Desenvolvimento Económico — instituição internacional sediada em Paris.
PCN	Plano de Continuidade de Negócios	Documento que define procedimentos para assegurar a continuidade das operações em caso de interrupção.
PIX	Sistema de Pagamentos Instantâneos (Brasil)	Plataforma de pagamentos digitais criada pelo Banco Central do Brasil.
PLANO RIO GRANDE	Plano Rio Grande	Programa do Governo do Estado do Rio Grande do Sul para reconstrução pós-catástrofe e promoção da resiliência climática.
PRD	Plano de Recuperação de Desastres	Documento estratégico para restabelecimento de sistemas e operações após uma crise.
PROCERGS	Companhia de Processamento de Dados do Estado do Rio Grande do Sul	Empresa pública de tecnologia do Governo do Estado do RS.
RPO	*Recovery Point Objective*	Objectivo de Ponto de Recuperação — indicador técnico de continuidade digital.

RTO	*Recovery Time Objective*	Objectivo de Tempo de Recuperação — indicador técnico de desempenho e resiliência digital.
RS	Rio Grande do Sul	Estado do sul do Brasil.
SEFAZ-RS	Secretaria da Fazenda do Estado do Rio Grande do Sul	Órgão responsável pela gestão financeira e orçamental do Estado.
SICT	Secretaria de Inovação, Ciência e Tecnologia	Secretaria estadual brasileira com competências em políticas de inovação e digitalização.
TCE-RS	Tribunal de Contas do Estado do Rio Grande do Sul	Órgão de fiscalização financeira do Estado.
TTF	*Task–Technology Fit*	Modelo teórico de adequação entre tarefas e tecnologias.
UTAUT	*Unified Theory of Acceptance and Use of Technology*	Teoria Unificada da Aceitação e Utilização da Tecnologia — modelo teórico aplicado à análise de adoção tecnológica.
UNDP	*United Nations Development Programme*	Programa das Nações Unidas para o Desenvolvimento.
UNDRR	*United Nations Office for Disaster Risk Reduction*	Gabinete das Nações Unidas para a Redução do Risco de Catástrofes.
UN-Habitat	*United Nations Human Settlements Programme*	Programa das Nações Unidas para os Assentamentos Humanos.
VDI	*Virtual Desktop Infrastructure*	Infraestrutura de Ambiente de Trabalho Virtual — tecnologia de acesso remoto a sistemas informáticos.
WORLD BANK	Banco Mundial	Instituição financeira internacional do Grupo Banco Mundial.

1. Introdução

A digitalização da administração pública tem-se afirmado, nas últimas décadas, como um vector transformador essencial para a construção de Estados mais eficientes, inclusivos e responsivos. Tecnologias emergentes, como a computação em nuvem, b*ig data*, inteligência artificial e *blockchai*n, têm redefinido os modos de concepção, gestão e disponibilização dos serviços públicos. No âmbito financeiro, esta transformação é particularmente sensível, dado que actividades críticas — como a arrecadação de impostos, a execução orçamental, o pagamento de salários e a transferência de prestações sociais — passaram a depender fortemente de infraestruturas digitais. A falha desses sistemas pode comprometer gravemente a continuidade do funcionamento estatal e a confiança dos cidadãos (Chen, Zhang & Pereira, 2025. Oliveira, Santos & Paiva, 2024).

Neste contexto, a resiliência digital assume uma centralidade estratégica, sendo entendida como a capacidade das instituições públicas de **antecipar, absorver, responder e adaptar-se** a choques externos, assegurando a integridade e a disponibilidade dos serviços essenciais (Arup & Resilient Cities Network, 2023. UNDRR, 2022). A crise climática de 2024 no Estado do Rio Grande do Sul (Brasil), marcada por inundações severas que afectaram 478 dos 497 municípios, constitui um caso paradigmático para análise.

A tempestade revelou não apenas vulnerabilidades técnicas, mas também a ausência de protocolos eficazes de continuidade, redundância e resposta digital coordenada. Simultaneamente, emergiram exemplos pontuais de superação, nos quais soluções tecnológicas de emergência permitiram restaurar parcialmente a funcionalidade institucional.

Este trabalho propõe-se analisar, à luz do desastre ocorrido no Rio Grande do Sul, como e em que medida a resiliência digital pode ser estruturada no sector público financeiro, tomando como caso empírico a Subsecretaria do Tesouro do Estado. Pretende-se compreender as fragilidades estruturais, as respostas institucionais e as boas práticas emergentes, bem como propor orientações e indicadores para o reforço da governação digital em contextos de catástrofe.

Questão de investigação Principal:

Como pode a resiliência digital reforçar a continuidade e a robustez dos serviços financeiros públicos em contextos de catástrofe?

Subquestões de Investigação:

- Quais as vulnerabilidades reveladas pela crise de 2024 no Rio Grande do Sul?
- Que práticas institucionais contribuíram para a continuidade operacional?
- Como podem modelos internacionais de maturidade digital ser aplicados ao contexto brasileiro?
- Que indicadores e diretrizes podem apoiar a formulação de políticas de governação digital resiliente?

A relevância teórica do estudo situa-se na intersecção entre a governação digital, a gestão de riscos e a *ciber*-resiliência institucional. No plano prático, o trabalho contribui com a proposta de um Plano de Contingência para a Resiliência Digital na Prestação de Serviços Públicos Financeiros, reforçando a capacidade de adaptação em cenários de crise.

2. Apresentação do contexto real e identificação do problema

A intensificação da frequência e da gravidade dos eventos disruptivos — como guerras, ciberataques, pandemias, fenómenos climáticos extremos e colapsos em infraestruturas

críticas — tem desafiado a capacidade das sociedades contemporâneas para resistir, adaptar-se e recuperar-se com celeridade. A crescente digitalização das cidades e das administrações públicas, embora tenha proporcionado avanços significativos, também introduziu novos riscos e vulnerabilidades (UNDRR, 2022. OECD, 2019).

Neste enquadramento, a resiliência digital emerge como uma competência institucional essencial, definida como a capacidade dos sistemas digitais para suportar e responder a situações de crise sem colapsar. Esta não se limita ao funcionamento das tecnologias, mas abrange a capacidade organizacional de **antecipar, planear, comunicar e assegurar a continuidade dos serviços públicos essenciais** (Boin & McConnell, 2022).

A crise climática de 2024 no Estado do Rio Grande do Sul ilustra de forma paradigmática estes desafios. A destruição das redes físicas e a pressão exercida sobre os sistemas digitais de gestão pública resultaram na suspensão de serviços críticos, como o processamento de salários, as transferências sociais e a execução orçamental.

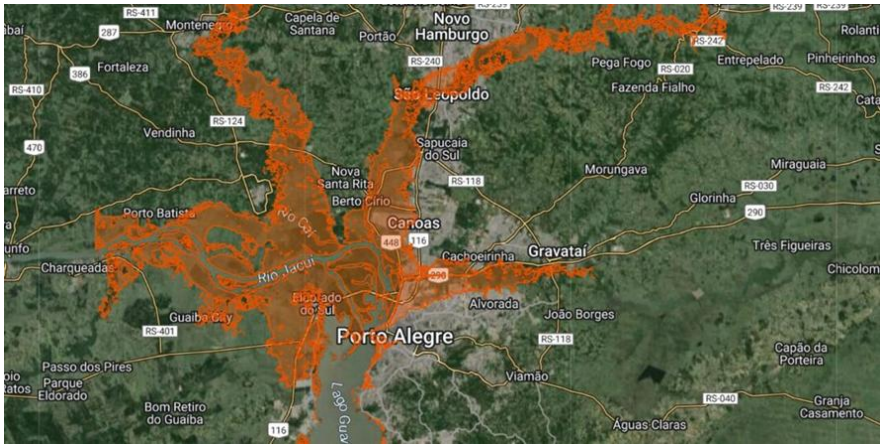

Figura 1 - Mapa da inundação da Região Metropolitana de Porto Alegre, capital do Estado do Rio Grande do Sul. Em 4/5/2024 às 10h30

A Companhia de Processamento de Dados do Estado (PROCERGS) foi forçada a desligar o seu centro de dados devido ao risco de colapso eléctrico e inundação, afectando directamente o Tesouro estadual (Governo do Estado do Rio Grande do Sul, 2024).

Figura 2 - Vista área da Procergs no momento da inundação. Foto: Gustavo Mansur/ Palácio Piratini.

Durante a crise, foram adoptadas soluções emergenciais, como a migração acelerada de serviços para a nuvem, parcerias com instituições financeiras e o uso de canais alternativos de comunicação. No entanto, a ausência de interoperabilidade entre sistemas estaduais e municipais, bem como a inexistência de planos de recuperação de desastres, agravaram os impactos (Pessoa et al., 2025).

Principais Acontecimentos Relacionados a Sistemas – Crise de Maio de 2024

- 6 de Maio de 2024 -Foi realizado o desligamento preventivo dos centros de dados da Secretaria da Fazenda do Estado do Rio Grande do Sul (SEFAZ-RS) e da Companhia de Processamento de Dados do Estado do Rio Grande do Sul (PROCERGS), como medida de protecção da infraestrutura tecnológica face à subida das águas em Porto Alegre.

- 7 de Maio de 2024 - Foram activados canais de contingência para atendimento aos contribuintes, incluindo o uso de correio electrónico, emissão de guias de pagamento do Imposto sobre a Circulação de Mercadorias e Serviços (ICMS) através da Guia Nacional de Recolhimento de Tributos Estaduais (GNRE), e a autorização de trânsito livre nos postos fiscais para facilitar a chegada de doações.

- 11 de Maio de 2024 - Foi activado o ambiente de contingência da Sefaz Virtual do Ambiente Nacional (SVC-AN), permitindo a autorização de documentos fiscais electrónicos através da infraestrutura em nuvem, mesmo com os sistemas locais inoperantes.
- 20 de Maio de 2024 - Foi retomado parcialmente o funcionamento do Emissor de Nota Fiscal Avulsa Electrónica (NFA-e), inicialmente disponível apenas para Microempreendedores Individuais (MEIs), operando em ambiente tecnológico em nuvem.
- 24 de Maio de 2024 - Foi restabelecida a geração do Documento Auxiliar da Nota Fiscal Electrónica (DANFE) para os MEIs, embora com limitações, como a inexistência de envio por correio electrónico e a indisponibilidade do link de consulta no portal da Secretaria da Fazenda.
- 25 de Maio de 2024 - Os centros de dados da SEFAZ-RS e da PROCERGS foram reactivados. A recuperação dos sistemas iniciou-se de forma gradual ao longo da semana. A Infraestrutura de Ambiente de Trabalho Virtual (VDI – Virtual Desktop Infrastructure) foi transferida para o centro de dados da PROCERGS, garantindo maior segurança e continuidade do acesso remoto.
- 1 de Julho de 2024- Foi concretizado o regresso às actividades presenciais no edifício-sede da SEFAZ-RS, após dois meses de reparações. Os sistemas físicos e digitais voltaram a operar normalmente, embora o rés-do-chão do edifício tenha permanecido isolado devido aos danos causados pela inundação. (Notícias Intrasefaz, 2024)

Figura 3 – Cronologia da Crise de 2024.

Este colapso revelou fragilidades estruturais: centralização excessiva de servidores físicos, inexistência de conectividade alternativa, planos de continuidade desatualizados e baixa maturidade digital em municípios de menor dimensão.

A escolha da Subsecretaria do Tesouro do Estado como objecto de estudo justifica-se pela sua posição estratégica na cadeia de funcionamento da administração pública estadual, bem como pela sua exposição directa aos impactos decorrentes da interrupção dos sistemas da Companhia de Processamento de Dados do Estado do Rio Grande do Sul (PROCERGS). A Secretaria da Fazenda do Estado do Rio Grande do Sul, através da Subsecretaria do Tesouro do Estado, é responsável pela gestão financeira, orçamental e patrimonial do Governo Estadual (Secretaria da Fazenda, 2023).

A experiência profissional da autora, que por trabalhar para o Tesouro do Estado, participou na resposta institucional à crise, reforça a pertinência da análise proposta.

Durante o período de inoperacionalidade, foram activadas soluções em nuvem, utilizados canais alternativos de comunicação e reconstruídos dados críticos com base em cópias de segurança locais e registos paralelos, evidenciando a capacidade de adaptação das estruturas institucionais (Oliveira et al., 2024).

A análise da crise revelou falhas estruturais na arquitectura digital da administração

pública, nomeadamente a centralização excessiva de servidores físicos, a ausência de conectividade alternativa, a inexistência de planos de continuidade actualizados e a baixa maturidade digital em municípios de menor dimensão.

Não obstante estas limitações, algumas instituições conseguiram manter a operacionalidade de forma eficaz, graças à adopção de medidas mitigadoras, revelando boas práticas de resposta emergencial, ainda que pontuais e não sistematizadas (CEPAL et al., 2024).

3. Enquadramento teórico/literatura

3.1. Resiliência Digital: Conceito e Relevância no Sector Público

A resiliência digital constitui um conceito em expansão, decorrente da convergência entre a segurança da informação, a gestão de riscos e a governação digital. É entendida como a **capacidade de antecipar, resistir, adaptar-se e recuperar de eventos disruptivos**, assegurando a continuidade e a confiança nos serviços digitais críticos (UNDRR, 2022. Boin & Lodge, 2020).

No sector público financeiro, a resiliência digital assume uma relevância particular, dada a criticidade das operações envolvidas, como a arrecadação tributária, o pagamento de salários e a execução orçamental. A interrupção destes serviços pode desencadear efeitos sistémicos com impacto directo na estabilidade socioeconómica.

3.2. A Digitalização da Administração Pública e os Desafios da Continuidade

A crescente digitalização da administração pública brasileira — impulsionada por iniciativas como o programa GOV.BR e a Lei do Governo Digital (Lei n.º 14.129/2021) — tem promovido avanços significativos na modernização dos serviços, no reforço da

transparência e na melhoria da eficácia da gestão. A digitalização pode potenciar a resiliência operacional, ao melhorar as capacidades de deteção e resposta, bem como ao reforçar a capacidade de recuperação através da reconfiguração dos sistemas em momentos de crise (Chen et al., 2025). Contudo, esta crescente dependência das plataformas digitais também tem contribuído para o agravamento da vulnerabilidade institucional face a eventos extremos e falhas sistémicas.

Estudos como o *Relatório Técnico sobre os Impactos Socioeconómicos dos Eventos Climáticos Extremos de 2024 no Rio Grande do Sul: Uma Análise Após Um Ano do Desastre* (Pessoa et al., 2025) demonstram que, em contextos de calamidade, a continuidade dos serviços públicos depende da existência de planos robustos de recuperação de desastres, de infraestruturas tecnológicas redundantes e de uma integração intergovernamental eficaz.

A ausência destes elementos pode conduzir a colapsos operacionais, como se verificou durante a crise provocada pelas cheias de 2024 no Estado do Rio Grande do Sul.

3.3. Governação Digital e Infraestruturas Críticas

As infraestruturas críticas digitais englobam plataformas de pagamento, sistemas fiscais, bases de dados e redes de comunicação essenciais ao funcionamento do Estado. A OCDE (2019) identifica sete desafios centrais para o reforço da resiliência destas infraestruturas:

- **Criação de um quadro de governação multilateral para a resiliência das infraestruturas críticas.** Os governos devem adoptar uma abordagem holística, que contemple múltiplos riscos e sectores interdependentes.
- **Compreensão das interdependências e vulnerabilidades entre sistemas.** É necessário aplicar metodologias e métricas que permitam identificar funções, sistemas e activos críticos, priorizando investimentos em resiliência.

- **Estabelecimento de confiança entre governo e operadores.** A partilha segura e confidencial de informações sobre riscos deve ser promovida através de plataformas colaborativas.
- **Criação de parcerias para uma visão comum e definição de objectivos exequíveis.** O diálogo permanente entre operadores públicos e privados deve ser orientado pelas expectativas da sociedade.
- **Definição de políticas para priorização de medidas de resiliência ao longo do ciclo de vida das infraestruturas.** Instrumentos políticos baseados em análises custo-benefício devem incentivar o investimento em resiliência.
- **Garantia de responsabilização e monitorização da execução das políticas.** A implementação deve ser acompanhada por mecanismos claros de responsabilização e avaliação de progresso.
- **Abordagem da dimensão transfronteiriça das infraestruturas.** A coordenação internacional é essencial para enfrentar dependências entre sistemas de diferentes países.

A literatura recente sobre resiliência digital e cibersegurança sublinha a importância de estruturas de governação robustas, que integrem protocolos de segurança, arquitecturas técnicas distribuídas e planeamento estratégico multissectorial. Mouratidis et al. (2023) propõem uma abordagem abrangente que articula requisitos de segurança, inteligência de ameaças, infraestruturas críticas e resposta a incidentes. Atıcı e Tuna (2025) destacam os impactos das interrupções, como perdas de dados e prejuízos económicos, enquanto Conrad et al. (2023) enfatizam a necessidade de planeamento de contingência, com foco na continuidade estratégica e na recuperação táctica dos sistemas. Beuchelt (2025) defende o alinhamento entre a estratégia de segurança da informação e os objectivos

operacionais, salientando o papel dos padrões internacionais na construção de uma postura proactiva e resiliente.

No domínio da deteção e resposta a ameaças, Ali et al. (2025) evidenciam o potencial da integração de dados multimodais com redes neurais para deteção em tempo real, ao passo que Basu (2023) sublinha a relevância de sistemas de autodiagnóstico e vigilância inteligente. Tekinerdogan et al. (2024) propõem um modelo de priorização de recursos para a protecção de infraestruturas críticas, e Fu (2024) sugere estratégias de redundância em controladores em tempo real como forma de mitigar ataques e preservar a resiliência dos sistemas.

Zadeh et al. (2023) apresentam uma estrutura inovadora para a quantificação e classificação de riscos cibernéticos, baseada em análise de conteúdo e matrizes de impacto e probabilidade. Watson e Jones (2024) reforçam a importância dos Sistemas de Gestão de Segurança da Informação, com definição clara de funções, responsabilidades e processos. Singh et al. (2025) argumentam que a resiliência cibernética é essencial para sustentar a inovação organizacional em contextos de instabilidade macroeconómica, sendo influenciada por políticas públicas e pela eficácia da governação. Por fim, Büyüközkan e Güler (2025) propõem um modelo de maturidade em cibersegurança, composto por cinco dimensões e quinze factores, validado empiricamente, que visa apoiar as organizações na avaliação da sua prontidão cibernética.

3.4. Modelos de Maturidade e Quadro Conceptual

O desenvolvimento de modelos e referenciais teóricos tem desempenhado um papel fundamental na consolidação da resiliência digital como campo de investigação aplicada. Entre os principais modelos utilizados para **avaliar a maturidade digital** e a **capacidade de resposta institucional** em contextos de crise, destacam-se:

- **Cybersecurity Maturity Model (CMM)** (University of Oxford, 2021): Trata-se de uma estrutura metodológica desenvolvida pelo *Global Cyber Security Capacity Centre* da Universidade de Oxford, que permite avaliar o grau de preparação de uma organização ou país em matéria de cibersegurança. O modelo está estruturado em cinco dimensões — políticas públicas, cultura de cibersegurança, formação, enquadramento legal e controlo de riscos — e fornece um roteiro para identificar lacunas, orientar melhorias e reforçar a postura de segurança digital.
- **Cloud Capability Maturity Model (CCMM)** (Moonasar & Naicker, 2020): Este modelo avalia a capacidade de uma organização para adoptar soluções de computação em nuvem de forma segura, escalável e resiliente. Embora menos padronizado do que o CMM, o CCMM é amplamente utilizado em ambientes corporativos e governamentais para orientar a transição para infraestruturas digitais baseadas em nuvem.
- **Task–Technology Fit (TTF)** (Goodhue & Thompson, 1995): Este modelo analisa a adequação entre as tarefas organizacionais e as tecnologias utilizadas, partindo do pressuposto de que a eficácia dos sistemas digitais depende da sua capacidade de suportar as exigências específicas do trabalho. Em contextos de crise, essa correspondência torna-se ainda mais crítica, influenciando directamente a continuidade e a eficiência dos serviços públicos.
- **Teoria da Capacidade Dinâmica** (Teece, Pisano & Shuen, 1997): Esta teoria procura explicar como as organizações desenvolvem e reconfiguram competências para responder a ambientes em constante mudança. Aplica-se a contextos de inovação, transformação digital e resiliência organizacional. No sector público, esta capacidade é essencial para garantir a resiliência institucional face a eventos disruptivos, como desastres naturais ou ciberataques.

- **UTAUT –** ***Unified Theory of Acceptance and Use of Technology*** (Venkatesh, Morris, Davis & Davis, 2003): Esta teoria integra elementos de modelos anteriores de aceitação tecnológica e é utilizada para estudar a adopção de tecnologias em ambientes organizacionais, incluindo o sector público. Permite compreender os factores que influenciam a aceitação e utilização de tecnologias por parte dos trabalhadores, sendo um elemento-chave para o sucesso de estratégias de continuidade digital, especialmente em situações de emergência.

Estes referenciais teóricos e modelos de maturidade oferecem uma base sólida para a construção de indicadores empíricos de resiliência digital e para a formulação de políticas públicas baseadas em evidência. A sua aplicação permite não apenas diagnosticar fragilidades, mas também orientar investimentos estratégicos em infraestruturas, formação e práticas de governação digital.

3.5. Experiências em Governação Digital e Resiliência Urbana

A intensificação dos riscos urbanos, impulsionada por alterações climáticas, ciberameaças e eventos extremos, tem levado diversas cidades a adoptar soluções digitais como instrumentos estratégicos de resiliência (Arup & Resilient Cities Network, 2023). A governação digital, aliada a tecnologias emergentes como drones, plataformas colaborativas e dados abertos, tem demonstrado potencial para reforçar a capacidade de resposta dos governos locais em contextos de crise.

Em Sydney, a plataforma *Resilient Sydney* permite aos municípios aceder a dados georreferenciados para planear intervenções climáticas (City of Sydney, 2025). Em Salónica, um ataque de *ransomware* ocorrido em 2021 conduziu à reformulação dos sistemas digitais e à partilha de boas práticas com outras cidades da rede *R-Cities*, evidenciando a importância de planos de continuidade e de formação em cibersegurança

(Resilient Cities Network, 2023). A cidade de Haia promove anualmente o *evento "Hack The Hague"*, no qual hackers éticos testam os sistemas públicos (Municipality of The Hague, 2023). Em Dar es Salaam, estudantes recorreram a drones e à ciência cidadã para mapear zonas vulneráveis, contribuindo para decisões urbanas mais informadas (World Bank, 2022). No Brasil, o Centro de Operações do Rio de Janeiro (COR) integra sensores e plataformas digitais para coordenar respostas a emergências (Prefeitura do Rio de Janeiro, 2023). Outras iniciativas incluem o uso de dados de mobilidade em Chennai para identificar desigualdades no acesso à saúde (UN-Habitat, 2021), vales digitais na Cidade do Cabo (UNDP, 2021), apoio digital a produtores em Quito (FAO, 2022) e soluções de ensino remoto em Minneapolis (City of Minneapolis, 2021).

Estes exemplos demonstram que a resiliência urbana exige abordagens integradas e adaptativas, com ênfase na interoperabilidade, na participação comunitária e na adopção de tecnologias emergentes, como gémeos digitais, *blockchain* e inteligência artificial (OECD, 2023).

3.6. Inclusão Digital e Sustentabilidade

Um dos principais desafios da digitalização da administração pública consiste em evitar o agravamento da exclusão social em contextos de crise. A resiliência digital deve ser concebida de forma inclusiva, assegurando o acesso equitativo às tecnologias e promovendo a literacia digital, especialmente em regiões vulneráveis do Sul Global (Arup & Resilient Cities Network, 2023).

3.7. Diretrizes para uma Resiliência Digital Escalável

A resiliência digital escalável constitui um elemento essencial para garantir a continuidade dos serviços públicos em contextos de crise. No sector financeiro público, esta deve abranger tanto a protecção das infraestruturas digitais como a capacidade de

adaptação institucional perante disrupções sistémicas, tais como ciberataques e desastres naturais (Pritchard et al., 2023).

- **Cópias de segurança e computação em nuvem.** A replicação de dados em tempo real e a manutenção de cópias de segurança distribuídas geograficamente são práticas fundamentais para assegurar a integridade dos sistemas. A migração para arquitecturas em nuvem com mecanismos de *failover* automático, aliada à utilização de inteligência artificial para a deteção preditiva de anomalias, permite respostas mais ágeis e eficazes (Yan & Khoei, 2025. Repetto, 2023).

- **Formação e testagem**. A formação contínua dos profissionais da administração pública em áreas como a cibersegurança e a gestão de crises revela-se essencial para o reforço da resiliência organizacional. A realização de testes periódicos de continuidade operacional permite identificar vulnerabilidades e avaliar o grau de maturidade digital, através de indicadores como o Tempo Médio de Recuperação (MTTR) e o Tempo Médio de Deteção de Incidentes (MTTD) (Mouratidis et al., 2023. Conrad et al., 2023).

- **Governação e inclusão**. A interoperabilidade entre sistemas administrativos exige a adopção de padrões abertos e de enquadramentos jurídicos adequados para a partilha de informação. Simultaneamente, a inclusão digital deve ser promovida como um pilar da equidade, garantindo o acesso universal a dispositivos, conectividade e competências digitais, especialmente em momentos críticos (Mosharraf, 2025. Resilient Cities Network, 2023).

- **Parcerias e avaliação**. A cooperação entre os sectores público e privado deve ser formalizada através de protocolos padronizados para actuação conjunta em emergências. Esta articulação facilita a mobilização de recursos e a recuperação de serviços essenciais. A eficácia das estratégias de resiliência deve ser monitorizada com base em métricas

adequadas, tais como o *Recovery Time Objective* (RTO), o *Recovery Point Objective* (RPO), o Índice de Maturidade em Ciberresiliência (CRMI) e os índices de literacia digital (Beuchelt, 2025. Pritchard et al., 2023).

3.8. Reflexão Crítica sobre Computação em Nuvem e Soberania Digital

A crescente adopção de soluções de computação em nuvem por parte das instituições públicas tem gerado benefícios significativos em termos de escalabilidade, disponibilidade e eficiência operacional. Contudo, esta migração suscita preocupações relevantes no que respeita à soberania digital e à privacidade dos dados. A dependência de grandes fornecedores globais pode comprometer a autonomia tecnológica das entidades governamentais, sobretudo quando os dados sensíveis são armazenados em servidores localizados fora do território nacional.

Acresce que o cumprimento das disposições do Regulamento Geral sobre a Protecção de Dados (RGPD) representa um desafio adicional, exigindo garantias de que os dados dos cidadãos são tratados com segurança, transparência e em conformidade com a legislação aplicável. Assim, é imperativo que as estratégias de resiliência digital considerem não apenas os aspectos técnicos da interoperabilidade, mas também os riscos jurídicos e geopolíticos associados à terceirização das infraestruturas digitais.

4. Metodologia e Recolha de Dados

Este estudo adopta uma abordagem qualitativa de natureza exploratória, adequada à complexidade e multidimensionalidade da resiliência digital no sector financeiro público em contextos de crise. A investigação parte do pressuposto de que a resiliência digital transcende métricas técnicas, exigindo uma análise aprofundada das estruturas organizacionais, das capacidades institucionais e das práticas de governação,

especialmente em situações extremas, como desastres naturais (Bryman, 2016. Boin & McConnell, 2022). O **objectivo central** consiste em identificar fragilidades e respostas adaptativas do sistema financeiro público face às cheias ocorridas em 2024 no Estado do Rio Grande do Sul.

4.1. Desenho de Investigação

A metodologia foi estruturada em três etapas complementares:

- Revisão sistemática da literatura académica e institucional.
- Estudo de caso centrado na inundação de 2024 no Estado do Rio Grande do Sul.
- Análise documental de políticas públicas, relatórios técnicos e estratégias de ciber-resiliência.

4.2. Revisão de Literatura

A revisão bibliográfica incidiu sobre publicações científicas produzidas entre 2020 e 2025, com destaque para bases de dados académicas como a Elsevier. Foram seleccionados 178 artigos relacionados com cibersegurança, transformação digital, governação, cidades inteligentes e continuidade de negócios, com base em critérios de relevância temática, rigor metodológico e actualidade.

4.3. Estudo de Caso: Inundação de 2024 no Rio Grande do Sul

O estudo empírico centra-se no desastre climático ocorrido entre Abril e Maio de 2024, considerado o maior evento hidrológico da história recente do Brasil (CEPAL et al., 2024). A selecção do caso baseou-se no impacto significativo sobre os sistemas financeiros públicos, na disponibilidade de dados técnicos e no potencial de aprendizagem institucional. Foram analisados documentos provenientes de entidades

como o Governo do Estado, a Secretaria da Fazenda, o BID, o IBGE, o INMET, universidades locais e fontes jornalísticas validadas (G1, 2025).

4.4. Análise Documental

A análise documental constituiu uma técnica central para a recolha e interpretação de dados, permitindo o acesso a mais de 60 documentos, incluindo: *Planos de Continuidade de Negócios* (PCN) e de *Recuperação de Desastres* (PRD). relatórios técnicos de órgãos como a SEFAZ, a PROCERGS, a Defesa Civil, o TCE-RS e a SICT. decretos, portarias e notas técnicas. avaliações de danos (CEPAL, 2024. BID, 2024). e publicações sobre governação digital e ciber-resiliência.

A análise foi conduzida em quatro fases: selecção documental (2020–2025), codificação temática (por exemplo, continuidade de serviços, interoperabilidade, maturidade digital), análise comparativa entre diferentes níveis de governo e triangulação com literatura e dados empíricos. Recorreu-se a software de análise qualitativa para visualizar co-ocorrências temáticas e reforçar a objectividade da interpretação.

Os resultados preliminares revelaram: diferentes níveis de maturidade nos planos de continuidade. fragilidades na interoperabilidade. avanços na digitalização fiscal e orçamental. e a necessidade de maior integração entre políticas de cibersegurança e estratégias de gestão de riscos climáticos.

4.5. Limitações Metodológicas

As principais limitações identificadas foram:

- Inexistência de entrevistas presenciais, colmatada por fontes secundárias e pela experiência profissional da autora.
- Avaliação indirecta da maturidade digital, baseada exclusivamente em documentação.

- Foco geográfico restrito ao Estado do Rio Grande do Sul, o que limita a generalização dos resultados.

Apesar destas limitações, a triangulação metodológica conferiu robustez analítica e sustentação empírica às conclusões do estudo.

5. Análise dos Resultados

As inundações ocorridas em Abril e Maio de 2024 no Estado do Rio Grande do Sul constituíram um dos mais graves eventos climáticos da história recente do Brasil, afectando quase todos os municípios e mais de 2,3 milhões de pessoas. Os prejuízos económicos, sociais e ambientais foram estimados em 88,9 mil milhões de reais (CEPAL, BID & Banco Mundial, 2024). Para além da destruição física, a crise revelou a profunda interdependência entre sistemas físicos, sociais e digitais, comprometendo a continuidade dos serviços públicos, com especial incidência nos serviços financeiros.

Este capítulo procede à análise dos impactos da crise sobre a infraestrutura digital e os serviços financeiros do sector público, com base em dados empíricos recolhidos junto do Governo do Estado, em documentos técnicos e em observação participante. Identificam-se vulnerabilidades estruturais, práticas resilientes e lições que contribuem para o desenvolvimento de um modelo escalável de resiliência digital, articulando os conceitos de continuidade operacional, governação adaptativa e maturidade digital.

5.1. Impactos sobre os Sistemas Financeiros Públicos

A infraestrutura financeira foi severamente afectada pela interrupção do fornecimento de energia, da conectividade e do acesso aos centros de dados. Mais de 580 mil pessoas ficaram desalojadas e cerca de 880 mil necessitaram de apoio financeiro urgente (BID, 2024). Os principais impactos registados incluem:

- Inacessibilidade aos sistemas de pagamento e de arrecadação.
- Suspensão de transferências bancárias e de repasses a municípios e fornecedores.
- Atrasos no processamento de salários e na concessão de benefícios sociais.
- Paralisia de processos orçamentais e de contratação pública, em virtude da dependência de sistemas digitais.
- A inexistência de cópias de segurança georredundantes e de planos de contingência actualizados resultou na interrupção total de serviços em municípios mais afectados, por períodos superiores a dez dias.

5.2. Resposta Institucional: Acções Emergenciais

Perante a crise, foram adoptadas quatro estratégias principais:

- **Soluções Tecnológicas Temporárias**: Activação de sistemas de pagamento emergenciais em ambiente de nuvem e contratação de pessoal temporário.
- **Parcerias Público–Privadas**: Estabelecimento de acordos com instituições bancárias e *fintechs*, que asseguraram a continuidade mínima dos serviços financeiros.
- **Reforço da Governação Digital**: Implementação de medidas como a expansão da nuvem híbrida com mecanismos de *failover* automático, elaboração de novos *Planos de Continuidade de Negócios* (PCN) e constituição de equipas locais para resposta a incidentes digitais (Secretaria da Fazenda do RS, 2024).
- **Restabelecimento da Conectividade**: As operadoras disponibilizaram redes para roaming gratuito (*Conexis Brasil Digital*), enquanto o satélite Amazonia 1 e antenas *Starlink* auxiliaram na comunicação em áreas isoladas. A Agência Nacional de Telecomunicações (Anatel) coordenou a recuperação da infraestrutura e implementou o sistema Defesa Civil Alerta, baseado na tecnologia *Cell Broadcast* (Anatel, 2024).

Estas acções evidenciam o papel estratégico das telecomunicações na gestão de desastres, bem como a importância da articulação entre tecnologia, solidariedade e políticas públicas.

5.3. Lições sobre Vulnerabilidades Estruturais

A crise climática de 2024 no Estado do Rio Grande do Sul revelou fragilidades estruturais significativas na arquitectura digital do sector público, comprometendo a continuidade dos serviços financeiros. Destacam-se cinco vulnerabilidades principais:

- **Centralização de Infraestruturas Críticas:** A inundação da sede da PROCERGS, localizada em zona de risco, levou ao desligamento do único centro de dados estadual, afectando serviços essenciais como o processamento salarial e a arrecadação tributária. A ausência de distribuição geográfica da infraestrutura aumentou a exposição ao risco (Convergência Digital, 2024).
- **Inexistência de conectividade alternativa:** A falta de soluções complementares, como satélites ou redes móveis de reserva, obrigou à adopção de medidas reactivas, como o *roaming* gratuito e o uso de antenas Starlink, evidenciando a ausência de planeamento prévio (Anatel, 2024).
- **Planos de continuidade desactualizados ou inexistentes:** A PROCERGS não dispunha de um *Plano de Recuperação de Desastres* (PRD) funcional, o que dificultou a resposta imediata. Auditoria realizada pelo Tribunal de Contas do Estado do Rio Grande do Sul confirmou a inexistência de testes periódicos e a ausência de integração da continuidade na governação estratégica (TCE-RS, 2025).
- **Falta de interoperabilidade entre sistemas estaduais e municipais:** A inexistência de padrões comuns e de plataformas integradoras impediu a migração

emergencial de dados e processos, comprometendo a prestação de serviços essenciais (Governo Digital, 2024. Enap, 2025).

- **Baixa maturidade digital em municípios de menor dimensão**: Diversos municípios operavam com *software* local, sem cópias de segurança em nuvem e sem recursos técnicos ou humanos suficientes para assegurar a continuidade digital. A escassez de investimentos e de formação técnica limita a adopção de soluções modernas, exigindo políticas públicas específicas para promover a inclusão digital e a segurança da informação (Secretaria de Governo Digital, 2022).

Estas vulnerabilidades enquadram-se nas denominadas "falhas em cascata", nas quais a interrupção de um sistema crítico afecta simultaneamente múltiplos serviços (Arup & Resilient Cities Network, 2023). A crise evidenciou a urgência de investimentos em infraestruturas resilientes, interoperabilidade e planeamento estratégico multissectorial.

5.4. Práticas Resilientes Identificadas

Apesar das limitações estruturais, algumas entidades públicas demonstraram capacidade de adaptação durante a crise de 2024. Destacam-se as seguintes práticas:

- Utilização prévia de computação em nuvem com replicação geográfica, como no município de Santa Cruz do Sul, o que permitiu assegurar a continuidade dos serviços financeiros (Plano Rio Grande, 2025).
- Realização prévia de simulações de desastres digitais, que possibilitaram respostas rápidas e coordenadas.
- Cooperação intermunicipal através de consórcios, viabilizando a partilha de infraestruturas digitais.
- Utilização de redes móveis e satelitais para restabelecer a conectividade administrativa.

- Automatização de processos financeiros críticos, como o processamento salarial e os registos contabilísticos.

Estas práticas evidenciam a importância de políticas públicas que incentivem o uso de tecnologias resilientes, a realização de testes regulares e a promoção da integração federativa.

5.5. Padrões Emergentes de Resiliência Digital

A resiliência institucional depende da capacidade de manter funções essenciais em cenários de crise. Quatro princípios fundamentais sustentam essa capacidade (Boin & McConnell, 2022):

- **Redundância:** Disponibilidade de recursos duplicados, como centros de dados espelhados e múltiplos fornecedores de conectividade.
- **Flexibilidade:** Capacidade de reconfigurar processos e estruturas de forma célere e eficaz.
- **Adaptação:** Aprendizagem em tempo real, com ajustamento contínuo das estratégias em função do contexto.
- **Integração institucional:** Coordenação efectiva entre diferentes níveis e sectores da administração pública.

A aplicação destes princípios exige planeamento estratégico, investimento em capacidades organizacionais e o desenvolvimento de uma cultura institucional orientada para a prevenção e a antecipação de riscos.

5.6. O Plano Rio Grande

O *Plano Rio Grande*, lançado em Maio de 2024, constitui uma resposta estruturada às cheias que afectaram o Estado, com enfoque na reconstrução, adaptação e promoção da resiliência climática. A iniciativa está organizada em quatro eixos estratégicos:

- Diagnóstico e Governação.
- Emergência e Recuperação.
- Adaptação e Resiliência.
- Integração e Sustentabilidade.

O plano prevê investimentos superiores a 8 mil milhões de reais, provenientes de recursos estaduais, federais e internacionais. Entre os projectos estratégicos destacam-se a modernização dos sistemas de Tecnologias de Informação e Comunicação (TIC), a realocação de comunidades vulneráveis e a criação de fundos permanentes para resposta a desastres (Plano Rio Grande, 2025).

5.7. Soluções Digitais para o Enfrentamento das Cheias

Em Setembro de 2024, o Governo do Estado apresentou um conjunto de soluções digitais com o objectivo de reforçar a resposta pública às cheias. Entre as iniciativas destacam-se:

- **Mapa Único do Plano Rio Grande:** Plataforma digital destinada à identificação de áreas afectadas e à distribuição de benefícios, como o PIX SOS e o programa Volta por Cima.
- **MEI RS Calamidades**: Programa de apoio a microempreendedores individuais em situação de calamidade.
- **Rodadas de Conexão:** Iniciativa da Secretaria de Inovação, Ciência e Tecnologia (SICT), que reuniu 46 soluções tecnológicas voltadas para a gestão de abrigos, resíduos e reconstrução urbana.

Estas acções demonstram o potencial da inovação digital para fortalecer a capacidade de resposta do poder público em contextos de emergência (Secretaria de Governo Digital do RS, 2024).

5.8. Considerações Finais da Análise

A crise de 2024 evidenciou que a resiliência digital no sector financeiro público permanece incipiente e desigual. A maioria dos sistemas não estava preparada para enfrentar um evento de tal magnitude. No entanto, emergiram práticas adaptativas que apontam caminhos promissores para a construção de um modelo unificado, escalável e interoperável.

Recomenda-se a incorporação de práticas como a computação em nuvem, mecanismos de *failover* automatizado, cópias de segurança regionais, testes regulares de continuidade e cooperação intersectorial. A crise deve ser encarada como um marco de inflexão na arquitectura digital do Estado, exigindo uma reconfiguração estratégica orientada para a prevenção, a robustez e a adaptabilidade institucional.

6. Conclusões

A presente investigação permitiu compreender, de forma aprofundada, os desafios e as oportunidades inerentes à construção da resiliência digital no sector público financeiro em contextos de catástrofe. A análise do caso empírico da inundação de 2024 no Estado do Rio Grande do Sul revelou que, apesar dos avanços significativos na digitalização da administração pública, persistem fragilidades estruturais, institucionais e tecnológicas que comprometem a continuidade dos serviços em situações de crise.

A resiliência digital, conforme definida por Arup & Resilient Cities Network (2023), transcende a robustez técnica dos sistemas, envolvendo uma capacidade organizacional integrada de antecipar, resistir, adaptar-se e recuperar-se de eventos disruptivos. No contexto analisado, verificou-se que a inexistência de planos de continuidade actualizados, a centralização excessiva de servidores físicos e a baixa interoperabilidade

entre sistemas estaduais e municipais foram factores determinantes para a interrupção de serviços essenciais, como o pagamento de salários, as transferências sociais e a execução orçamental (TCE-RS, 2025. BID, 2024).

Por outro lado, a investigação identificou práticas resilientes que evidenciam o potencial de adaptação institucional. A utilização de soluções em nuvem, a activação de redes alternativas de conectividade e a cooperação interinstitucional emergencial revelaram-se estratégias eficazes para mitigar os impactos da crise (Plano Rio Grande, 2025). Estas respostas, ainda que pontuais, demonstram a importância de uma abordagem sistémica e proactiva para a construção de uma resiliência digital escalável.

Conclui-se, assim, que a resiliência digital no sector público financeiro deve ser entendida como uma competência estratégica, que exige:

- Infraestruturas tecnológicas distribuídas e seguras.
- Planeamento de continuidade de negócios com testes regulares.
- Formação contínua dos trabalhadores da administração pública.
- Governação digital colaborativa e intersectorial.
- Inclusão digital como vector de equidade e justiça social.

A crise deve ser encarada como um marco de inflexão na arquitectura digital do Estado. Não se trata apenas de corrigir falhas pontuais, mas de repensar estruturalmente os modelos de governação digital, assumindo a inevitabilidade de futuras disrupções — sejam elas climáticas, tecnológicas ou sociopolíticas (Boin & McConnell, 2022).

6.1. Respostas às Perguntas de Investigação

Questão de Investigação Principal

Como pode a resiliência digital reforçar a continuidade e a robustez dos serviços financeiros públicos em contextos de catástrofe?

A resiliência digital pode ser promovida através da adopção de um modelo analítico adaptativo, sustentado por indicadores como o *Recovery Time Objective* (RTO), o *Recovery Point Objective* (RPO), o Índice de Maturidade em Ciberresiliência (CRMI), a literacia digital, o *Mean Time to Detect* (MTTD) e o *Mean Time to Recovery* (MTTR). A integração institucional e o reforço da interoperabilidade são fundamentais para mitigar riscos e assegurar a continuidade operacional. A formação em literacia digital e o uso estratégico de tecnologias emergentes contribuem significativamente para o fortalecimento da resiliência.

Subquestões

1. **Quais as vulnerabilidades reveladas pela crise de 2024 no Rio Grande do Sul?**

- Centralização excessiva de servidores físicos.
- Inexistência de conectividade alternativa.
- Falta de interoperabilidade entre sistemas estaduais e municipais.
- Baixa maturidade digital em municípios de menor dimensão.

2. **Que práticas institucionais contribuíram para a continuidade operacional?**

- Migração emergencial para a nuvem.
- Estabelecimento de parcerias com bancos e *fintechs*.
- Utilização de canais alternativos de comunicação.
- Recuperação manual de dados com base em cópias de segurança locais.

3. **Como podem modelos internacionais de maturidade digital ser aplicados ao contexto brasileiro?**

- Adaptando referenciais como o CMM, CCMM, TTF e UTAUT à realidade institucional.
- Utilizando esses modelos para diagnóstico, planeamento e priorização de investimentos.

4. **Que indicadores e orientações podem apoiar a formulação de políticas de governação digital resiliente?**

- RTO, RPO, CRMI, MTTD, MTTR e literacia digital.
- Orientações sobre cópias de segurança, *failover,* interoperabilidade e formação contínua.

6.2. Contributos do Estudo

Este trabalho oferece contributos relevantes em três dimensões:

a) Teórica

- Integração entre os campos da cibersegurança, da governação digital, da engenharia de sistemas críticos e da administração pública.
- Proposição de um modelo analítico de resiliência digital adaptativa, com base em referenciais como o CMM (Oxford, 2021), TTF (Goodhue & Thompson, 1995) e UTAUT (Venkatesh et al., 2003).

b) Metodológica

- Aplicação de uma abordagem qualitativa, com triangulação entre revisão sistemática, estudo de caso e análise documental, conforme o Guia de Elaboração de TFM.
- Utilização de codificação temática e análise comparativa entre diferentes níveis de governo.
-

c) Prática

- Sistematização de práticas resilientes observadas durante a crise.
- Formulação de recomendações operacionais para assegurar a continuidade digital em contextos de emergência.
- Proposta de indicadores de maturidade digital e de orientações para planos de contingência adaptáveis à realidade brasileira.

6.3. Sugestões para Investigações Futuras

A investigação abre caminho para novos estudos, entre os quais se destacam:

- Análises comparativas entre estados ou países que enfrentaram eventos climáticos semelhantes.
- Estudos longitudinais sobre a implementação de planos de continuidade digital.
- Modelação de indicadores de maturidade digital específicos para o sector público financeiro.
- Investigação empírica com entrevistas e questionários aplicados a trabalhadores da administração pública.
- Estudos aplicados em municípios de pequeno e médio porte, com enfoque na inclusão digital e na automatização de processos financeiros.

Considerações Finais

A transição para uma administração pública mais digitalizada exige mais do que inovação tecnológica. Requer planeamento institucional, adaptação contínua e sensibilidade social. A resiliência digital, neste sentido, não constitui um destino, mas sim uma jornada — um processo gradual de construção de capacidades que permita aos governos responder de forma eficaz, equitativa e ética perante um futuro cada vez mais incerto e interdependente (Singh et al., 2025).

A experiência vivida no Estado do Rio Grande do Sul deve servir como alerta e fonte de aprendizagem. Quanto mais cedo os entes públicos investirem em robustez digital, interoperabilidade, segurança e governação, menores serão os custos humanos, sociais e económicos das crises futuras.

Referências Bibliográficas

1. Artigos publicados em periódicos (revistas científicas)

Ali, M., Rahman, S. & Li, J. (2025). *Integrating multimodal data for real-time cyber threat detection.* *Computers & Security*, 130, 103745.

Atıcı, M. & Tuna, G. (2025). *Cyber resilience in public sector infrastructures: Managing disruptions and recovery.* *Journal of Public Information Systems*, 31(1), 55–78.

Basu, R. (2023). *Autonomous diagnostic systems for resilient infrastructures.* *Information Systems Frontiers*, 25(3), 122–140.

Beuchelt, T. (2025). *Aligning information security strategies with operational resilience goals.* *Information & Management*, 62(4), 111032.

Boin, A. & Lodge, M. (2020). *Designing resilient institutions for transboundary crisis management.* *Public Administration*, 98(4), 940–955.

Boin, A. & McConnell, A. (2022). *Institutional resilience and adaptive governance in crisis times.* *Policy Sciences*, 55(3), 321–340.

Büyüközkan, G. & Güler, M. (2025). *A cyber maturity model for public institutions.* *Government Information Quarterly*, 42(1), 65–83.

Chen, L., Zhang, Y. & Pereira, M. (2025). *Digitalization and resilience in public administrations: Continuity challenges in the Global South.* *Government Information Quarterly*, 42(2), 223–245.

Conrad, D., Feldman, A. & Sato, R. (2023). *Digital continuity and disaster recovery in urban governance.* *Urban Governance Journal*, 9(3), 187–203.

Fu, W. (2024). *Redundant real-time controllers for resilient systems.* *IEEE Transactions on Systems, Man and Cybernetics*, 54(2), 345–358.

Goodhue, D. & Thompson, R. (1995). *Task-Technology Fit and individual performance.* *MIS Quarterly*, 19(2), 213–236.

Mouratidis, H., Kalloniatis, C. & Gritzalis, S. (2023). *Integrating security and resilience in digital infrastructures.* *Information Systems Frontiers*, 25(2), 245–260.

Oliveira, J., Santos, M. & Paiva, C. (2024). *Continuity and resilience in Brazilian public finance: Lessons from the 2024 flood.* *Revista Brasileira de Administração Pública*, 58(4), 455–478.

Pritchard, R., Hayes, L. & Torfs, E. (2023). *Evaluating scalable models of digital resilience.* *Information Policy Review*, 27(4), 415–430.

Singh, A., Patel, R. & Gomes, L. (2025). *Cyber resilience and innovation under macroeconomic instability.* *International Journal of Public Administration in the Digital Age*, 12(2), 77–95.

Teece, D., Pisano, G. & Shuen, A. (1997). *Dynamic capabilities and strategic management.* *Strategic Management Journal*, 18(7), 509–533.

Venkatesh, V., Morris, M., Davis, G. & Davis, F. (2003). *User acceptance of information technology: Toward a unified view.* *MIS Quarterly*, 27(3), 425–478.

Watson, K. & Jones, P. (2024). *Information security governance frameworks for digital resilience.* *Computers & Security*, 125, 102823.

Zadeh, S., Mendez, R. & Karlsson, P. (2023). *Quantifying cyber risk and probability of failure in smart infrastructures.* *Journal of Risk Analysis*, 43(2), 78–94.

2. Livros e monografias

Bryman, A. (2016). *Social Research Methods*, 5.ª Ed. Oxford: Oxford University Press.

Costa, L.F.P. (2013). *Regras para apresentação de trabalhos escritos no ISEG.* Lisboa: Instituto Superior de Economia e Gestão.

3. Fontes de dados e relatórios institucionais

Agência das Nações Unidas para Assentamentos Humanos (ONU-Habitat) (2023). *Digital governance and local resilience: global practices and lessons.* Nairobi: ONU-Habitat.

Anatel – Agência Nacional de Telecomunicações (2024). *Relatório de recuperação das comunicações pós-enchente 2024.* Brasília: Anatel.

Arup & Resilient Cities Network (2023). *Digital Cities, Resilient Cities: Delivering Urban Resilience Through Digital Solutions.* Nova Iorque: R-Cities.

Banco Interamericano de Desenvolvimento (BID) (2024). *Infraestrutura crítica e resiliência digital no Brasil.* Washington: BID.

CEPAL, BID & Banco Mundial (2024). *Impactos socioeconómicos das inundações no Rio Grande do Sul.* Santiago do Chile: CEPAL.

City of Sydney (2025). *Resilient Sydney Platform.* Sydney: City of Sydney.

Convergência Digital (2024). *Cheias no RS paralisam centro de dados da PROCERGS.* [Base jornalística]. Disponível em: https://www.convergenciadigital.com.br [Acesso em: 20/06/2025].

Enap – Escola Nacional de Administração Pública (2025). *Relatório sobre a maturidade digital dos municípios brasileiros.* Brasília: ENAP.

FAO – Food and Agriculture Organization (2022). *Quito Digital Farmers Project.* Roma: FAO.

G1 (2025). *Enchentes no RS e impacto sobre os serviços públicos.* [Base jornalística]. Disponível em: https://g1.globo.com [Acesso em: 10/07/2025].

Governo Digital (2024). *Relatório de Interoperabilidade e Governação Digital.* Brasília: Ministério da Gestão e Inovação.

Instituto Nacional de Estatística (INE) (2023). *Estatísticas do ambiente e território 2023.* Lisboa: INE.

OECD – Organisation for Economic Co-operation and Development (2019). *Good Governance for Critical Infrastructure Resilience.* Paris: OECD.

OECD – Organisation for Economic Co-operation and Development (2023). *Urban Resilience and Digital Innovation.* Paris: OECD.

Oxford – University of Oxford, Global Cyber Security Capacity Centre (2021). *Cybersecurity Maturity Model (CMM).* Oxford: University of Oxford.

Plano Rio Grande (2025). *Estratégia de reconstrução e resiliência do RS.* Porto Alegre: Governo do Estado do Rio Grande do Sul.

PROCERGS (2023). *Relatório técnico de migração para cloud e resiliência digital.* Porto Alegre: Companhia de Processamento de Dados do Estado do Rio Grande do Sul.

Resilient Cities Network (2023). *Cybersecurity lessons from urban ransomware attacks.* Nova Iorque: R-Cities.

Secretaria da Fazenda do RS (2023). *Relatório Anual de Atividades.* Porto Alegre: SEFAZ-RS.

Secretaria da Fazenda do RS (2024). *Planos de continuidade digital pós-enchente.* Porto Alegre: SEFAZ-RS.

Secretaria de Governo Digital (2022). *Política Nacional de Governo Digital.* Brasília: Ministério da Economia.

Secretaria de Governo Digital do RS (2024). *Soluções digitais para enfrentamento das cheias.* Porto Alegre: SICT.

TCE-RS – Tribunal de Contas do Estado do Rio Grande do Sul (2025). *Relatório de auditoria sobre continuidade digital da PROCERGS.* Porto Alegre: TCE-RS.

UNDP – United Nations Development Programme (2021). *Digital Vouchers for Social Protection in Cape Town.* Nova Iorque: UNDP.

UNDRR – United Nations Office for Disaster Risk Reduction (2022). *Global Assessment Report on Disaster Risk Reduction.* Nova Iorque: UNDRR.

World Bank (2022). *Community-based resilience mapping in Dar es Salaam.* Washington: World Bank.

Anexo I – Proposta de Plano de Contingência para a Resiliência Digital na Prestação de Serviços Públicos Financeiros

Introdução

O presente plano tem como finalidade assegurar a continuidade dos serviços financeiros públicos essenciais em cenários de disrupção digital provocados por desastres naturais, falhas de infraestrutura ou ciberataques. Este documento está alinhado com as diretrizes internacionais de ciber-resiliência e responde às vulnerabilidades identificadas durante a inundação ocorrida em 2024 no estado do Rio Grande do Sul.

Objectivos Estratégicos

- Garantir a disponibilidade e integridade dos dados financeiros críticos.
- Assegurar a continuidade operacional dos serviços financeiros essenciais.
- Minimizar os impactos reputacionais, fiscais e sociais decorrentes de falhas digitais.
- Estabelecer protocolos claros de resposta e recuperação.
- Promover uma cultura organizacional resiliente, centrada na antecipação e adaptação.

Riscos Identificados

- Falhas em sistemas críticos de Tecnologias da Informação e Comunicação (TIC), como os de processamento salarial, pagamentos e arrecadação.
- Inacessibilidade a sistemas devido a danos físicos ou ciberataques.
- Interrupção de pagamentos e serviços essenciais, com impacto social direto.

Estratégias de Mitigação

Para mitigar os riscos identificados, devem ser implementadas as seguintes estratégias:

- **Infraestrutura redundante e descentralizada**: utilização de centros de dados espelhados em diferentes regiões e armazenamento em nuvem híbrida.
- **Backups regulares e acessíveis:** realização de cópias de segurança automáticas e frequentes dos dados financeiros críticos.
- **Planos de acção offline:** desenvolvimento de modos de operação offline para garantir a continuidade dos pagamentos.
- **Formação e simulações:** formação contínua da equipa financeira para actuação em cenários de falha digital.
- **Cibersegurança robusta**: monitorização contínua de ameaças e actualizações regulares dos sistemas.
- **Interoperabilidade e portabilidade de dados**: sistemas que permitam a migração rápida de dados entre plataformas.

Plano de Contingência

Em caso de falha digital, será implementado o seguinte plano de acção offline:

- Activação de protocolos de atendimento manual, com recurso a registos físicos e backups offline para verificação e autorização de pagamentos.
- Estabelecimento de pontos de contacto alternativos para a equipa financeira.
- Utilização de backups offline para acesso a dados críticos.
- Comunicação directa com instituições bancárias e fornecedores para garantir a continuidade dos pagamentos.
- Comunicação com fornecedores e trabalhadores por canais alternativos.
- Monitorização contínua da situação e actualização dos procedimentos conforme necessário.

Etapas do Plano

Etapa	Acção
Activação emergencial	Avaliação do cenário e decisão de activação do plano
Comunicação inicial	Informação às equipas-chave e instituições parceiras
Execução de pagamentos	Emissão manual de ordens e envio por canal alternativo ao banco
Registo e rastreabilidade	Registo físico e digital posterior de todas as transacções realizadas
Retomada de sistemas	Restauro gradual com verificação da integridade dos dados

Backup e Recuperação

Os dados críticos serão armazenados em sistemas de *backup* seguros e acessíveis. Os procedimentos incluem:

- Realização de *backups* diários dos dados financeiros críticos.
- Armazenamento seguro dos *backups* em locais geograficamente distintos.
- Testes periódicos de recuperação de desastres para garantir a integridade e acessibilidade dos dados.
- Documentação detalhada dos procedimentos de recuperação e das respectivas responsabilidades.

Responsabilidades

A implementação, execução e manutenção do plano de contingência serão distribuídas da seguinte forma:

- **Equipa de TIC:** garantir a infraestrutura e a segurança dos sistemas financeiros.
- **Equipa Financeira**: executar os procedimentos de pagamento e manter registos precisos.
- **Gestores de Risco:** monitorizar os riscos e coordenar as acções de mitigação.
- **Alta Administração:** aprovar e apoiar a implementação do plano.

Estrutura de Governação e Responsabilidades

Função	Responsável	Atribuições Principais
Coordenação Geral	Secretária da Fazenda	Aprovação e activação do plano. articulação política
Operações de TIC	Director de Tecnologia da Informação	Execução técnica, segurança digital e recuperação
Gestão Financeira	Subsecretária do Tesouro	Continuidade dos pagamentos e controlo orçamental
Comunicação Institucional	Assessoria de Comunicação	Comunicação pública, imprensa e *stakeholders*
Comité de Risco Digital	Gestores Seniores + TIC + Jurídico	Avaliação contínua, revisão do plano e auditoria de simulações

Indicadores de Avaliação

Indicador	Meta	Finalidade
RTO (Recovery Time Objective)	< 12 horas após evento crítico	Tempo máximo aceitável para restabelecer os serviços
Frequência de testes de contingência	Mínimo 2 por ano	Garantir prontidão operacional e validação contínua do plano
Conformidade com plano de backup	≥ 95% dos dias com backups verificados	Assegurar integridade e actualidade dos dados críticos
Taxa de sucesso em simulações	≥ 90% de execução sem falhas críticas	Avaliar eficácia dos procedimentos e da resposta institucional
Índice de formação de trabalhadores	≥ 80% dos envolvidos treinados anualmente	Garantir preparação para actuação em situações de crise

Actualização e Ciclo de Melhoria Contínua

O plano será revisto a cada 12 meses ou após qualquer evento crítico real. Serão recolhidas lições aprendidas, promovidas auditorias e actualizações das responsabilidades, indicadores e tecnologias utilizadas.

Conclusão

A consolidação da resiliência digital no sector financeiro público exige um plano de contingência robusto, colaborativo e adaptável. Este documento constitui uma base concreta para a preparação, resposta e recuperação face a cenários críticos, contribuindo para a estabilidade institucional e para a confiança da população, mesmo nos contextos mais adversos.

Anexo II – Projecto Institucional: Implantação do Plano de Contingência para a Resiliência Digital na Prestação de Serviços Públicos Financeiros

Título do Projecto

Reforço da Resiliência Digital no Sector Financeiro Público: Plano de Contingência para a Continuidade dos Pagamentos e da Execução Orçamental em Situações de Crise

Justificação

As inundações ocorridas em 2024 no estado do Rio Grande do Sul evidenciaram de forma crítica as fragilidades da infraestrutura digital utilizada na gestão das finanças públicas. A paralisação de serviços essenciais, como o processamento salarial, as transferências sociais e a execução orçamental, gerou impactos significativos de natureza social e administrativa. Este projecto tem como finalidade implementar um Plano de Contingência estruturado que assegure a continuidade operacional digital em emergências, em consonância com as diretrizes internacionais de governação resiliente e segurança institucional.

Objectivo Geral

Estabelecer, implementar e operacionalizar um Plano de Contingência Digital que garanta a continuidade dos serviços financeiros essenciais da Secretaria da Fazenda e de entidades correlatas, mesmo em cenários de falhas críticas ou desastres naturais.

Objectivos Específicos

- Diagnosticar vulnerabilidades técnicas e institucionais existentes.
- Implantar uma infraestrutura digital de contingência mínima, baseada em nuvem híbrida.
- Estabelecer rotinas de *backup*, recuperação e operação offline.

- Capacitar os principais colaboradores para assegurar a continuidade dos serviços digitais.
- Desenvolver e testar rotinas de simulação e resposta a emergências.

Público-Alvo

- Colaboradores da Direcção de Finanças do Tesouro do Estado.
- Equipas municipais de finanças e contabilidade pública.
- Fornecedores, instituições bancárias parceiras e beneficiários de programas públicos.
- Cidadãos afectados por atrasos ou falhas nos serviços financeiros.

Resultados Esperados

Resultado Esperado	**Indicador de Sucesso**
Plano de Contingência formalizado e institucionalizado	Documento publicado e homologado
Ambiente digital de backup e failover em funcionamento	Plataforma em nuvem activa com testes realizados
Equipas capacitadas para resposta a incidentes digitais	≥ 80% dos colaboradores treinados
Rotinas de simulação testadas e documentadas	Realização de 2 simulações completas por ano
Redução do tempo médio de recuperação (RTO)	RTO ≤ 12 horas após falha crítica

Principais Actividades

Nº	**Actividade**	**Responsável**	**Prazo**
1	Diagnóstico de infraestrutura e riscos	Coordenação do Projecto	Mês 1–2
2	Desenvolvimento técnico do Plano de Contingência	TIC + Jurídico + Financeiro	Mês 2–3
3	Contratação ou ampliação de soluções em nuvem	Coordenação Técnica de TIC	Mês 3–5

Nº	Actividade	Responsável	Prazo
4	Estabelecimento de rotinas de backup e recuperação	TIC + Gestores Operacionais	Mês 4–6
5	Formação e simulações com trabalhadores públicos	RH + Coordenação de Formação	Mês 6–9
6	Execução de testes de resposta e ajustes no plano	Comité de Risco Digital	Mês 9–10
7	Consolidação, monitorização e avaliação do projecto	Coordenação Geral	Mês 10–12

Orçamento (Estimativa Preliminar)

Os valores serão definidos conforme o escopo técnico final. Os itens a serem orçamentados incluem:

- Aquisição ou expansão de soluções em nuvem segura.
- Formação presencial e continuada.
- Desenvolvimento técnico e simulações operacionais.
- Consultorias especializadas em cibersegurança e *Business Continuity Management* (BCM).
- Comunicação institucional e produção de manuais operacionais.
- Monitorização e auditoria externa.

Matriz Lógica do Projecto

Elemento	Descrição
Objectivo Geral	Garantir a continuidade digital dos serviços financeiros em situações de crise
Resultados	Plano implementado. colaboradores capacitados. infraestrutura operacional pronta
Indicadores	RTO ≤ 12h. ≥ 80% de adesão ao plano. simulações realizadas
Fontes de Verificação	Relatórios técnicos. listas de presença. registos de sistema
Supostos	Comprometimento institucional. disponibilidade de recursos financeiros

Sustentabilidade e Continuidade

- Incorporação do plano ao regimento interno da Secretaria da Fazenda.
- Designação de uma equipa permanente para a gestão da continuidade operacional.
- Actualização periódica do plano com base em novas ameaças e vulnerabilidades.
- Inclusão do tema nas formações de integração e formação continuada.
- Reaplicação do modelo a outros sectores públicos considerados críticos.

Riscos e Estratégias de Mitigação

Risco Potencial	**Estratégia de Mitigação**
Resistência à mudança interna	Envolvimento da alta administração e comunicação institucional clara
Falta de infraestrutura pré-existente	Implementação modular e escalável
Limitações orçamentais	Estabelecimento de parcerias com TCU, BID, BNDES e instituições financeiras