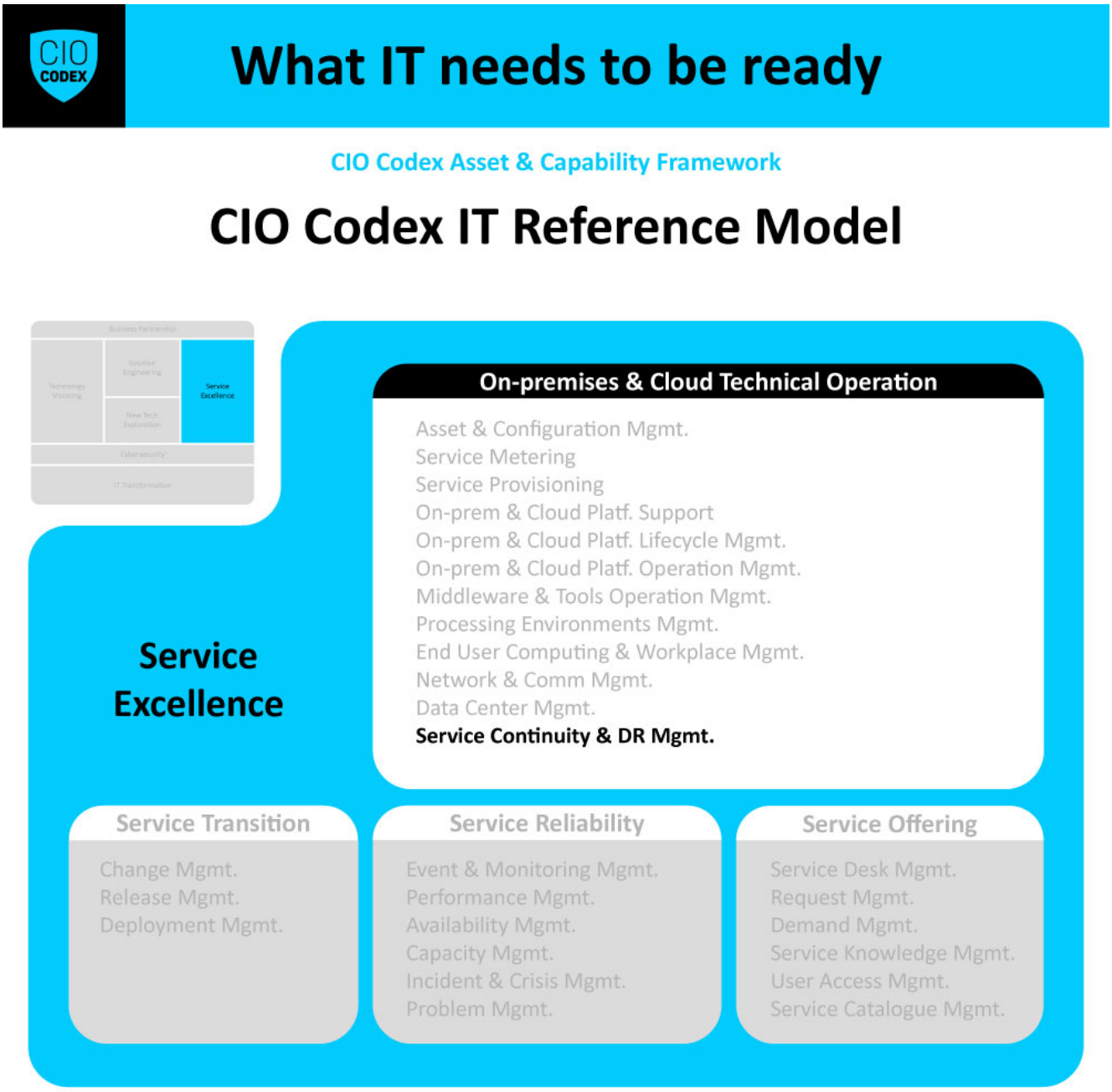

A Service Continuity & Disaster Recovery Management representa uma capability crítica no espectro do CIO Codex Capability Framework, sob a égide da macro capability On premises & Cloud Technical Operation e alinhada à camada de Service Excellence.

Esta capability é vital para assegurar a resiliência organizacional e a disponibilidade contínua dos serviços de TI.

Por meio de estratégias proativas e planos meticulosamente elaborados, esta função minimiza os efeitos negativos de interrupções inesperadas, fortalecendo a confiança e a dependência dos clientes e parceiros de negócios na capacidade da organização de manter operações ininterruptas.

Os conceitos fundamentais que permeiam a Service Continuity & Disaster Recovery Management incluem a continuidade de serviço, que é a habilidade da organização de manter funções essenciais de TI durante e após crises, recuperação de desastres, que engloba a restauração de sistemas e dados após ocorrências disruptivas, e testes de resiliência, que validam a eficácia dos planos de continuidade e recuperação por meio de simulações controladas.

Entre as características distintivas desta capability, salientam-se a análise de riscos, que mapeia potenciais ameaças aos serviços de TI, o desenvolvimento de planos de continuidade robustos, a implementação de sistemas de backup e restauração, o treinamento e a conscientização das equipes, a coordenação eficaz durante crises, e o monitoramento constante da disponibilidade de sistemas, preparando a organização para reagir prontamente a interrupções.

O propósito essencial da Service Continuity & Disaster Recovery Management é estabelecer e manter planos e processos robustos que assegurem a continuidade dos serviços de TI durante eventos disruptivos e permitam uma recuperação efetiva e ordenada após tais eventos.

A natureza essencial desta capability reside na sua capacidade de sustentar a continuidade dos negócios e na sua contribuição para a eficiência operacional da organização.

Dentro do contexto do CIO Codex Capability Framework, os objetivos desta capability são claros: assegurar a eficiência operacional através da implementação de planos de continuidade de serviço e recuperação de desastres eficazes, fomentar a inovação tecnológica para aprimorar esses processos e sustentar a vantagem competitiva da organização, garantindo a confiança dos clientes através da demonstração de uma infraestrutura robusta e resiliente.

O impacto da Service Continuity & Disaster Recovery Management se estende por diversas dimensões tecnológicas, incluindo a infraestrutura de TI, que deve ser projetada com redundâncias, a arquitetura de TI, que deve incorporar considerações de recuperação de desastres em sua concepção, e os sistemas e aplicações críticas, que devem ser capazes de rápida restauração.

Além disso, a cybersecurity é um componente integral, garantindo que os serviços de continuidade incorporem defesas contra ameaças cibernéticas e físicas, e o modelo operacional é reforçado para assegurar que as práticas de gestão de continuidade e recuperação estejam alinhadas com os padrões de segurança e compliance.

Conceitos e Características

A Service Continuity & Disaster Recovery Management é uma capability fundamental para garantir a resiliência e a disponibilidade dos serviços de TI.

Ao adotar abordagens proativas e planos bem elaborados, as organizações podem minimizar os impactos de eventos adversos e manter a continuidade das operações, proporcionando maior confiabilidade aos clientes e parceiros de negócios.

Conceitos

- Continuidade de Serviço: Refere-se à capacidade de manter operações de TI essenciais durante situações de crise, evitando interrupções significativas nos serviços.
- Recuperação de Desastres: Envolve a implementação de planos e procedimentos para restaurar sistemas e dados após eventos catastróficos.
- Testes de Resiliência: A realização regular de testes e simulações para garantir a eficácia dos planos de continuidade e recuperação.

Características

- Análise de Riscos: Identificação e avaliação de ameaças potenciais que podem afetar a continuidade dos serviços.
- Planos de Continuidade: Desenvolvimento e documentação de estratégias detalhadas para manter as operações durante situações adversas.
- Backup e Restauração: Implementação de práticas para realizar cópias de segurança de dados críticos e a capacidade de restaurá-los rapidamente.
- Treinamento e Conscientização: Capacitação de equipes e criação de conscientização sobre os procedimentos de continuidade e recuperação.
- Coordenação de Crises: Estabelecimento de estruturas de gerenciamento de crises para tomar decisões rápidas e coordenadas durante eventos adversos.
- Monitoramento de Disponibilidade: Acompanhamento constante da disponibilidade dos sistemas e serviços para detecção precoce de problemas.

Como é usualmente organizado um Plano de Disaster Recovery

Em um ambiente empresarial cada vez mais dependente de tecnologia, os planos de DR são essenciais para garantir a continuidade das operações em face de interrupções inesperadas.

Estes planos são complexos e multidimensionais, abrangendo desde a recuperação de dados e sistemas críticos até a gestão de comunicações durante crises.

Um plano de recuperação de desastres típico é composto por várias seções que cobrem todos os aspectos necessários para restaurar rapidamente a operacionalidade após um incidente.

A estrutura pode variar dependendo das necessidades específicas da organização, mas geralmente inclui os seguintes elementos:

- Introdução: Define o escopo, os objetivos e os princípios orientadores do plano.
- Governança: Estabelece a estrutura de comando e controle, incluindo os papéis e responsabilidades durante um desastre.
- Análise de Risco e Impacto nos Negócios (BIA): Identifica as funções críticas de negócios e os recursos necessários para manter essas funções operando.
- Estratégias de Recuperação: Descreve as abordagens para a recuperação de sistemas, aplicações e dados.
- Planos de Ação de DR: Fornece procedimentos detalhados para a execução da recuperação em resposta a diferentes tipos de desastres.
- Comunicação de Crise: Detalha os processos de comunicação interna e externa.
- Teste e Manutenção: Descreve a frequência e os métodos para testar e atualizar o plano.

Componentes Chave de um Plano de DR

- Análise de Impacto nos Negócios (BIA): Este componente é vital para entender quais aspectos do negócio são mais críticos. A BIA ajuda a identificar e priorizar os sistemas e processos que necessitam de recuperação rápida para minimizar o impacto financeiro e operacional.

- Identificação de Riscos: Uma análise detalhada dos riscos potenciais que podem causar interrupções. Isso inclui desastres naturais, falhas de hardware, ataques cibernéticos e outros riscos relevantes.
- Estratégias de Recuperação: Definir claramente as estratégias para restaurar as operações de TI e negócios. Isso pode envolver a recuperação de dados, a substituição de equipamentos, o uso de sites alternativos e a contratação de serviços terceirizados.
- Planos de Implementação: Procedimentos passo-a-passo que devem ser seguidos durante um desastre para recuperar operações e serviços. Isso inclui a inicialização de sistemas em um site de recuperação e o restabelecimento de conexões de rede.
- Comunicação: Planos detalhados para informar as partes interessadas internas e externas, incluindo empregados, clientes, fornecedores e a mídia sobre o estado das operações.
- Testes e Exercícios: Um componente crítico que envolve a realização regular de testes para garantir que o plano de DR é eficaz e que a equipe está preparada para agir em caso de desastre.
- Revisão e Manutenção: O plano deve ser revisado e atualizado regularmente para refletir mudanças no ambiente de negócios e tecnológico.

Alcance de um Plano de DR

O alcance de um plano de DR varia amplamente dependendo da natureza e do tamanho da empresa.

Para algumas organizações, pode ser suficiente ter planos que cubram apenas os sistemas de TI críticos.

Para outras, especialmente aquelas em setores altamente regulamentados ou que lidam com grandes volumes de dados sensíveis, o alcance pode ser muito mais abrangente, incluindo:

- Recuperação completa do centro de dados: Capacidade de restaurar todas as operações de TI, incluindo servidores, redes, aplicações e bases de dados.
- Continuidade dos serviços essenciais: Garantir que as funções empresariais vitais possam continuar sem interrupções significativas,

mesmo durante um desastre.
- Gestão da cadeia de suprimentos: Planos para manter ou restaurar rapidamente a logística e os suprimentos essenciais em caso de interrupção nas operações normais.
- Recuperação regulatória e de conformidade: Assegurar que todas as recuperações respeitem as regulamentações legais e normativas aplicáveis, evitando assim penalidades adicionais.

Propósito e Objetivos

A Service Continuity & Disaster Recovery Management desempenha um papel crítico na garantia da continuidade das operações de TI e na mitigação de impactos adversos em caso de desastres ou interrupções.

Seu propósito central é assegurar que a organização tenha planos e processos robustos em vigor para manter a continuidade dos serviços de TI durante eventos adversos e, ao mesmo tempo, permitir uma recuperação eficaz após esses eventos.

Objetivos

Dentro do contexto do CIO Codex Capability Framework, os objetivos dessa capability incluem:

- Eficiência Operacional: Implementar planos de continuidade de serviço e recuperação de desastres eficazes, minimizando o tempo de inatividade e as perdas financeiras.
- Inovação: Adotar tecnologias emergentes para aprimorar os processos de continuidade de serviço e recuperação de desastres, tornando-os mais ágeis e eficientes.
- Vantagem Competitiva: Contribuir para a vantagem competitiva da organização, fornecendo a capacidade de manter a operação ininterrupta e recuperar-se rapidamente de eventos adversos, ganhando assim a confiança dos clientes e parceiros de negócios.

Impacto na Tecnologia

A Service Continuity & Disaster Recovery Management tem um impacto significativo em várias dimensões da tecnologia:

- Infraestrutura: Define políticas para redundância de infraestrutura, garantindo que sistemas críticos tenham backups e recursos alternativos disponíveis em caso de falhas.
- Arquitetura: Influencia a arquitetura de TI, exigindo que os sistemas sejam projetados com considerações de recuperação de desastres desde o início.
- Sistemas: Mantém planos de recuperação para aplicativos e sistemas críticos, garantindo que eles possam ser restaurados rapidamente após uma interrupção.
- Cybersecurity: Garantir a continuidade dos serviços inclui planos de recuperação em caso de incidentes de segurança.
- Modelo Operacional: Estabelece procedimentos de operação durante eventos de interrupção, definindo papéis e responsabilidades para a equipe de TI.

Roadmap de Implementação

A capability de Service Continuity & Disaster Recovery Management é um elemento essencial para a resiliência e a disponibilidade dos serviços de TI.

Ao adotar abordagens proativas e planos bem elaborados, as organizações podem minimizar os impactos de eventos adversos e manter a continuidade das operações.

Dentro do contexto do CIO Codex Capability Framework, as principais etapas para a implementação bem-sucedida dessa capability:

- Definição de Objetivos Estratégicos: O primeiro passo é estabelecer objetivos estratégicos claros para a Service Continuity & Disaster Recovery Management, alinhados com a estratégia global de TI e os objetivos de negócios da organização.
- Avaliação de Riscos: Realize uma análise de riscos abrangente para identificar ameaças potenciais que possam afetar a continuidade dos serviços de TI. Isso inclui ameaças naturais, cibernéticas e outras.

- Desenvolvimento de Planos de Continuidade: Com base na análise de riscos, desenvolva planos detalhados de continuidade de serviço, documentando estratégias para manter as operações durante situações adversas.
- Recuperação de Desastres: Implemente planos e procedimentos de recuperação de desastres que permitam a restauração eficaz de sistemas e dados após eventos catastróficos.
- Testes de Resiliência: Realize testes regulares de resiliência para garantir a eficácia dos planos de continuidade e recuperação. Isso inclui simulações de cenários de desastres.
- Treinamento e Conscientização: Capacite a equipe de TI com treinamento adequado e crie conscientização sobre os procedimentos de continuidade e recuperação. Garanta que todos compreendam seus papéis e responsabilidades.
- Implementação de Backup e Restauração: Estabeleça práticas sólidas de backup de dados críticos e a capacidade de restaurá-los rapidamente em caso de falhas.
- Coordenação de Crises: Defina estruturas de gerenciamento de crises para facilitar tomadas de decisões rápidas e coordenadas durante eventos adversos.
- Monitoramento de Disponibilidade: Mantenha um sistema de monitoramento constante da disponibilidade dos sistemas e serviços de TI para detectar problemas precocemente.
- Auditorias e Conformidade: Realize auditorias regulares dos planos de continuidade e recuperação para garantir a conformidade com padrões e regulamentações relevantes.
- Melhoria Contínua: Estabeleça um processo contínuo de melhoria, onde os planos e procedimentos sejam revisados e atualizados de acordo com as mudanças nas ameaças e nas tecnologias.

A implementação bem-sucedida da Service Continuity & Disaster Recovery Management resultará em uma organização preparada para enfrentar eventos adversos com resiliência e eficácia.

Isso proporcionará maior confiabilidade aos clientes e parceiros de negócios, garantindo a continuidade das operações de TI mesmo diante de desafios imprevistos.

Portanto, seguir esse roadmap estratégico é fundamental para o sucesso na gestão da

continuidade e recuperação de serviços de TI.

Melhores Práticas de Mercado

A Service Continuity & Disaster Recovery Management desempenha um papel fundamental na garantia da resiliência e disponibilidade dos serviços de TI.

As melhores práticas de mercado incluem análise de riscos, planos detalhados, testes regulares, backup eficiente, considerações geográficas, coordenação de crises, monitoramento contínuo, treinamento, automação, simulações de incidentes e avaliação de fornecedores.

Melhores Práticas de Mercado para Service Continuity & Disaster Recovery Management:

- Análise de Riscos e Avaliação de Impacto: Realize análises abrangentes de riscos e avaliações de impacto para identificar ameaças potenciais e priorizar os serviços críticos que requerem recuperação rápida em caso de desastre.
- Planos de Continuidade de Serviço e Recuperação de Desastres: Desenvolva planos detalhados de continuidade de serviço e recuperação de desastres que incluam procedimentos claros, responsabilidades definidas e uma estratégia de comunicação eficaz.
- Testes Regulares: Realize testes regulares de resiliência para validar a eficácia dos planos e identificar áreas de melhoria.
- Backup e Restauração: Implemente políticas de backup adequadas para garantir que dados críticos sejam copiados com segurança e que a restauração seja rápida e confiável.
- Localização Geográfica de Data Centers: Considere a localização geográfica dos data centers para garantir que eles não sejam afetados simultaneamente por desastres naturais ou eventos adversos.
- Coordenação de Crises: Estabeleça uma equipe de gerenciamento de crises bem treinada e definida para tomar decisões rápidas durante situações de interrupção.
- Monitoramento de Disponibilidade: Implemente sistemas de monitoramento contínuo para detectar problemas de disponibilidade e

tomar medidas preventivas.
- Treinamento e Conscientização: Forneça treinamento regular para a equipe de TI e crie conscientização sobre os procedimentos de continuidade e recuperação.
- Automatização de Processos: Utilize automação para acelerar a recuperação de sistemas e reduzir o tempo de inatividade.
- Teste de Incidentes Simulados: Realize exercícios de simulação de incidentes para treinar a equipe e avaliar a capacidade de resposta em situações de crise.
- Avaliação de Terceiros: Avalie regularmente a resiliência de fornecedores e parceiros de negócios que desempenham um papel crítico na cadeia de valor da organização.

Essas práticas visam aumentar a eficiência operacional, promover a inovação, garantir a vantagem competitiva e assegurar a continuidade das operações mesmo diante de eventos adversos.

A Service Continuity & Disaster Recovery Management impacta a infraestrutura, arquitetura, sistemas, cibersegurança e modelo operacional de TI, contribuindo para a confiabilidade dos serviços de TI em um mundo onde a interrupção não é uma opção.

Desafios Atuais

A Service Continuity & Disaster Recovery Management é uma capability crucial no cenário de TI, pois é responsável por garantir a resiliência e a disponibilidade dos serviços em caso de eventos adversos.

No entanto, as organizações enfrentam uma série de desafios atuais ao adotar e integrar essa capability em seus processos de negócios e operações de TI.

Abaixo os principais desafios atuais do mercado, de acordo com o CIO Codex Capability Framework:

- Complexidade das Infraestruturas: Com a crescente complexidade das infraestruturas de TI, que incluem nuvens públicas, privadas e ambientes on-premises, é desafiador manter planos de continuidade abrangentes que abranjam todas essas áreas de forma eficaz.

- Velocidade das Mudanças Tecnológicas: A rápida evolução tecnológica cria desafios na adaptação de planos de continuidade e recuperação para novas tecnologias, como a adoção de contêineres e orquestração de contêineres.
- Recuperação de Dados em Tempo Real: A demanda por recuperação de dados em tempo real tem aumentado, especialmente em setores que não podem tolerar qualquer perda de dados, como instituições financeiras.
- Integração de Nuvens Múltiplas: À medida que as organizações adotam múltiplas nuvens, garantir a continuidade em um ambiente híbrido se torna mais complexo, exigindo uma estratégia de recuperação eficaz.
- Cibersegurança: A crescente ameaça de ataques cibernéticos e ransomware requer planos de recuperação específicos para lidar com incidentes de segurança.
- Testes de Resiliência Efetivos: Realizar testes de resiliência frequentes e eficazes pode ser um desafio logístico, mas é essencial para garantir a eficácia dos planos de continuidade.
- Gestão de Fornecedores de Serviços: Coordenar a continuidade de serviços com provedores de serviços de nuvem e outros fornecedores pode ser complexo, especialmente em ambientes multicloud.
- Orçamento Limitado: Muitas organizações enfrentam restrições orçamentárias, o que pode dificultar a implementação de soluções robustas de continuidade e recuperação.
- Conscientização da Equipe: Garantir que toda a equipe esteja ciente dos planos de continuidade e saiba como agir em situações de crise é essencial, mas pode ser desafiador.
- Avaliação de Riscos Constante: A evolução das ameaças exige uma avaliação contínua de riscos e a adaptação dos planos de continuidade para enfrentar novas ameaças.

Esses desafios refletem a natureza dinâmica do ambiente de TI atual e a importância crítica da Service Continuity & Disaster Recovery Management.

Lidar com a complexidade das infraestruturas, manter-se atualizado com as mudanças tecnológicas, enfrentar ameaças cibernéticas e realizar testes eficazes são apenas alguns dos desafios que as organizações enfrentam ao buscar a resiliência e a continuidade dos serviços de TI.

A superação desses desafios é fundamental para garantir a confiabilidade e a

disponibilidade dos serviços, bem como para atender às expectativas dos clientes e parceiros de negócios.

Investir na capability de gerenciar a continuidade e a recuperação de serviços de forma eficaz é um passo crítico para enfrentar os desafios atuais e preparar as organizações para um futuro cada vez mais dependente da tecnologia.

Tendências para o Futuro

A Service Continuity & Disaster Recovery Management desempenha um papel crítico na garantia da resiliência e disponibilidade dos serviços de TI em organizações.

À medida que o cenário tecnológico e as ameaças evoluem, é fundamental identificar as tendências futuras que moldarão essa capability, considerando as expectativas do mercado.

Abaixo estão as principais tendências para o futuro no contexto do CIO Codex Capability Framework:

- Inteligência Artificial (IA) para Resposta Automatizada: A IA será cada vez mais usada para detecção automática de eventos adversos e para acionar ações de recuperação instantânea, reduzindo o tempo de inatividade.
- Resiliência Distribuída: Organizações adotarão abordagens de resiliência distribuída, com data centers redundantes em várias regiões geográficas para mitigar riscos regionais.
- Recuperação de Dados em Tempo Real: A demanda por recuperação de dados em tempo real crescerá, com organizações exigindo a capacidade de recuperar instantaneamente informações críticas.
- Segurança Integrada na Recuperação de Desastres: A segurança cibernética será integrada aos planos de recuperação de desastres, garantindo que a restauração dos sistemas ocorra de maneira segura.
- Blockchain para Proteção de Dados: A tecnologia blockchain será usada para garantir a integridade e a autenticidade dos dados durante a recuperação de desastres.
- Resposta a Ameaças Cibernéticas em Tempo Real: Soluções de resposta a ameaças cibernéticas em tempo real serão incorporadas aos planos de recuperação para lidar com ataques em andamento.

- Automação de Testes de Recuperação: A automação desempenhará um papel central nos testes de recuperação de desastres, tornando-os mais eficientes e frequentes.
- Edge Computing e Resiliência: A crescente adoção de edge computing exigirá planos de resiliência específicos para esses ambientes distribuídos.
- Treinamento de Conscientização em Segurança: A conscientização em segurança será enfatizada, garantindo que as equipes estejam preparadas para enfrentar ameaças durante eventos de interrupção.
- Monitoramento Avançado de Eventos: A análise de dados em tempo real e a monitorização avançada de eventos permitirão uma resposta mais rápida a ameaças e desastres.

Essas tendências refletem a evolução das necessidades e das tecnologias relacionadas à Service Continuity & Disaster Recovery Management.

A adaptação a essas mudanças será essencial para garantir a continuidade das operações de TI e a resiliência diante de eventos adversos.

É fundamental que as organizações estejam preparadas para enfrentar os desafios futuros, mantendo a disponibilidade e a integridade dos serviços de TI.

KPIs Usuais

A capacidade de Service Continuity & Disaster Recovery Management desempenha um papel crucial na garantia da resiliência e disponibilidade dos serviços de TI, permitindo que as organizações minimizem os impactos de eventos adversos.

A avaliação eficaz dessa capability requer o acompanhamento de KPIs relevantes.

Abaixo estão os principais KPIs usuais no contexto do CIO Codex Capability Framework:

- Tempo de Recuperação de Desastres (Disaster Recovery Time): Mede o tempo necessário para recuperar completamente os sistemas e serviços de TI após um evento de desastre.
- Ponto de Recuperação Objetivo (Recovery Point Objective – RPO): Define o ponto no tempo até o qual os dados podem ser recuperados após um

incidente. Indica a perda máxima de dados tolerável.

- Testes de Continuidade (Continuity Testing): Avalia a frequência e eficácia dos testes regulares de continuidade e recuperação para garantir a preparação adequada para eventos adversos.
- Tempo de Inatividade Não Planejado (Unplanned Downtime): Mede o tempo em que os sistemas de TI estão inoperantes devido a eventos não planejados, como falhas de hardware ou ataques cibernéticos.
- Taxa de Sucesso de Recuperação (Recovery Success Rate): Avalia a capacidade de recuperar com sucesso sistemas e dados após um evento de desastre, indicando a eficácia dos planos de recuperação.
- Custo de Recuperação de Desastres (Disaster Recovery Cost): Calcula os custos associados à implementação de planos de recuperação de desastres, incluindo investimentos em tecnologia e recursos humanos.
- Frequência de Backup (Backup Frequency): Indica com que frequência são realizados backups de dados críticos para garantir a recuperação eficaz.
- Conformidade com Normas de Recuperação (Recovery Standards Compliance): Avalia o grau de conformidade dos planos de recuperação de desastres com as normas e regulamentos aplicáveis.
- Tempo Médio para Ativação de Planos (Mean Time to Plan Activation): Calcula o tempo médio necessário para ativar planos de continuidade de serviço e recuperação após a detecção de um evento adverso.
- Avaliação de Riscos (Risk Assessment): Mede a eficácia na identificação e avaliação de riscos que podem afetar a continuidade dos serviços de TI.
- Taxa de Adoção de Tecnologias Emergentes (Adoption of Emerging Technologies): Avalia a incorporação de tecnologias emergentes para melhorar os processos de continuidade de serviço e recuperação de desastres.
- Tempo Médio de Detecção de Incidentes (Mean Time to Detect Incidents): Calcula o tempo médio necessário para detectar incidentes que podem levar à ativação de planos de continuidade.
- Taxa de Retorno ao Estado Normal (Return to Normal State Rate): Mede a eficiência na restauração dos sistemas e serviços de TI ao estado normal após um evento adverso.
- Avaliação da Conscientização da Equipe (Team Awareness Assessment): Avalia o nível de conscientização e preparação da equipe em relação aos procedimentos de continuidade e recuperação.

- Monitoramento de Disponibilidade Contínua (Continuous Availability Monitoring): Acompanha a disponibilidade contínua dos sistemas e serviços de TI para detecção precoce de problemas.

Esses KPIs são essenciais para garantir a eficácia da Service Continuity & Disaster Recovery Management, permitindo que as organizações continuem operando de forma resiliente, minimizando riscos e impactos adversos, e mantendo a confiabilidade dos serviços de TI para clientes e parceiros de negócios.

Exemplos de OKRs

A capability de Service Continuity & Disaster Recovery Management na macro capability On premises & Cloud Technical Operation da camada Service Excellence é de extrema importância, pois se dedica à gestão da continuidade dos serviços e recuperação de desastres.

Esta capability assegura que existam planos e processos robustos para manter as operações de TI durante e após eventos adversos, minimizando interrupções e perdas.

A seguir, são apresentados exemplos de Objetivos e Resultados-Chave (OKRs) relacionados a esta capability:

Desenvolvimento de Planos de Continuidade e Recuperação

Objetivo: Desenvolver planos de continuidade e recuperação sólidos para todos os serviços críticos de TI.

- KR1: Identificar e documentar todos os serviços críticos e suas dependências.
- KR2: Criar planos detalhados de continuidade e recuperação para cada serviço.
- KR3: Realizar simulações de recuperação de desastres para avaliar a eficácia dos planos.

Minimização do Tempo de Recuperação

Objetivo: Minimizar o tempo necessário para recuperar os serviços após um

incidente ou desastre.

- KR1: Estabelecer metas de tempo de recuperação (RTO) para cada serviço.
- KR2: Implementar soluções de recuperação rápida, como replicação de dados em tempo real.
- KR3: Realizar testes regulares de recuperação para garantir a conformidade com os RTOs.

Testes e Treinamento

Objetivo: Garantir que a equipe esteja preparada para lidar com incidentes e desastres.

- KR1: Realizar treinamento regular em procedimentos de recuperação de desastres.
- KR2: Conduzir testes de recuperação simulados em intervalos programados.
- KR3: Avaliar o desempenho da equipe durante os testes e identificar áreas de melhoria.

Avaliação de Riscos e Vulnerabilidades

Objetivo: Identificar e mitigar riscos que possam afetar a continuidade dos serviços.

- KR1: Realizar avaliações de risco regulares em todas as operações de TI.
- KR2: Implementar medidas de segurança adicionais com base nas avaliações de risco.
- KR3: Manter uma lista atualizada de ameaças e vulnerabilidades conhecidas.

Recuperação de Dados e Infraestrutura

Objetivo: Garantir a recuperação eficaz de dados e infraestrutura após um desastre.

- KR1: Implementar estratégias de backup e recuperação de dados abrangentes.
- KR2: Estabelecer locais de recuperação alternativos para infraestrutura crítica.
- KR3: Testar regularmente a recuperação de dados e infraestrutura em um ambiente de recuperação.

Esses OKRs destacam a importância crítica da capability de Service Continuity & Disaster Recovery Management.

Ao desenvolver planos sólidos, minimizar o tempo de recuperação, treinar a equipe, avaliar riscos e garantir a recuperação eficaz de dados e infraestrutura, esta capability desempenha um papel vital na proteção das operações de TI durante eventos adversos.

Ela contribui para a resiliência e a continuidade dos serviços de uma organização em face de desafios imprevistos.

Critérios para Avaliação de Maturidade

A capability Service Continuity & Disaster Recovery Management, inserida na macro capability On-premises & Cloud Technical Operation e na camada Service Excellence, desempenha um papel fundamental na gestão da continuidade dos serviços e na recuperação de desastres.

A avaliação da maturidade dessa capability é baseada em um modelo inspirado no CMMI, que compreende cinco níveis: Inexistente, Inicial, Definido, Gerenciado e Otimizado.

Nível de Maturidade Inexistente

- Não há planos ou procedimentos formais para a gestão da continuidade dos serviços ou recuperação de desastres.
- A organização não identificou ou avaliou riscos potenciais para a continuidade dos serviços.
- Não existem práticas para a criação e manutenção de backups de dados ou sistemas críticos.

- Não foram realizados testes de recuperação de desastres ou simulações de incidentes.
- A comunicação interna e externa em caso de desastre não está definida.

Nível de Maturidade Inicial

- Planos e procedimentos iniciais para a gestão da continuidade dos serviços e recuperação de desastres estão sendo desenvolvidos.
- Riscos foram identificados, mas a avaliação ainda é superficial.
- Iniciativas para criação de backups e armazenamento seguro de dados estão em andamento.
- Testes de recuperação de desastres são realizados ocasionalmente.
- Um plano básico de comunicação em caso de desastre foi estabelecido.

Nível de Maturidade Definido

- Planos e procedimentos formais para a gestão da continuidade dos serviços e recuperação de desastres estão documentados.
- Riscos foram identificados e avaliados com base em critérios específicos.
- Práticas para criação e manutenção de backups estão bem definidas e seguidas.
- Testes de recuperação de desastres são realizados regularmente e as lições aprendidas são incorporadas.
- Um plano de comunicação detalhado em caso de desastre foi desenvolvido e é revisado periodicamente.

Nível de Maturidade Gerenciado

- Os planos de continuidade dos serviços e recuperação de desastres são eficazes e alinhados com os objetivos de negócios.
- A gestão de riscos é proativa, com análises contínuas e atualizações dos planos.
- A organização mantém backups de dados e sistemas críticos de forma segura e eficaz.

- Testes de recuperação de desastres são frequentes e abrangentes, abordando diferentes cenários.
- A comunicação em caso de desastre é eficiente, envolvendo todas as partes interessadas internas e externas.

Nível de Maturidade Otimizado

- A gestão da continuidade dos serviços e recuperação de desastres é altamente automatizada e baseada em análises avançadas.
- A organização é proativa na identificação e mitigação de riscos emergentes.
- Os backups são realizados de forma contínua e os dados são replicados em tempo real.
- A recuperação de desastres é rápida e eficaz, minimizando a interrupção dos serviços.
- A comunicação durante e após desastres é otimizada para garantir a coordenação eficiente de todas as partes envolvidas.

Esses critérios de maturidade são essenciais para avaliar a eficácia da capability Service Continuity & Disaster Recovery Management.

À medida que a organização progride nos níveis de maturidade, sua capacidade de manter a continuidade dos serviços e recuperar-se de desastres de forma eficaz é aprimorada, garantindo a resiliência das operações de TI.

Convergência com Frameworks de Mercado

A capability Service Continuity & Disaster Recovery Management, pertencente à macro capability On premises & Cloud Technical Operation e situada na camada Service Excellence, desempenha um papel essencial na garantia da continuidade dos serviços de TI e na gestão da recuperação de desastres.

Esta capability enfoca o estabelecimento de planos e processos robustos para manter as operações de TI durante e após eventos adversos, visando minimizar interrupções e

perdas.

A seguir, é analisada a convergência desta capability em relação a um conjunto dez frameworks de mercado reconhecidos e bem estabelecidos em suas respectivas áreas de expertise:

COBIT

- Nível de Convergência: Alto
- Racional: O COBIT, com seu enfoque na governança de TI, exige uma gestão rigorosa da continuidade dos serviços e recuperação de desastres. Esta capability está alinhada com os princípios do COBIT, pois garante que os riscos sejam minimizados e a governança de TI seja efetiva em situações de crise.

ITIL

- Nível de Convergência: Alto
- Racional: O ITIL valoriza a gestão eficaz de serviços, incluindo a capacidade de responder e se recuperar de desastres. Esta capability complementa o ITIL ao garantir a continuidade dos serviços e a gestão efetiva de incidentes.

SAFe

- Nível de Convergência: Médio
- Racional: Enquanto o SAFe se concentra na entrega ágil de software, a capacidade de manter a continuidade dos serviços durante interrupções é benéfica para manter a agilidade e resiliência do negócio.

PMI

- Nível de Convergência: Médio
- Racional: O PMI foca na gestão de projetos, e uma gestão eficaz da continuidade do serviço e recuperação de desastres garante que os

projetos de TI possam continuar ou ser rapidamente retomados após interrupções.

CMMI

- Nível de Convergência: Médio
- Racional: O CMMI promove a melhoria de processos, e esta capability contribui para a resiliência e confiabilidade dos processos de TI, elementos fundamentais para a melhoria contínua.

TOGAF

- Nível de Convergência: Médio
- Racional: No contexto de arquitetura empresarial do TOGAF, a gestão da continuidade dos serviços e recuperação de desastres ajuda a garantir que a infraestrutura de TI esteja alinhada com as necessidades e objetivos estratégicos da organização.

DevOps SRE

- Nível de Convergência: Alto
- Racional: Em DevOps e SRE, a estabilidade e recuperação rápida são críticas. Esta capability alinha-se diretamente com esses objetivos ao assegurar a continuidade dos serviços e uma rápida recuperação após desastres.

NIST

- Nível de Convergência: Alto
- Racional: O NIST enfatiza a segurança e resiliência cibernéticas. A capacidade de continuar operações de TI e se recuperar de desastres é fundamental para cumprir as diretrizes de segurança do NIST.

Six Sigma

- Nível de Convergência: Médio
- Racional: Six Sigma visa a redução de variação e melhoria da qualidade. A gestão eficaz da continuidade dos serviços ajuda a manter a qualidade e consistência das operações de TI, mesmo em face de desastres.

Lean IT

- Nível de Convergência: Médio
- Racional: Lean IT foca na eficiência e eliminação de desperdícios. A gestão da continuidade dos serviços e recuperação de desastres contribui para a eficiência ao reduzir o tempo de inatividade e garantir operações enxutas, mesmo sob condições adversas.

A gestão eficiente da continuidade dos serviços e recuperação de desastres é fundamental para assegurar que a infraestrutura e os serviços de TI permaneçam resilientes e disponíveis, apoiando os objetivos estratégicos da organização e minimizando o impacto dos desastres.

KPIs relevantes para esta capability incluem o tempo de recuperação após desastres (RTO), o ponto de recuperação objetiva (RPO), e o tempo médio para reparo (MTTR).

Estes indicadores ajudam a avaliar a eficácia da gestão da continuidade dos serviços e recuperação de desastres, garantindo que a organização esteja preparada e capacitada para lidar com interrupções e retomar rapidamente as operações normais.

Processos e Atividades

Develop Continuity Plans

O desenvolvimento de planos de continuidade de serviços e recuperação de desastres é fundamental para garantir que uma organização esteja preparada para enfrentar e superar eventos adversos que possam interromper suas operações.

Este processo envolve a criação de estratégias detalhadas que abrangem desde a

análise de riscos e identificação de recursos críticos até a definição de procedimentos específicos para resposta a incidentes.

Os planos de continuidade devem contemplar todas as possíveis ameaças, incluindo desastres naturais, falhas de sistemas, ataques cibernéticos e outras emergências.

É essencial que esses planos sejam abrangentes, alinhados com os objetivos estratégicos da organização e que incluam mecanismos de comunicação claros para garantir a coordenação eficaz durante crises.

A documentação completa dos planos deve estar acessível a todos os envolvidos e ser revisada regularmente para garantir sua relevância e eficácia.

- PDCA focus: Plan
- Periodicidade: Anual

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Risk Assessment	Realizar avaliação de riscos para identificar ameaças potenciais aos serviços de TI.	Dados de riscos, histórico de incidentes	Relatório de avaliação de riscos	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: All areas; Informed: All areas	Decider: IT Infrastructure & Operation; Advisor: Cybersecurity; Recommender: IT Governance & Transformation; Executer: IT Infrastructure & Operation
2	Identify Critical Resources	Identificar recursos e sistemas críticos necessários para a continuidade dos serviços.	Relatório de avaliação de riscos	Lista de recursos críticos	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: All areas; Informed: All areas	Decider: IT Infrastructure & Operation; Advisor: Solution Engineering & Development; Recommender: Data, AI & New Technology; Executer: IT Infrastructure & Operation

3	Develop Response Procedures	Desenvolver procedimentos detalhados de resposta a incidentes e recuperação de desastres.	Lista de recursos críticos	Procedimentos de resposta	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Cybersecurity; Informed: All areas	Decider: IT Infrastructure & Operation; Advisor: Cybersecurity; Recommender: Solution Engineering & Development; Executer: IT Infrastructure & Operation
4	Establish Communication Plan	Estabelecer um plano de comunicação para coordenar ações durante crises.	Procedimentos de resposta	Plano de comunicação	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: All areas; Informed: All areas	Decider: IT Infrastructure & Operation; Advisor: IT Governance & Transformation; Recommender: Cybersecurity; Executer: IT Infrastructure & Operation
5	Document Continuity Plans	Documentar todos os planos de continuidade de serviços e recuperação de desastres.	Plano de comunicação	Planos documentados	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: All areas; Informed: All areas	Decider: IT Infrastructure & Operation; Advisor: IT Governance & Transformation; Recommender: All areas; Executer: IT Infrastructure & Operation

Identify Continuity Requirements

A identificação dos requisitos para continuidade de serviços e recuperação de desastres é um processo crítico que assegura que todas as necessidades de infraestrutura, capacidade, segurança e eficiência sejam compreendidas e atendidas.

Este processo envolve a coleta e análise de dados sobre a utilização atual dos recursos, bem como a realização de entrevistas e consultas com stakeholders para compreender

suas expectativas e desafios.

A análise detalhada dessas informações permite definir os requisitos técnicos e funcionais que orientarão o desenvolvimento e a implementação de soluções de TI.

A identificação precisa dos requisitos é crucial para evitar lacunas e garantir que as soluções implantadas sejam alinhadas com os objetivos de negócio e as necessidades dos usuários finais, assegurando que os serviços possam suportar a carga de trabalho de maneira eficaz e segura, promovendo a eficiência operacional e a inovação contínua.

- PDCA focus: Plan
- Periodicidade: Anual

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Conduct Stakeholder Interviews	Realizar entrevistas com stakeholders para identificar suas necessidades e expectativas.	Questionários e entrevistas	Dados coletados	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: All areas; Informed: All areas	Decider: IT Infrastructure & Operation; Advisor: Solution Engineering & Development; Recommender: Data, AI & New Technology; Executer: IT Infrastructure & Operation

2	Analyze Usage Data	Analisar dados de uso e desempenho dos serviços para identificar padrões e demandas.	Dados de uso e desempenho	Relatório de análise	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Data, AI & New Technology; Informed: All areas	Decider: IT Infrastructure & Operation; Advisor: Data, AI & New Technology; Recommender: Solution Engineering & Development; Executer: IT Infrastructure & Operation
3	Define Technical Requirements	Estabelecer os requisitos técnicos com base nos dados coletados e analisados.	Relatório de análise, dados coletados	Requisitos técnicos	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: All areas; Informed: All areas	Decider: IT Infrastructure & Operation; Advisor: Architecture & Technology Visioning; Recommender: Data, AI & New Technology; Executer: IT Infrastructure & Operation
4	Define Functional Requirements	Definir os requisitos funcionais que os serviços devem atender.	Requisitos técnicos	Requisitos funcionais	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: All areas; Informed: All areas	Decider: IT Infrastructure & Operation; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: IT Infrastructure & Operation

5	Validate Requirements	Validar os requisitos definidos com as partes interessadas e usuários finais.	Requisitos técnicos e funcionais	Requisitos validados	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: All areas; Informed: All areas	Decider: IT Infrastructure & Operation; Advisor: All areas; Recommender: All areas; Executer: IT Infrastructure & Operation

Implement Continuity Solutions

A implementação das soluções de continuidade de serviços e recuperação de desastres conforme planejado é um processo que assegura a execução das estratégias definidas para garantir que a infraestrutura e os serviços estejam configurados e operando de acordo com os requisitos estabelecidos.

Este processo inclui a instalação e configuração de hardware e software, a aplicação de políticas de segurança, a realização de testes e a implementação de práticas de backup e recuperação de desastres.

A implementação deve ser realizada de maneira organizada e eficiente para minimizar interrupções no trabalho dos usuários e garantir que todas as soluções sejam entregues com a qualidade e segurança necessárias.

A correta execução deste processo é vital para assegurar que os serviços possam suportar as operações de TI de forma eficaz, segura e contínua, promovendo a eficiência operacional e a inovação.

- PDCA focus: Do
- Periodicidade: Ad-hoc

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE

1	Prepare Implementation Plan	Preparar o plano detalhado de implementação das soluções de continuidade e recuperação.	Plano de gestão aprovado	Plano de implementação detalhado	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: All areas; Informed: All areas	Decider: IT Infrastructure & Operation; Advisor: Solution Engineering & Development; Recommender: Data, AI & New Technology; Executer: IT Infrastructure & Operation
2	Install and Configure Hardware	Instalar e configurar o hardware necessário para os serviços de continuidade.	Plano de implementação detalhado	Hardware instalado e configurado	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: All areas; Informed: All areas	Decider: IT Infrastructure & Operation; Advisor: Architecture & Technology Visioning; Recommender: Solution Engineering & Development; Executer: IT Infrastructure & Operation
3	Deploy Continuity Software	Distribuir e configurar software nos dispositivos necessários.	Hardware configurado	Software de continuidade implantado	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: All areas; Informed: All areas	Decider: IT Infrastructure & Operation; Advisor: Cybersecurity; Recommender: Data, AI & New Technology; Executer: IT Infrastructure & Operation

4	Apply Security Policies	Implementar políticas de segurança nos dispositivos e sistemas.	Software de continuidade implantado	Políticas de segurança aplicadas	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Cybersecurity; Informed: All areas	Decider: IT Infrastructure & Operation; Advisor: Cybersecurity; Recommender: Architecture & Technology Visioning; Executer: IT Infrastructure & Operation
5	Perform System Testing	Realizar testes nos sistemas para garantir que todas as soluções estão funcionando conforme esperado.	Políticas de segurança aplicadas	Relatório de testes	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: All areas; Informed: All areas	Decider: IT Infrastructure & Operation; Advisor: Solution Engineering & Development; Recommender: Data, AI & New Technology; Executer: IT Infrastructure & Operation

Monitor Continuity Performance

O monitoramento contínuo do desempenho da gestão de continuidade de serviços e recuperação de desastres é essencial para garantir que os planos e soluções implementados estejam funcionando conforme esperado.

Este processo envolve a utilização de ferramentas de monitoramento para acompanhar o desempenho dos sistemas, identificar e solucionar problemas proativamente e garantir a conformidade com as políticas de segurança e regulatórias.

Através do monitoramento contínuo, é possível detectar falhas ou anomalias antes que se transformem em problemas maiores, permitindo ações corretivas imediatas.

Além disso, este processo fornece dados valiosos para análises de tendências e melhorias contínuas, garantindo que os serviços de continuidade estejam sempre operando no mais alto nível de eficiência e disponibilidade.

- PDCA focus: Check

- Periodicidade: Contínua

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Set Up Monitoring Tools	Configurar e calibrar ferramentas de monitoramento para acompanhar os sistemas de continuidade.	Ferramentas de monitoramento	Ferramentas configuradas	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: All areas; Informed: All areas	Decider: IT Infrastructure & Operation; Advisor: Solution Engineering & Development; Recommender: Data, AI & New Technology; Executer: IT Infrastructure & Operation
2	Monitor System Performance	Monitorar o desempenho dos sistemas e a utilização dos recursos dos serviços de continuidade.	Ferramentas configuradas	Relatórios de desempenho	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Data, AI & New Technology; Informed: All areas	Decider: IT Infrastructure & Operation; Advisor: Data, AI & New Technology; Recommender: Solution Engineering & Development; Executer: IT Infrastructure & Operation
3	Identify and Resolve Issues	Identificar e resolver proativamente problemas detectados nos serviços de continuidade.	Relatórios de desempenho	Problemas resolvidos	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Cybersecurity; Informed: All areas	Decider: IT Infrastructure & Operation; Advisor: Cybersecurity; Recommender: Solution Engineering & Development; Executer: IT Infrastructure & Operation

4	Ensure Compliance	Garantir que todas as operações dos serviços de continuidade estejam em conformidade com políticas e regulamentos.	Relatórios de desempenho	Conformidade assegurada	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: All areas; Informed: All areas	Decider: IT Infrastructure & Operation; Advisor: IT Governance & Transformation; Recommender: Cybersecurity; Executer: IT Infrastructure & Operation
5	Report Performance Metrics	Relatar métricas de desempenho e insights para a alta gestão e stakeholders.	Conformidade assegurada	Relatórios de métricas	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: All areas; Informed: All areas	Decider: IT Infrastructure & Operation; Advisor: Data, AI & New Technology; Recommender: Solution Engineering & Development; Executer: IT Infrastructure & Operation

Review and Optimize Continuity Processes

A revisão e otimização dos processos de gestão de continuidade de serviços e recuperação de desastres é essencial para garantir a eficácia contínua dos planos implementados.

Este processo envolve a análise detalhada dos resultados de monitoramento, a realização de auditorias e testes regulares, e a identificação de áreas de melhoria.

Através da revisão periódica, é possível ajustar estratégias e procedimentos, incorporando novas tecnologias e melhores práticas para melhorar a resiliência e a eficiência dos serviços de continuidade.

Além disso, este processo promove uma cultura de melhoria contínua, assegurando que a organização esteja sempre preparada para responder a novos desafios e ameaças.

A otimização constante dos processos de continuidade é fundamental para minimizar os riscos e garantir a disponibilidade ininterrupta dos serviços de TI, proporcionando

maior confiança aos stakeholders.

- PDCA focus: Act
- Periodicidade: Anual

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Conduct Performance Review	Realizar uma revisão detalhada do desempenho dos processos de continuidade.	Relatórios de desempenho, métricas	Relatório de revisão	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: All areas; Informed: All areas	Decider: IT Infrastructure & Operation; Advisor: IT Governance & Transformation; Recommender: Data, AI & New Technology; Executer: IT Infrastructure & Operation
2	Identify Improvement Areas	Identificar áreas de melhoria com base nos resultados da revisão de desempenho.	Relatório de revisão	Lista de áreas de melhoria	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: All areas; Informed: All areas	Decider: IT Infrastructure & Operation; Advisor: Solution Engineering & Development; Recommender: Data, AI & New Technology; Executer: IT Infrastructure & Operation

3	Develop Optimization Plan	Desenvolver um plano detalhado para otimizar os processos de continuidade.	Lista de áreas de melhoria	Plano de otimização	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: All areas; Informed: All areas	Decider: IT Infrastructure & Operation; Advisor: IT Governance & Transformation; Recommender: Architecture & Technology Visioning; Executer: IT Infrastructure & Operation
4	Implement Improvements	Implementar as melhorias identificadas e planejadas.	Plano de otimização	Processos otimizados	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: All areas; Informed: All areas	Decider: IT Infrastructure & Operation; Advisor: Solution Engineering & Development; Recommender: Cybersecurity; Executer: IT Infrastructure & Operation
5	Validate Effectiveness	Validar a eficácia das melhorias implementadas através de testes e auditorias.	Processos otimizados	Relatório de validação	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: All areas; Informed: All areas	Decider: IT Infrastructure & Operation; Advisor: Cybersecurity; Recommender: Data, AI & New Technology; Executer: IT Infrastructure & Operation