REVISTA TÓPICOS

RECUPERAÇÃO DE DESASTRES DE TECNOLOGIA: COMPARAÇÃO ENTRE OS PRINCIPAIS FRAMEWORKS DE MERCADO DIRECIONADOS PARA RECUPERAÇÃO DE DESASTRES DE TI

DOI: 10.5281/zenodo.15355730

Felisvaldo de Novaes Alcantara[1]

RESUMO

Este artigo examina a crescente importância da gestão de riscos e da recuperação de desastres em tecnologias da informação (TI) no ambiente corporativo atual, caracterizado por um aumento na frequência de falhas técnicas, ataques cibernéticos e desastres naturais. O objetivo principal desta pesquisa é comparar e proporcionando uma compreensão abrangente das melhores práticas e abordagens para a recuperação de desastres, observando os principais frameworks de mercado, incluindo as diretrizes das normas ISO/IEC, os processos e práticas profissionais do DRI (Disaster Recovery Institute) e as diretrizes do National Institute of Standards and Technology (NIST). O artigo define o conceito de desastre em TI, enfatizando a necessidade de um planejamento eficaz para prevenir e responder adequadamente a incidentes. Além disso, discute a aplicação de frameworks propostos na ISO/IEC, DRI e NIST, que oferecem diretrizes estruturadas para a implementação de estratégias robustas de continuidade

de negócios. A comparação entre esses modelos evidencia suas características, vantagens e desvantagens, e destaca a importância da capacitação contínua das equipes. As conclusões sugerem que, embora exista uma diversidade de enfoques, todos os frameworks abordam aspectos cruciais para fortalecer a resiliência organizacional e garantir a continuidade tecnológica e operacional.
Palavras-chave: Recuperação de Desastres. Continuidade de Negócios. Gestão de Crises. Frameworks.

ABSTRACT

This paper examines the growing importance of risk management and disaster recovery in information technology (IT) in today's corporate environment, characterized by an increase in the frequency of technical failures, cyberattacks, and natural disasters. The main objective of this research is to compare and provide a comprehensive understanding of best practices and approaches for disaster recovery, observing the main market frameworks, including the guidelines of ISO/IEC standards, the processes and professional practices of the DRI (Disaster Recovery Institute) and the guidelines of the National Institute of Standards and Technology (NIST). The paper defines the concept of disaster in IT, emphasizing the need for effective planning to prevent and adequately respond to incidents. In addition, it discusses the application of frameworks proposed by ISO/IEC, DRI and NIST, which offer structured guidelines for the implementation of robust business continuity strategies. The comparison between these models highlights their characteristics, advantages, and disadvantages, and highlights the importance of continuous training of teams. The findings

suggest that, although there is a diversity of approaches, all frameworks address crucial aspects to strengthen organizational resilience and ensure technological and operational continuity.
Keywords: Disaster Recovery. Business Continuity. Crisis Management. Frameworks.

1 INTRODUÇÃO

A crescente dependência de tecnologias da informação (TI) no ambiente corporativo torna a gestão de riscos e a recuperação de desastres uma prioridade inadiável para organizações de diversos setores. No cenário atual, onde a incidência de falhas técnicas, ataques cibernéticos e desastres naturais é cada vez mais frequente, torna-se crucial a adoção de frameworks eficazes que garantam a continuidade operacional e a integridade dos dados.

Este artigo apresentará o comparativo entre os principais frameworks de mercado direcionados para a recuperação de desastres de TI, como as normas ISO/IEC 22301 e ISO/IEC 27001, bem como diretrizes do National Institute of Standards and Technology (NIST). Através desta comparação, busca-se delinear as características, vantagens e desvantagens de cada um, permitindo uma análise crítica que possa guiar organizações na escolha do modelo mais adequado às suas necessidades específicas.

Adicionalmente, a pesquisa a seguir analisa as melhores práticas acadêmicas relacionadas à implementação desses frameworks, enfatizando a importância de um planejamento adequado, testes regulares e a

capacitação contínua das equipes. A proposta central é fornecer um arcabouço que permita uma compreensão mais clara das opções disponíveis, facilitando, assim, a adoção de estratégias robustas para a recuperação de desastres em um mundo digital cada vez mais complexo.

2 METODOLOGIA DE PESQUISA

A metodologia adotada para a elaboração deste estudo fundamenta-se na revisão sistemática da literatura, que envolve a leitura e análise crítica de fontes acadêmicas, normativas e artigos relevantes sobre a recuperação de desastres em tecnologias da informação. Este processo visa garantir a contextualização adequada das informações, proporcionando uma base sólida e fundamentada em melhores práticas de mercado. Por meio da coleta e integração de referências confiáveis, busca-se oferecer uma visão abrangente e atualizada das abordagens disponíveis, contribuindo assim para o entendimento aprofundado do tema.

3 DEFINIÇÃO DE DESASTRE EM TI

Um desastre em TI pode ser definido como um evento ou um conjunto de eventos que resulta na interrupção abrupta e severa dos sistemas, aplicações e infraestrutura tecnológica de uma organização. Tais incidentes comprometem não apenas a integridade e a disponibilidade dos dados, mas também podem afetar a continuidade operacional, impactando financeiramente e alterando a reputação institucional.

Além disso, a abrangência do termo “desastre” em TI inclui desde falhas de hardware e problemas de software até ataques cibernéticos e desastres naturais, evidenciando que a vulnerabilidade pode ter origens diversas. Compreender essas nuances é essencial para o desenvolvimento de estratégias eficazes de recuperação e, simultaneamente, para a mitigação dos riscos inerentes a um ambiente digital cada vez mais complexo.

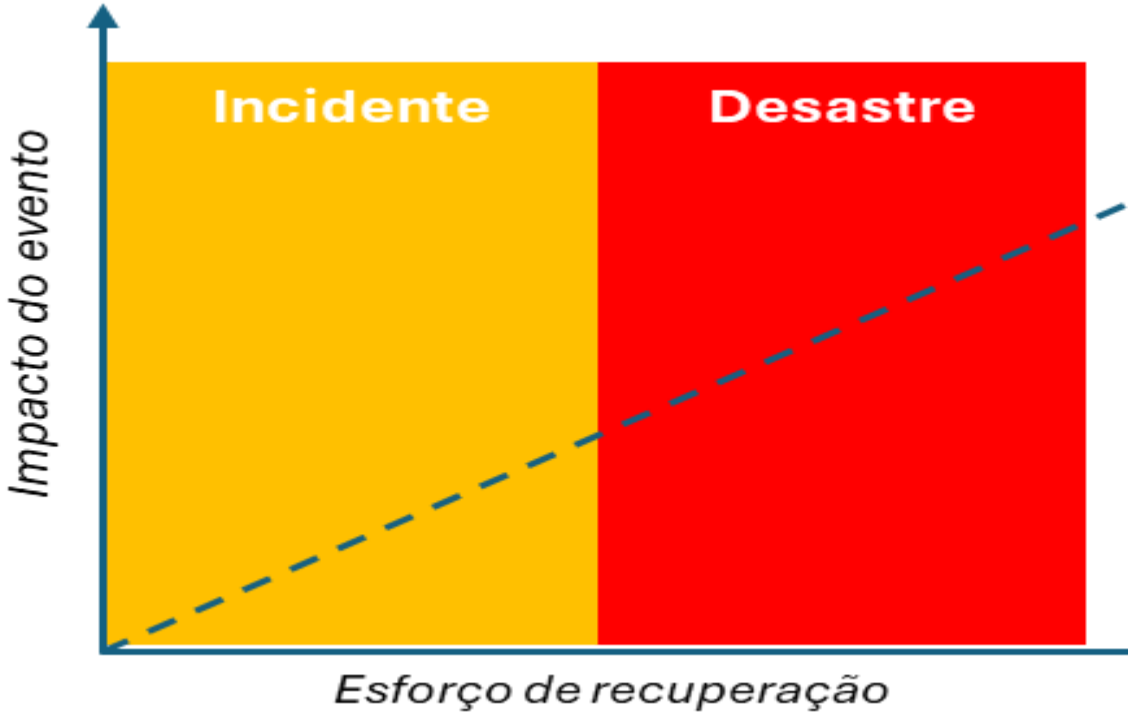
Segundo a ABNT NBR ISO/IEC 22300 (2022), desastre é a situação emergencial, pela qual, ocorrem perdas humanas, materiais econômicas ou ambientais que excedem a capacidade de resposta e recuperação de uma organização, paralelamente, segundo o DRI (2025), a recuperação de desastres é o elemento da continuidade de negócios, da qual, concentra-se os recursos e atividades para se restabelecer serviços de tecnologia da informação, considerando componentes, telecomunicações, sistemas e dados de uma organização, e por fim, segundo Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., & Lynes, D (2010), em publicação do NIST, conceituando-se através dos requisitos de um plano para essa finalidade, a recuperação de desastres é entendida como o conjunto de procedimentos, estratégias e técnicas adotadas para restaurar a funcionalidade dos sistemas de tecnologia da informação (TI) e dados críticos após a ocorrência de um evento disruptivo ou catastrófico.

Desta forma, podemos sintetizar que, qualquer evento crítico no campo tecnológico em uma organização, que através da sua indisponibilidade cause prejuízos a companhia, e que exija esforços significativos para sua

resposta e recuperação, seja causado por problema técnico ou ataque cibernético, podemos considerar como um desastre de tecnologia.

Vale destacar que, quando um problema de tecnologia é de menor gravidade, que não impacte toda a companhia ou exija um esforço controlado para sua resposta e recuperação, podemos considerar esse evento como um incidente, que segundo a ABNT NBR ISO/IEC 27035-1 (2023), é um evento de segurança da informação é uma ocorrência que indica uma possível violação de segurança da informação ou falha de controles que pode impactar as capacidades tecnológicas de uma organização. Um incidente pode se tornar um desastre com seu agravamento, mas em abrangência e impacto, um desastre é muito mais massivo que um evento classificado como incidente.

Imagem 1 – Matriz de definição de incidente ou desastre com base em impacto do evento x esforço de recuperação



Fonte: Autor

Por fim, um desastre em TI representa uma ameaça significativa à integridade, disponibilidade e continuidade operacional de uma organização, podendo surgir de diversas fontes, desde falhas técnicas até ataques cibernéticos. É vital que as organizações compreendam a diferenciação entre incidentes e desastres, pois essa distinção orienta as respostas e as alocações de recursos durante crises. Assim, um planejamento eficaz e a conscientização sobre as potencialidades de um desastre são fundamentais para fortalecer a resiliência organizacional em um ambiente digital complexo e em constante evolução.

4 PRINCIPAIS FRAMEWORKS DE GESTÃO DE DESASTRE

Os frameworks de recuperação de desastres oferecem linhas diretrizes estruturadas que possibilitam às organizações implementar práticas sistemáticas de retomada das operações após desastres tecnológicos. Tomar como base um framework para se planejar e mitigar impactos de um desastre tecnológico é tomar como base práticas amplamente aceitas e testadas pelo mercado.

As Normas técnicas ISO/IEC, como a ISO 22301, voltada para a gestão da continuidade de negócios, e a ISO/IEC 27001, focada na segurança da informação, fornecem uma base robusta para o estabelecimento de processos, auditorias e a melhoria contínua dos planos de recuperação, alinhando as práticas à mitigação de riscos críticos. Adicionalmente, o Disaster Recovery Institute (DRI) disponibiliza um glossário e diretrizes práticas que auxiliam na criação de competências operacionais voltadas à recuperação de desastres, e o National Institute of Standards and Technology (NIST) oferece recomendações fundamentadas em pesquisas e experiências acumuladas em ambientes de alta complexidade, o que tem contribuído para a consolidação de abordagens ágeis e adaptáveis na resposta a incidentes.

4.1 Normas Técnicas ISO/IEC

As normas ISO/IEC, que no Brasil são fornecidas pela Associação Brasileira de Normas Técnicas (ABNT), têm como objetivo estabelecer um sistema abrangente e integrado de gestão para a continuidade dos negócios e recuperação de desastres. A metodologia enfatiza a necessidade de um

conjunto de requisitos formalizados, baseados em processos bem estruturados e na melhoria contínua.

As normas, como a ABNT NBR ISO/IEC 27031 (2023), que dispõe de diretrizes para continuidade da segurança da informação, e a ABNT NBR ISO 22301 (2024), que fornecem diretrizes para continuidade de negócios e resiliência, buscam alinhar a recuperação de desastres aos outros sistemas de gestão, criando um framework integrado e compatível com padrões internacionais, preparando as companhias para abordagens em conformidade com as melhores práticas e integradas entre sistemas de gestão. O estabelecimento de processos análogos as normas técnicas requerem uma documentação extensa e revisões periódicas, garantindo a conformidade normativa e a possibilidade de certificação por organismos independente.

Por fim, destaca-se a aplicação do ciclo PDCA (Plan, Do, Check, Act) como framework de implantação e manutenção de processos oriundos de normas técnicas, o que reforça o caráter dinâmico e proativo na identificação de riscos, mitigação de vulnerabilidades e adaptação às mudanças do ambiente organizacional. Este conjunto de práticas contribui para que empresas de diversos portes e setores construam uma estratégia robusta diante de eventos adversos, com ênfase na consistência e na melhoria contínua dos processos.

Imagem 2 – Ciclo PDCA para implantação de um sistema de continuidade de negócios baseado na ISO/IEC 22301

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

Fonte: ABNT NBR ISO/IEC 22313 (Orientações para o uso da ISO/IEC 22301)

4.2 DRI (Disaster Recovery Institute)

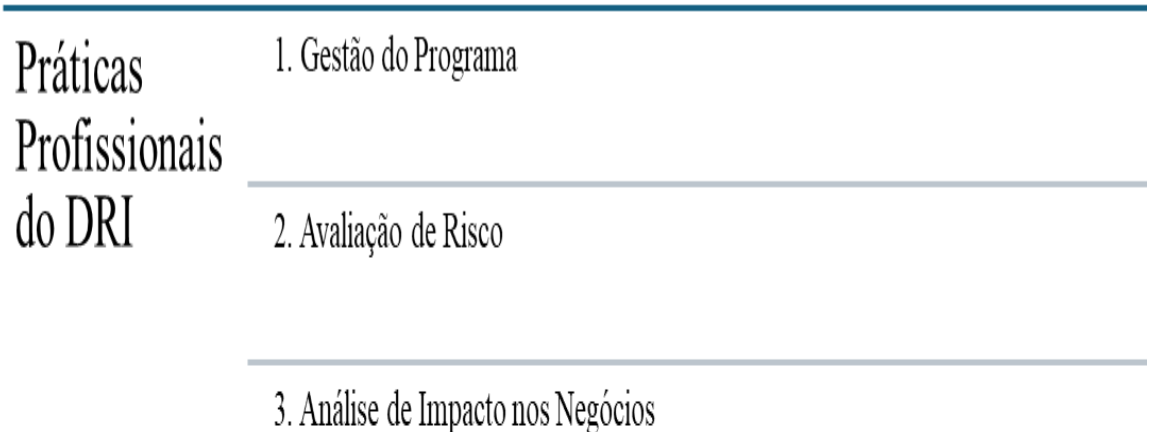
Sob a perspectiva do Disaster Recovery Institute (DRI), que se centra na experiência prática e na capacitação dos profissionais. Essa abordagem prioriza a operação dinâmica dos planos de recuperação por meio de atividades que incentivam a prática e o aprendizado contínuo:

O DRI enfatiza a realização de simulações, testes regulares e exercícios de recuperação para garantir que as equipes estejam preparadas para responder de forma rápida e eficaz a incidentes reais, o que reforça uma abordagem pragmática no desenvolvimento de estratégias de recuperação de desastres.

Ao valorizar os feedbacks obtidos durante os exercícios práticos, a abordagem do DRI permite a rápida adaptação e aprimoramento dos procedimentos, integrando as lições aprendidas de incidentes passados, adicionalmente, possuem forte atuação na formação e certificação de novos profissionais, reforçando a importância da expertise e do conhecimento prático para a execução dos planos de recuperação. Essa visão prática favorece a internalização das melhores práticas e contribui para que a organização se torne mais resiliente frente à imprevisibilidade dos desastres.

O DRI (2023) possui uma abordagem que explora 10 práticas profissionais, da qual, em conjunto, fomentam a criação de culturas organizacionais que priorizam a resiliência. Seu framework abrange não apenas a recuperação técnica, mas também a gestão de crises e a comunicação interna durante situações adversas. O DRI enfatiza a importância do planejamento estratégico e da prática contínua para que as organizações estejam sempre preparadas.

Imagem 3 – As 10 Práticas Profissionais do DRI



4. Estratégias de Continuidade de Negócios
5. Prontidão e Resposta a Incidentes
6. Desenvolvimento e Implantação do Plano
7. Programas de Conscientização e Treinamento
8. Exercício / Teste, Avaliação e Manutenção do Plano de Continuidade de Negóci
9. Comunicação em Crise
10. Coordenação com Agências e Recursos Externos

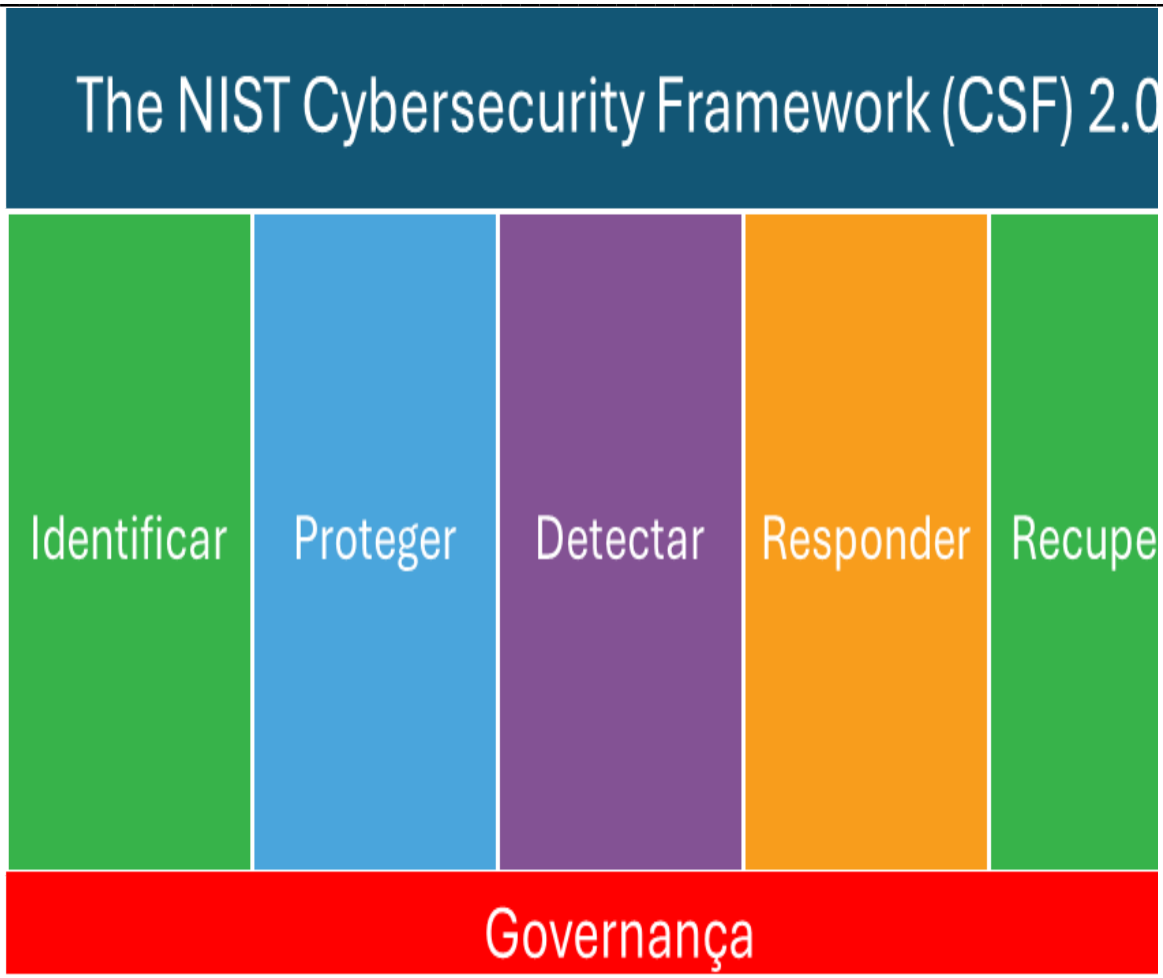
Fonte: Autor (Adaptado DRI – Práticas Profissionais)

4.3 NIST (National Institute of Standards and Technology)

O NIST (National Institute of Standards and Technology) é uma das agências do departamento de comércio dos Estados Unidos, que se dedica desde 1901 na construção de padrões para gestão e estabelecimento das melhores práticas de segurança da informação, sendo referência internacional e amplamente utilizados por diversos segmentos de negócio.

Em sua publicação The NIST Cybersecurity Framework (CSF) 2.0 (2024), o NIST estabelece um framework direcionado principalmente no como se preparar para se proteger contra riscos cibernéticos. Nesta publicação, o NIST determina um modelo de pautado em processos e funções de negócio que contemplam etapas desde a identificação de potenciais incidentes cibernéticos até como recuperar tecnologias afetadas por um ataque cibernético. Este mesmo modelo é fortemente alicerçado por um modelo de governança com o objetivo de garantir a integridade do modelo sugerido.

Imagem 4 – The NIST Cybersecurity Framework (CSF) 2.0

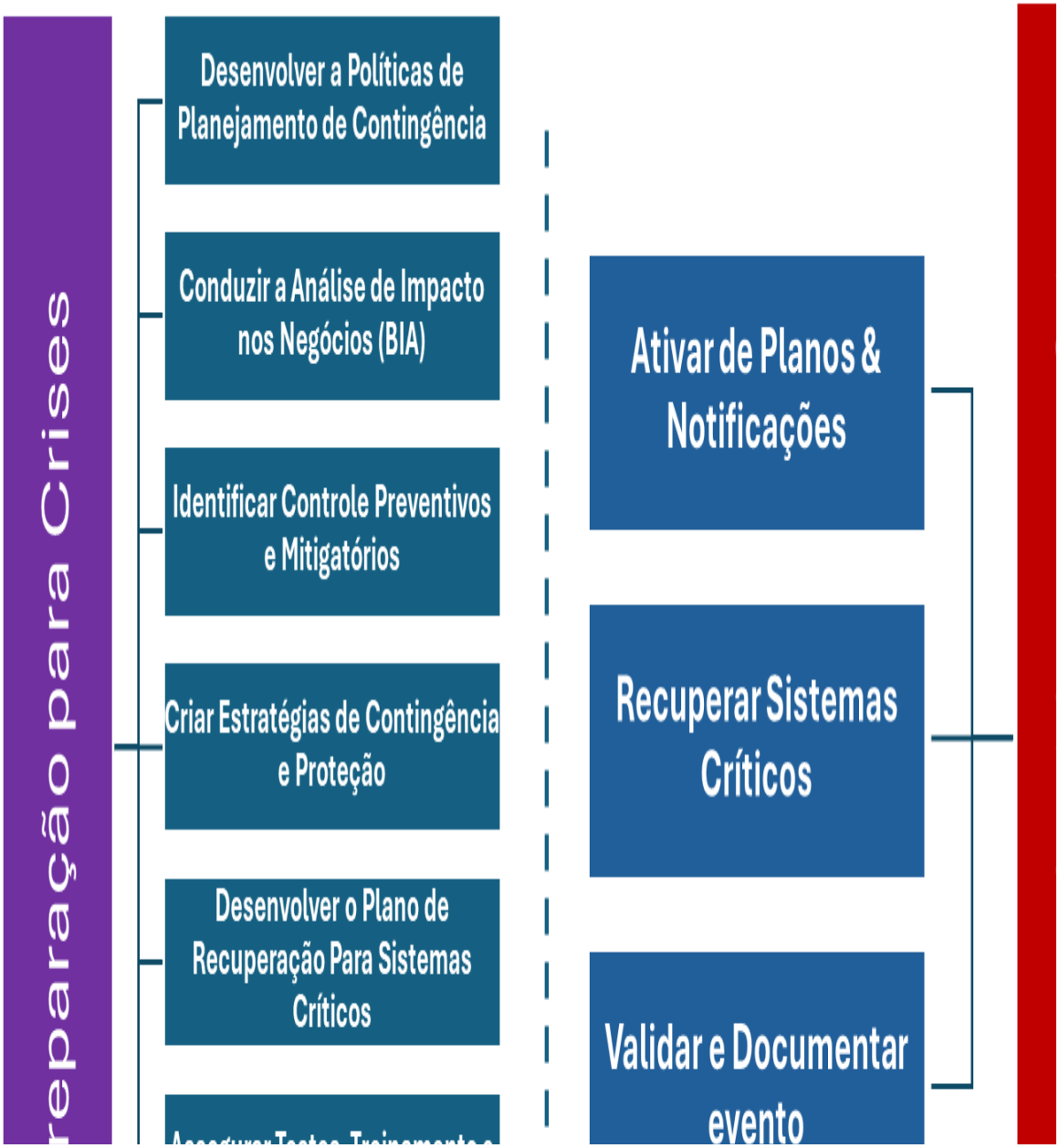


Fonte: Autor (Adaptado NIST)

Complementarmente, segundo Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., & Lynes, D. (2010) na publicação NIST SP 800-34 Rev. 1 - Contingency Planning Guide for Federal Information Systems, se estabelece uma série de processos relacionados aos processos de preparação de políticas e processos para preparação e resposta a crises e incidentes, apresentando um fluxo de atividades estruturadas para

estabelecer processos robustos que asseguram adequada proteção dos sistemas críticos de uma companhia.

Imagem 5 – Processos de preparação e resposta a incidentes e crises conforme o NIST SP 800-34



Fonte: Autor (Adaptado NIST)

4.4 Comparativo entre frameworks ISO/IEC, DRI e NIST

Os frameworks ISO/IEC, DRI e NIST apresentam convergências no fato de todos se concentrarem em melhorar a resiliência organizacional e a recuperação de desastres, mas divergências significativas aparecem em suas abordagens e escopos. A ISO/IEC foca em criar padrões internacionais amplamente reconhecidos com um enfoque estruturado, visando a padronização global. Por outro lado, o DRI se concentra principalmente em fornecer certificações e treinamento para profissionais, destacando-se como uma entidade que promove o reconhecimento profissional na área de continuidade de negócios e recuperação de desastres. O NIST, no entanto, adota uma abordagem mais orientada para o governo dos EUA, estabelecendo diretrizes e padrões principalmente aplicáveis aos sistemas de informação federais.

No aspecto de integração com outros frameworks, a ISO/IEC possui uma grande flexibilidade devido à sua adoção mundial, permitindo que suas normas sejam integradas com diversos outros sistemas de gestão e

segurança. O DRI, estando mais focado em certificações, não possui a mesma amplitude de integração, mas contribui para a capacitação profissional que pode harmonizar diferentes padrões e práticas. O NIST, porém, oferece orientações específicas que podem ser implantadas em conjunto com medidas de segurança cibernética e outros padrões de segurança modernizados dentro dos Estados Unidos.

Em termos de enfoque em segurança cibernética, o NIST se destaca por sua ênfase em controles técnicos e procedimentos relacionados à proteção de dados e infraestrutura crítica. Em contraste, a ISO/IEC oferece uma abordagem mais abrangente que cobre uma ampla gama de riscos operacionais, enquanto o DRI proporciona uma perspectiva prática e de capacitação técnica para indivíduos envolvidos na recuperação de desastres, focando menos em segurança cibernética direta e mais no conjunto de habilidades necessários para gerenciar interrupções.

Imagem 6 – Comparativo entre frameworks propostos pelas ISO/IEC, DRI e NIST

Critério	Normas Técnicas ISO/IEC	DRI (Disaster Recovery Institute)	NIST

/Aspecto			
Objetivo Principal	Estabelece um sistema integrado de gestão da continuidade de negócios e recuperação de desastres (ex.: ISO 22301 e ISO/IEC 27031), com forte ênfase na segurança da informação e na melhoria contínua.	Promove melhores práticas, capacitar profissionais e oferecer metodologias práticas para garantir a rápida retomada das operações e a resiliência organizacional.	Fornece diretrizes técnicas e orientações detalhadas para o planejamento e execução de planos de contingência, com foco especial na segurança cibernética e na proteção dos sistemas de TI (ex.: NIST SP 800-34).
A	Baseada em	Apoiada na	Orientada pelo

bordagem	normas internacionais, com um conjunto de requisitos bem definidos, processos estruturados e integração com outros padrões (como ISO/IEC 27001 e ISO/IEC 22301).	experiência prática e nos aprendizados de incidentes reais, enfatizando a execução de testes, simulações e a adaptabilidade dinâmica do plano de recuperação.	gerenciamento de riscos, dividindo as atividades em fases (preparação, resposta, recuperação) e oferecendo recomendações específicas para ambientes tecnológicos e operacionais.
Certificação e	Possibilita certificação formal por meio de auditorias realizadas por organismos independentes, o que confere reconhecimento internacional.	Oferece certificações profissionais especializadas, valorizando a expertise e o treinamento dos profissionais em recuperação de desastres.	Funciona como um guia de referência adotado pela indústria e órgãos governamentais, sem certificação formal, mas com reconhecimento pela robustez técnica de suas diretrizes.

Reconhecimento			
Escopo de Apli	Amplo e aplicável a organizações de diversos setores e portes, integrando não só a recuperação de desastres, mas também os aspectos de continuidade dos	Voltado para empresas que buscam aprimorar suas práticas operacionais e de recuperação, sendo especialmente útil para aquelas que desejam internalizar as melhores práticas obtidas por meio de	Inicialmente direcionado ao setor público, infraestrutura crítica e organizações com grande foco em TI, mas também adaptável ao ambiente

cação	negócios e segurança da informação.	certificações e treinamentos especializados.	corporativo de forma geral.
Integração com Outros F	Altamente compatível com outros padrões e frameworks internacionais (ex.: COBIT, ITIL, ISO/IEC 27001, ISO 22301), facilitando a implementação de uma estratégia de continuidade holística.	Suas práticas podem complementar outras metodologias e frameworks, enfatizando a execução prática e a integração de lições aprendidas com diferentes abordagens de continuidade.	Permite a integração com normas internacionais e frameworks correlatos, como o NIST Cybersecurity Framework, de forma que as diretrizes técnicas se complementem com controles e melhores práticas globais.

rameworks			
Testes e Exercíci	Incentiva a realização de testes periódicos e simulações para validar a eficácia dos processos e a melhoria contínua dos planos.	Dá grande ênfase a exercícios práticos, simulações e treinamentos regulares, pois a experiência operacional real é fundamental para a eficácia dos planos de recuperação.	Recomenda testes e revisões periódicas dos planos de contingência, com foco na validação técnica e operacional para manter a eficácia frente às novas ameaças.

os			
Documentação e Atualização	Exige documentação extensa e formal, com revisões e auditorias regulares para garantir a conformidade com os requisitos normativos.	Valoriza a documentação detalhada, mas prioriza também a capacidade de resposta ágil e a adaptação prática dos planos com base em feedback dos exercícios realizados.	Enfatiza um alto nível de documentação detalhada, com atualizações regulares baseadas na evolução das ameaças, incidentes reais e avanços tecnológicos.

Enfoque em Segurança Cibernética	Integra aspectos de segurança da informação, considerando os princípios de confidencialidade, integridade e disponibilidade (ex.: ISO/IEC 27031), de forma a alinhar continuidade e segurança.	Embora o foco principal seja a continuidade operacional e a recuperação física/operacional, também abrange medidas de proteção de TI conforme a relevância para a organização.	Possui forte ênfase na segurança cibernética, refletindo a importância dos sistemas de TI no cenário atual, com diretrizes detalhadas para proteger contra ameaças digitais.

ca			
Investimentos e Custos	Pode envolver investimentos significativos na implementação, treinamento e certificação formal, refletindo o rigor dos requisitos internacionais.	Requer investimentos em capacitação e na estrutura interna para a execução dos planos, com um custo-benefício associado à redução dos impactos de desastres.	As diretrizes estão disponíveis gratuitamente, mas a implantação efetiva das recomendações (especialmente aquelas que envolvem tecnologia e infraestrutura) pode demandar investimentos substanciais.

Fonte: Autor (Adaptado DRI – Práticas Profissionais)

Por fim, enquanto ISO/IEC, DRI e NIST compartilham o objetivo comum de fortalecer as capacidades de recuperação e resiliência organizacional, suas abordagens distintas refletem suas origens e finalidades específicas. A ISO/IEC se destaca pela padronização internacional, o DRI pela capacitação e certificação de profissionais, e o NIST pela criação de diretrizes rigorosas voltadas principalmente para a segurança de sistemas governamentais nos Estados Unidos. Essa diversidade de enfoques permite que organizações de diferentes setores e contextos escolham a abordagem que melhor se adapta às suas necessidades, garantindo uma proteção robusta contra interrupções e desastres.

5 CONCLUSÃO/CONSIDERAÇÕES FINAIS

Ao longo deste artigo, foi possível verificar a relevância da recuperação de desastres de tecnologia como um componente essencial para a resiliência organizacional. A comparação entre os principais frameworks de mercado evidencia que não existe uma solução única; cada modelo apresenta características que podem ser mais ou menos adequadas dependendo das particularidades de cada organização.

A análise dos frameworks, como ISO/IEC 22301, ISO/IEC 27001 e diretrizes do NIST, demonstram que a integração entre gestão de riscos e a elaboração de planos de recuperação é fundamental para lidar com as diversas ameaças que as empresas enfrentam. O fortalecimento do planejamento, aliado a simulações e testes regulares, proporciona às instituições a capacidade de responder de forma assertiva a incidentes, minimizando impactos e garantindo a continuidade dos serviços.

Por fim, destaca-se que todos os frameworks apresentados neste estudo apresentam elementos e processos convergentes e complementares, que demonstram sinergia e até mesmo um teor de complementariedade entre eles. Observa-se ainda que os frameworks apresentados podem figurar alguns tópicos com maior ou menor profundidade, mas não deixam de cobrir o critério/aspecto alvo da análise, diferindo apenas na abordagem ou foco dele.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT. NBR ISO 22300 – Vocabulário. 2022. Associação Brasileira de Normas Técnicas.

ABNT. NBR ISO/IEC 27031 – Tecnologia da informação — Técnicas de segurança — Diretrizes para a prontidão para a continuidade de negócios da tecnologia da informação e comunicação. 2023. Associação Brasileira de Normas Técnicas.

ABNT. NBR ISO/IEC 27035-1 – Tecnologia da informação — Gestão de incidentes de segurança da informação - Parte 1: Princípios e processos. 2023. Associação Brasileira de Normas Técnicas.

ABNT. NBR ISO/IEC 22301 – Segurança e resiliência – Sistema de gestão de continuidade de negócios – Diretrizes. 2024. Associação Brasileira de Normas Técnicas.

ABNT. NBR ISO/IEC 27001 – Segurança da informação, segurança cibernética e proteção à privacidade – Sistema de gestão da segurança da

informação – Requisitos. 2024. Associação Brasileira de Normas Técnicas.

DISASTER RECOVERY INSTITUTE (DRI). Glossary. 2023. Disponível em: https://drii.org/resources/viewglossary. Acesso em: 20 abr. 2025.

DISASTER RECOVERY INSTITUTE (DRI). Professional Practices. Disponível em: https://drii.org/resources/professionalpractices/EN. Acesso em: 23 abr. 2025.

NIST. The NIST Cybersecurity Framework (CSF) 2.0. 2024. National Institute of Standards and Technology.

SWANSON, M.; BOWEN, P.; PHILLIPS, A. W.; GALLUP, D.; LYNES, D. Contingency planning guide for federal information systems. 2010. National Institute of Standards and Technology.

[1] Bacharel em Administração pela Universidade Anhembi Morumbi. Especialista em Gestão de Projetos e Portfólios pela Universidade Anhembi Morumbi. Especialista em Recursos Humanos e Liderança pela Business School São Paulo. Especialista em Segurança da Informação e Gestão de TI pela Universidade Anhembi Morumbi. Especialista em Business Intelligence e Analytics pela Universidade Anhembi Morumbi. Mestrando em Administração pela Must University (EUA – Flórida). E-mail: Felixvaldo14@gmail.com .