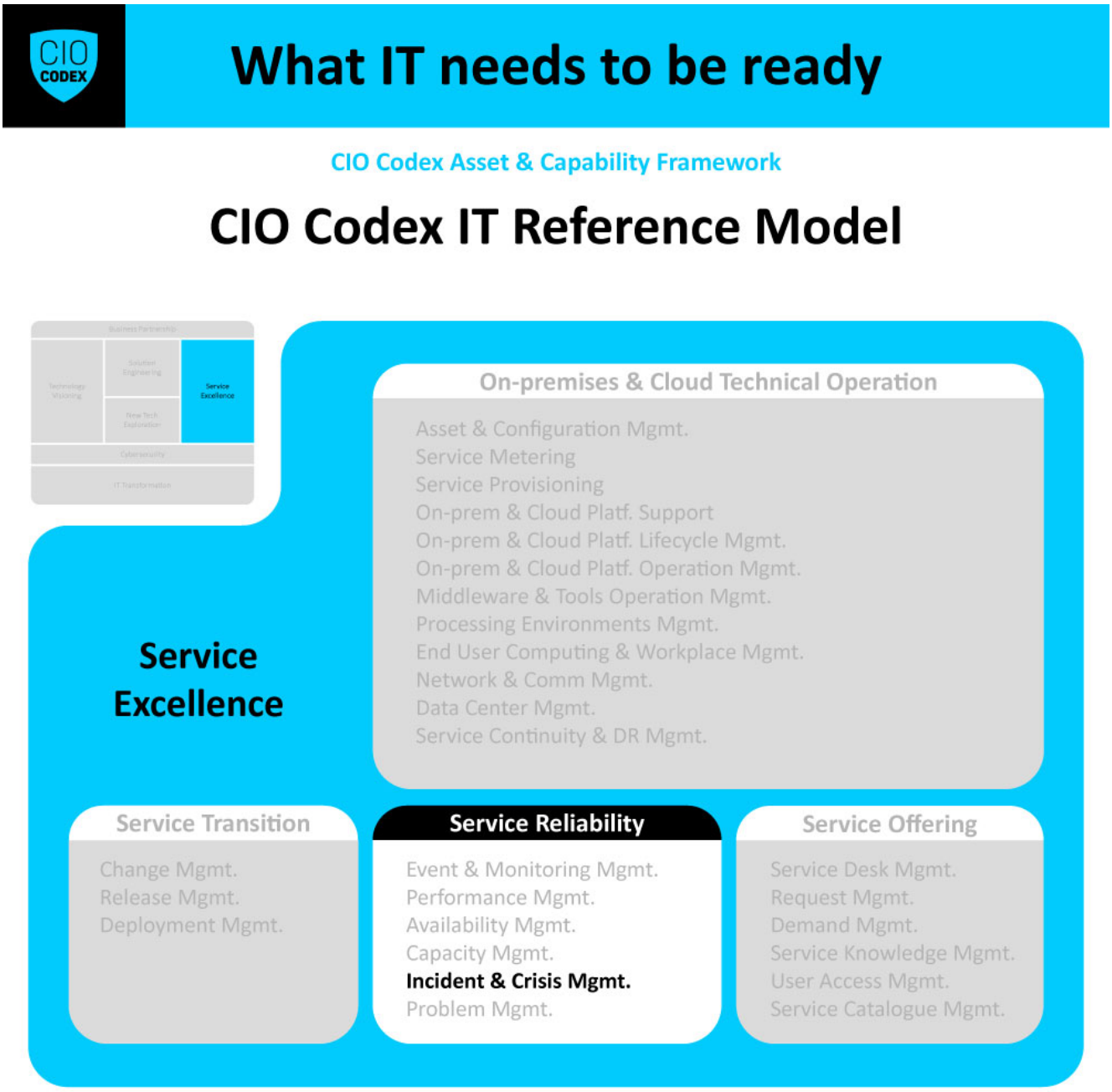

A Incident & Crisis Management, situada na macro capability Service Reliability e na camada Service Excellence do CIO Codex Capability Framework, é fundamental para manter a confiabilidade dos serviços de TI e proteger os interesses da organização em situações adversas.

Esta capability é vital para assegurar uma resposta rápida e eficaz, minimizando perdas e garantindo a continuidade das operações, contribuindo significativamente para a resiliência do negócio.

Os conceitos chave da Incident & Crisis Management incluem o Incidente de TI, que se refere a qualquer evento não planejado que cause ou possa causar uma interrupção nos serviços de TI.

A Crisis Management lida com situações mais graves, que ameaçam a operação normal do negócio e exigem ação imediata.

A Comunicação de Crise é essencial, envolvendo a comunicação transparente e eficaz com todas as partes interessadas durante uma crise.

Características distintas desta capability incluem uma Rápida Resposta, priorizando a resposta imediata a incidentes e crises para minimizar o impacto nos negócios.

A Coordenação de Equipes multifuncionais é essencial para lidar com incidentes e crises de forma eficiente.

A Análise Pós-Incidente é realizada após a resolução para compreender as causas e implementar medidas preventivas.

A Prevenção de Recorrências é alcançada aprendendo com incidentes anteriores e implementando melhorias contínuas.

Planos de Continuidade de Negócios são desenvolvidos e alinhados com a capability para garantir resiliência em caso de crises.

O propósito central da Incident & Crisis Management é garantir uma resposta eficaz a incidentes, minimizando o impacto nos negócios e restaurando os serviços o mais rápido possível.

Esta capability também visa à coordenação eficiente de equipes, à comunicação eficaz com stakeholders e à análise pós-incidente para prevenir recorrências.

Dentro do CIO Codex Capability Framework, os objetivos da Incident & Crisis Management incluem garantir a Eficiência Operacional, proporcionando uma resposta rápida e eficaz a incidentes, minimizando o tempo de inatividade e os custos associados.

A Inovação é impulsionada pela adoção de melhores práticas e tecnologias para melhorar a capacidade de resposta.

A Vantagem Competitiva é fortalecida ao manter a continuidade dos serviços em face de incidentes críticos.

A Infraestrutura de TI é coordenada para restauração rápida em caso de incidentes ou crises.

A Arquitetura de TI é projetada para integrar considerações de gestão de incidentes e crises, garantindo resiliência.

A minimização do impacto de incidentes nos Sistemas de TI é crucial, e o Modelo Operacional integra a gestão de incidentes e crises aos processos operacionais,

assegurando uma resposta organizada e coordenada.

O impacto da Incident & Crisis Management nas dimensões tecnológicas é abrangente.

A Infraestrutura de TI é coordenada para uma rápida recuperação em caso de incidentes ou crises.

A Arquitetura de TI integra considerações de resiliência, garantindo a continuidade dos serviços.

A minimização do impacto de incidentes nos Sistemas de TI é essencial.

Em Cybersecurity, a gestão eficaz de incidentes é vital para lidar com ameaças de maneira adequada.

O Modelo Operacional integra a gestão de incidentes e crises, garantindo uma resposta organizada e coordenada.

Em síntese, a Incident & Crisis Management é uma capability crucial para qualquer organização que dependa de serviços de TI confiáveis.

Ela não apenas assegura uma resposta eficaz a incidentes, mas também contribui para a resiliência organizacional, integrando-se harmoniosamente a outras capabilities dentro do CIO Codex Capability Framework.

Conceitos e Características

A Incident & Crisis Management é essencial para a manutenção da confiabilidade dos serviços de TI e a proteção dos interesses da organização durante situações adversas.

Sua capacidade de resposta rápida e eficaz é fundamental para minimizar perdas e garantir a continuidade das operações, contribuindo para a resiliência do negócio.

Conceitos

- Incidente de TI: Refere-se a qualquer evento não planejado que cause ou possa causar uma interrupção nos serviços de TI.
- Crisis Management: Lida com situações mais graves que ameaçam a operação normal do negócio e exigem ação imediata.
- Comunicação de Crise: Envolve a comunicação transparente e eficaz com

todas as partes interessadas durante uma crise.

Características

- Rápida Resposta: A capability prioriza a resposta rápida a incidentes e crises para minimizar o impacto nos negócios.
- Coordenação de Equipes: Ela coordena equipes multifuncionais para lidar com incidentes e crises de forma eficiente.
- Análise Pós-Incidente: Após a resolução, a análise pós-incidente é realizada para entender as causas e implementar medidas preventivas.
- Prevenção de Recorrências: A capacidade de aprender com incidentes anteriores e implementar melhorias contínuas ajuda a prevenir recorrências.
- Planos de Continuidade de Negócios: Trabalha em estreita colaboração com a continuidade de negócios para garantir que os planos estejam alinhados em caso de crises.

Propósito e Objetivos

A capability de Incident & Crisis Management desempenha um papel crítico na gestão de incidentes e crises de TI.

Seu propósito central é garantir uma resposta eficaz a incidentes, minimizando o impacto nos negócios e restaurando os serviços o mais rápido possível.

Além disso, visa à coordenação de equipes, à comunicação eficaz com stakeholders e à análise pós-incidente para prevenir recorrências.

Objetivos

Dentro do contexto do CIO Codex Capability Framework, a Incident & Crisis Management busca atingir os seguintes objetivos:

- Eficiência Operacional: Garantir uma resposta rápida e eficaz a incidentes, minimizando o tempo de inatividade e os custos associados.
- Inovação: Adotar melhores práticas e tecnologias para melhorar a

capacidade de resposta a incidentes e a gestão de crises.
- Vantagem Competitiva: Contribuir para a vantagem competitiva da organização, mantendo a continuidade dos serviços mesmo em face de incidentes críticos.
- Infraestrutura: Coordenar ações para restaurar a infraestrutura de TI afetada por incidentes ou crises.
- Arquitetura: Integrar considerações de gestão de incidentes e crises na arquitetura de sistemas, garantindo a resiliência.
- Sistemas: Minimizar o impacto de incidentes nos sistemas de TI, restaurando o funcionamento normal de maneira eficaz.
- Modelo Operacional: Integrar a gestão de incidentes e crises aos processos operacionais, assegurando uma resposta organizada e coordenada.

Impacto na Tecnologia

A capability de Incident & Crisis Management afeta várias dimensões tecnológicas:

- Infraestrutura: Coordenar a recuperação de infraestrutura de TI afetada por incidentes ou crises, minimizando o tempo de inatividade.
- Arquitetura: Integrar considerações de resiliência na arquitetura de sistemas, garantindo a continuidade dos serviços.
- Sistemas: Minimizar o impacto de incidentes nos sistemas de TI, restaurando o funcionamento normal de maneira eficaz.
- Cybersecurity: Uma gestão eficaz de incidentes é vital para lidar com ameaças à segurança de forma adequada.
- Modelo Operacional: Integrar a gestão de incidentes e crises aos processos operacionais, garantindo uma resposta organizada e coordenada.

Roadmap de Implementação

A capability de Incident & Crisis Management desempenha um papel crucial na gestão de incidentes e crises de TI, assegurando uma resposta eficaz para minimizar o

impacto nos negócios e garantir a continuidade das operações.

Abaixo, um roadmap de implementação para a Incident & Crisis Management, considerando os principais pontos do CIO Codex Capability Framework:

- Definição de Papéis e Responsabilidades: Inicie o processo definindo claramente os papéis e responsabilidades das equipes envolvidas na gestão de incidentes e crises. Isso inclui a designação de líderes de incidentes e especialistas técnicos.
- Desenvolvimento de Políticas e Procedimentos: Elabore políticas e procedimentos detalhados para lidar com incidentes e crises de TI. Esses documentos devem abordar a identificação, classificação, priorização e escalonamento de incidentes.
- Formação de Equipes Multifuncionais: Monte equipes multifuncionais que incluam representantes de diferentes áreas da organização, como TI, segurança cibernética, comunicação e gestão de negócios. Garanta que essas equipes sejam treinadas e estejam preparadas para responder eficazmente.
- Avaliação de Riscos: Realize uma avaliação abrangente dos riscos que a organização enfrenta, identificando as possíveis fontes de incidentes e crises. Isso ajuda a priorizar o planejamento e a alocação de recursos.
- Desenvolvimento de Planos de Continuidade de Negócios: Trabalhe em estreita colaboração com a continuidade de negócios para garantir que os planos estejam alinhados em caso de crises. Isso inclui a identificação de sistemas críticos e medidas de recuperação.
- Implementação de Plataforma de Gestão de Incidentes: Adote uma plataforma de gestão de incidentes que permita o registro, acompanhamento e resolução eficiente de incidentes. Essa ferramenta deve ser acessível a todas as equipes envolvidas.
- Exercícios de Simulação de Crises: Realize exercícios de simulação de crises regularmente para testar a eficácia dos planos e a coordenação das equipes. Isso ajuda a identificar áreas de melhoria.
- Comunicação Transparente: Desenvolva um plano de comunicação de crises que inclua a comunicação com todas as partes interessadas, internas e externas. Garanta que a comunicação seja transparente e eficaz durante situações adversas.
- Análise Pós-Incidente e Melhoria Contínua: Após a resolução de

incidentes e crises, realize análises pós-incidente para entender as causas e identificar oportunidades de melhoria. Implemente medidas preventivas para evitar recorrências.
- Auditorias e Revisões Regulares: Realize auditorias e revisões regulares dos processos de Incident & Crisis Management para garantir que estejam alinhados com as melhores práticas e os requisitos regulatórios.
- Treinamento e Conscientização: Mantenha um programa contínuo de treinamento e conscientização para as equipes envolvidas, mantendo todos atualizados sobre as políticas, procedimentos e melhores práticas.
- Integração com outras capabilities: Colabore com outras capabilities, como Risk Management e Security Management, para garantir uma abordagem abrangente à gestão de incidentes e crises.

Ao seguir este roadmap de implementação, as organizações podem fortalecer sua capacidade de gerenciar incidentes e crises de TI de forma eficaz.

A capability de Incident & Crisis Management desempenha um papel crítico na proteção dos interesses da organização durante situações adversas, contribuindo para a resiliência do negócio, a continuidade das operações e a minimização de perdas.

Melhores Práticas de Mercado

A capability Incident & Crisis Management desempenha um papel crítico na gestão de situações adversas, garantindo a continuidade das operações e protegendo os interesses da organização.

A rápida identificação, resposta coordenada e análise pós-incidente são elementos essenciais para manter a resiliência do negócio.

Melhores práticas de mercado relacionadas à capability Incident & Crisis Management no contexto do CIO Codex Capability Framework:

- Rápida Identificação de Incidentes: Estabelecer processos e ferramentas eficazes para identificar rapidamente os incidentes de TI, permitindo uma resposta imediata.
- Classificação e Priorização: Implementar sistemas de classificação e priorização de incidentes com base em seu impacto e urgência,

garantindo que os recursos sejam alocados de acordo com a gravidade.
- Equipes Multifuncionais de Resposta: Montar equipes multifuncionais de resposta a incidentes, que incluam especialistas em TI, segurança, comunicação e outras áreas relevantes.
- Comunicação Transparente: Ter um plano de comunicação de crise claro, garantindo que todas as partes interessadas sejam informadas de forma transparente durante uma crise.
- Análise Pós-Incidente: Realizar análises detalhadas após a resolução de incidentes para identificar causas raiz e implementar medidas preventivas.
- Simulações e Testes: Realizar simulações regulares de incidentes e testes de resposta a crises para garantir que as equipes estejam preparadas.
- Integração com Continuidade de Negócios: Trabalhar em estreita colaboração com a continuidade de negócios para alinhar os planos de recuperação de desastres e garantir a continuidade das operações.
- Gestão de Crises: Implementar um sistema de gestão de crises que permita uma resposta coordenada e eficaz em situações de crise.
- Aprendizado Contínuo: Estabelecer um ciclo de aprendizado contínuo, onde as lições aprendidas com incidentes e crises anteriores são usadas para melhorar a capacidade de resposta.
- Documentação Detalhada: Manter registros detalhados de todos os incidentes e crises, incluindo ações tomadas, resoluções e melhorias implementadas.

Essas melhores práticas de mercado são cruciais para garantir uma resposta eficaz a incidentes e crises de TI.

Desafios Atuais

A Capability de Incident & Crisis Management, pertencente à macro capability Service Reliability e à camada Service Excellence, desempenha um papel fundamental na manutenção da confiabilidade dos serviços de TI e na proteção dos interesses da organização durante situações adversas.

Contudo, ao adotar e integrar essa capability em seus processos de negócios e operações de TI, as organizações deparam-se com diversos desafios atuais que

demandam atenção e estratégias eficazes para enfrentá-los, seguindo as melhores práticas de mercado.

- Dentro do contexto do CIO Codex Capability Framework, os principais desafios atuais relacionados à Incident & Crisis Management são:
- Amplitude de Incidentes: Lidar com a crescente variedade de incidentes de TI, desde falhas de sistemas até ameaças cibernéticas sofisticadas, é um desafio complexo.
- Rapidez de Resposta: A pressão por uma resposta rápida a incidentes é intensa, considerando o impacto financeiro e de reputação que atrasos podem causar.
- Coordenação Efetiva: Coordenar equipes multifuncionais durante situações de crise exige uma estrutura organizacional clara e planos de ação bem definidos.
- Gerenciamento de Crises Externas: Lidar com crises que envolvem partes externas à organização, como fornecedores, clientes e reguladores, adiciona complexidade.
- Comunicação de Crise: Garantir uma comunicação transparente e eficaz com todas as partes interessadas durante uma crise é essencial para manter a confiança.
- Análise Pós-Incidente: Realizar análises aprofundadas pós-incidente para identificar causas raiz e implementar melhorias é um desafio constante.
- Prevenção de Recorrências: Aprender com incidentes anteriores e implementar medidas preventivas eficazes é crucial para evitar recorrências.
- Integração com Continuidade de Negócios: Coordenar as ações de Incident & Crisis Management com planos de continuidade de negócios é fundamental para a resiliência.
- Cibersegurança: Gerenciar incidentes cibernéticos requer uma abordagem especializada para enfrentar ameaças em constante evolução.
- Treinamento e Conscientização: Capacitar a equipe e criar uma cultura de conscientização sobre a importância da gestão de incidentes e crises é um desafio cultural.
- Mudanças na Legislação: A evolução das leis de privacidade e conformidade aumenta a pressão para lidar adequadamente com incidentes que envolvem dados sensíveis.

Esses desafios atuais destacam a necessidade crítica de uma abordagem abrangente e estratégica para a Incident & Crisis Management.

A capacidade de resposta rápida e eficaz a incidentes e crises é fundamental para minimizar perdas financeiras, proteger a reputação da organização e garantir a continuidade das operações.

Para superar esses desafios, as organizações devem investir em tecnologia, treinamento, processos eficientes e uma cultura organizacional que valorize a preparação para incidentes e a gestão de crises.

A capacidade de Incident & Crisis Management é um pilar fundamental da resiliência empresarial na era digital.

Tendências para o Futuro

A Incident & Crisis Management, uma parte integral da macro capability de Service Reliability e situada na camada Service Excellence, desempenha um papel essencial na manutenção da confiabilidade dos serviços de TI e na proteção dos interesses da organização durante situações adversas.

Sua capacidade de resposta rápida e eficaz é fundamental para minimizar perdas e garantir a continuidade das operações, contribuindo para a resiliência do negócio.

Considerando as expectativas do mercado e as tendências emergentes que podem moldar o futuro da Incident & Crisis Management, as seguintes tendências:

- Inteligência Artificial para Detecção de Incidentes: A IA será amplamente utilizada na detecção precoce de incidentes, permitindo uma resposta mais rápida e eficaz.
- Automatização de Resposta a Incidentes: A automação desempenhará um papel fundamental na resposta imediata a incidentes de rotina, liberando equipes para lidar com situações mais complexas.
- Gestão de Crises Virtuais: Com a crescente digitalização, a capacidade de gerenciar crises virtuais, como ciberataques, será essencial para a proteção da reputação da empresa.
- Integração com Business Continuity: Uma colaboração mais estreita entre Incident & Crisis Management e Business Continuity garantirá uma resposta coordenada a incidentes que afetam a continuidade dos

negócios.

- Monitoramento Proativo de Ameaças Cibernéticas: A capacidade de monitorar proativamente ameaças cibernéticas em tempo real ajudará a prevenir incidentes graves.
- Resposta Global a Incidentes: Empresas com operações globais precisarão de uma capacidade de resposta a incidentes que leve em consideração as diferenças culturais e regulatórias em várias regiões.
- Comunicação Multicanal em Crises: A comunicação eficaz durante crises exigirá o uso de múltiplos canais, incluindo mídias sociais e aplicativos de mensagens.
- Treinamento Contínuo de Equipes: O treinamento contínuo das equipes de Incident & Crisis Management será fundamental para manter a prontidão e a eficácia.
- Análise Avançada pós-Incidente: A análise pós-incidente será aprimorada com o uso de análise avançada de dados para identificar causas subjacentes e padrões emergentes.
- Cultura de Resiliência Organizacional: As empresas buscarão promover uma cultura de resiliência em toda a organização, reconhecendo que a capacidade de resposta a incidentes é responsabilidade de todos.

Essas tendências refletem a crescente complexidade e dinâmica do ambiente empresarial e de TI.

A capacidade de Incident & Crisis Management evoluirá para atender às demandas emergentes, abraçando a automação, a inteligência artificial e a colaboração interdisciplinar para garantir que as organizações possam enfrentar incidentes e crises com eficácia e resiliência.

KPIs Usuais

A Incident & Crisis Management é uma capability essencial no contexto da Service Excellence, pertencendo à macro capability Service Reliability.

Sua missão central é garantir a resposta eficaz a incidentes e crises de TI, minimizando impactos nos negócios e mantendo a continuidade operacional.

A medição do desempenho dessa capability é crucial para a proteção dos interesses da

organização e a preservação da confiabilidade dos serviços de TI.

A seguir, uma lista dos principais KPIs usuais para Incident & Crisis Management, alinhados com o CIO Codex Capability Framework:

- Tempo Médio de Resposta a Incidentes (Average Incident Response Time): Mede o tempo médio necessário para iniciar a resposta a incidentes de TI, desde o momento em que são detectados.
- Tempo Médio de Recuperação (Average Recovery Time): Calcula o tempo médio necessário para restaurar os serviços de TI afetados por incidentes.
- Taxa de Sucesso na Resolução de Incidentes (Incident Resolution Success Rate): Avalia a eficácia da capability em resolver incidentes de forma bem-sucedida.
- Número de Incidentes Críticos Não Gerenciados (Number of Unmanaged Critical Incidents): Conta o número de incidentes críticos que não foram gerenciados eficazmente.
- Taxa de Recorrência de Incidentes (Incident Recurrence Rate): Mede a frequência com que os mesmos tipos de incidentes ocorrem novamente após sua resolução.
- Tempo Médio para Comunicação de Crise (Average Crisis Communication Time): Calcula o tempo médio necessário para iniciar a comunicação de crise durante situações adversas.
- Taxa de Preparação para Crises (Crisis Preparedness Rate): Avalia a prontidão da organização para lidar com crises, incluindo a eficácia dos planos de continuidade de negócios.
- Tempo Médio para Mobilização de Equipes (Average Team Mobilization Time): Mede o tempo médio necessário para reunir e mobilizar equipes multidisciplinares durante crises.
- Taxa de Recuperação de Dados (Data Recovery Rate): Avalia a capacidade de recuperar dados após incidentes que envolvem perda de informação.
- Taxa de Documentação Pós-Incidente (Post-Incident Documentation Rate): Mede a frequência com que a análise pós-incidente e as lições aprendidas são documentadas.
- Taxa de Treinamento em Gestão de Crises (Crisis Management Training Rate): Avalia a taxa de treinamento das equipes envolvidas em gestão de crises.
- Tempo Médio para Ativação de Planos de Continuidade (Average Business

Continuity Plan Activation Time): Calcula o tempo médio necessário para ativar os planos de continuidade de negócios durante crises.
- Número de Interrupções Evitadas (Number of Avoided Disruptions): Contabiliza o número de interrupções de serviços que foram evitadas devido à eficácia da capability.
- Taxa de Atualização de Planos de Continuidade (Business Continuity Plan Update Rate): Avalia a regularidade com que os planos de continuidade de negócios são revisados e atualizados.
- Taxa de Comunicação Eficaz de Crise (Effective Crisis Communication Rate): Mede a eficácia da comunicação com todas as partes interessadas durante crises.

Esses KPIs desempenham um papel crucial na avaliação e aprimoramento da capacidade de Incident & Crisis Management.

Eles garantem que a organização esteja preparada para responder a incidentes e crises de forma eficaz, minimizando riscos e impactos nos negócios.

O monitoramento constante desses indicadores permite uma melhoria contínua da capacidade e contribui para a resiliência do negócio diante de desafios inesperados.

Exemplos de OKRs

A capability de Incident & Crisis Management na macro capability Service Reliability da camada Service Excellence desempenha um papel crítico na gestão eficaz de incidentes e crises de TI.

Esta capability assegura uma rápida resposta, minimiza o impacto nos negócios e restaura os serviços o mais rápido possível. Além disso, inclui a coordenação de equipes, comunicação com stakeholders e análise pós-incidente para prevenir recorrências.

Abaixo, exemplos de Objetivos e Resultados-Chave (OKRs) relacionados a esta capability:

Resposta Rápida a Incidentes

Objetivo: Garantir uma resposta rápida e eficaz a incidentes de TI para minimizar o impacto nos negócios.

- KR1: Criar uma equipe de resposta a incidentes de prontidão 24 horas por dia, 7 dias por semana.
- KR2: Estabelecer procedimentos de resposta a incidentes que permitam a detecção e ação imediatas.
- KR3: Reduzir o tempo médio de resolução de incidentes em 30% em relação ao ano anterior.

Coordenação de Equipes e Recursos

Objetivo: Coordenar efetivamente equipes e recursos durante incidentes e crises.

- KR1: Designar responsabilidades claras para membros da equipe durante incidentes.
- KR2: Manter uma lista atualizada de recursos de backup prontos para serem acionados em caso de necessidade.
- KR3: Realizar treinamentos regulares de simulação de incidentes para melhorar a coordenação da equipe.

Comunicação com Stakeholders

Objetivo: Manter uma comunicação eficaz com todas as partes interessadas durante incidentes e crises.

- KR1: Estabelecer canais de comunicação de emergência com partes interessadas internas e externas.
- KR2: prover atualizações regulares sobre o status do incidente e as ações tomadas.
- KR3: Realizar revisões pós-incidente com as partes interessadas para avaliar a resposta e identificar melhorias.

Análise Pós-Incidente e Prevenção de Recorrências

Objetivo: Realizar análises pós-incidente para identificar causas raiz e implementar medidas para prevenir recorrências.

- KR1: Realizar análises detalhadas de todos os incidentes significativos.

- KR2: Identificar causas raiz e desenvolver planos de ação corretiva.
- KR3: Reduzir em 50% o número de recorrências de incidentes no próximo ano.

Treinamento e Conscientização

Objetivo: Garantir que todos os funcionários estejam treinados e cientes dos procedimentos de gestão de incidentes.

- KR1: prover treinamento de conscientização sobre incidentes para todos os funcionários.
- KR2: Realizar exercícios regulares de treinamento de resposta a incidentes.
- KR3: Avaliar a competência da equipe por meio de testes práticos.

Esses OKRs demonstram a importância crítica da capability de Incident & Crisis Management na macro capability Service Reliability, dentro da camada Service Excellence.

A gestão eficaz de incidentes e crises de TI é essencial para garantir a continuidade dos serviços, a satisfação do cliente e a minimização de impactos financeiros.

Essa capability atua como um elemento fundamental na resiliência da organização em um ambiente de TI cada vez mais complexo e sujeito a ameaças.

Critérios para Avaliação de Maturidade

A capability Incident & Crisis Management, inserida na macro capability Service Reliability e na camada Service Excellence, desempenha um papel crítico na gestão eficaz de incidentes e crises em ambientes de TI.

Sua missão é garantir uma resposta rápida, minimizar o impacto nos negócios e restaurar os serviços o mais rápido possível.

Para avaliar a maturidade dessa capability dentro do contexto do CIO Codex Capability Framework, foram desenvolvidos critérios de avaliação de maturidade, inspirados no modelo CMMI, abrangendo cinco níveis de maturidade:

Nível de Maturidade Inexistente

- A organização não reconhece a necessidade de gerenciamento de incidentes e crises.
- Não há procedimentos ou políticas para lidar com incidentes e crises.
- A falta de conscientização sobre a importância da gestão de incidentes e crises é evidente.
- Não há recursos designados para responder a incidentes e crises.
- Ausência de comunicação formal com stakeholders durante incidentes ou crises.

Nível de Maturidade Inicial

- Reconhecimento inicial da importância do gerenciamento de incidentes e crises.
- Procedimentos básicos são definidos, mas não completamente abrangentes.
- A conscientização sobre a gestão de incidentes e crises está aumentando.
- Alguns recursos são designados para responder a incidentes e crises.
- Comunicação limitada com stakeholders durante incidentes ou crises.

Nível de Maturidade Definido

- Políticas e procedimentos para gerenciamento de incidentes e crises estão estabelecidos e documentados.
- Procedimentos são consistentemente seguidos.
- A conscientização sobre a gestão de incidentes e crises é difundida em toda a organização.
- Recursos são alocados e treinados para responder eficazmente.
- Comunicação com stakeholders é eficaz e padronizada durante incidentes e crises.

Nível de Maturidade Gerenciado

- A gestão de incidentes e crises é monitorada e medida regularmente.
- Procedimentos são altamente eficazes e adaptáveis.
- A conscientização e o treinamento são contínuos e avançados.
- Recursos são alocados de forma otimizada para uma resposta eficaz.
- A comunicação com stakeholders é proativa e eficiente durante incidentes ou crises.

Nível de Maturidade Otimizado

- A gestão de incidentes e crises é altamente automatizada e eficaz.
- Processos são altamente otimizados e adaptáveis a diferentes tipos de incidentes e crises.
- A conscientização é parte da cultura organizacional.
- Recursos são alocados de forma dinâmica para uma resposta ágil.
- A comunicação com stakeholders é personalizada e estratégica durante incidentes ou crises.

Esses critérios de maturidade são cruciais para garantir que a capability Incident & Crisis Management seja capaz de gerenciar incidentes e crises de forma eficiente, minimizando interrupções nos serviços de TI e protegendo os interesses da organização.

À medida que a organização progride nos níveis de maturidade, sua capacidade de lidar com incidentes e crises se torna mais eficaz e adaptável às necessidades em constante mudança do ambiente de TI e de negócios.

Convergência com Frameworks de Mercado

No contexto do CIO Codex Capability Framework, a capability Incident & Crisis Management é essencial para uma resposta efetiva e ágil a incidentes e crises dentro do ambiente de TI.

Esta capability assegura que, no evento de uma interrupção inesperada, as operações críticas possam ser restauradas o mais rapidamente possível, minimizando impactos

negativos e mantendo a continuidade do negócio.

A gestão de incidentes e crises envolve não apenas a resolução de problemas técnicos, mas também uma comunicação eficiente com todas as partes interessadas e uma análise aprofundada após a resolução, para aprimorar os processos e evitar futuras ocorrências.

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 provê um modelo para governança e gestão que inclui a gestão de incidentes como parte de suas práticas recomendadas, enfatizando a importância de controles e processos estruturados para lidar com interrupções de serviços.

ITIL

- Nível de Convergência: Alto
- Racional: A framework ITIL possui um processo dedicado ao gerenciamento de incidentes, que é diretamente relevante para a capability Incident & Crisis Management. As práticas recomendadas de ITIL para a resolução e prevenção de incidentes são amplamente aceitas como padrão no mercado.

SAFe

- Nível de Convergência: Médio
- Racional: O SAFe aborda a resiliência e a capacidade de resposta a mudanças, o que pode ser relacionado com a gestão de crises no contexto de desenvolvimento ágil e entrega contínua.

PMI

- Nível de Convergência: Médio
- Racional: O PMI foca no gerenciamento de projetos, onde a gestão de riscos pode incluir a preparação para incidentes e crises, embora não seja um foco principal do framework.

CMMI

- Nível de Convergência: Médio
- Racional: O CMMI inclui práticas para planejamento e gestão de processos que podem ser aplicadas à gestão de incidentes, visando a melhoria contínua e a resiliência organizacional.

TOGAF

- Nível de Convergência: Baixo
- Racional: Enquanto o TOGAF é focado em arquitetura empresarial, suas práticas podem influenciar indiretamente a capacidade de resposta a incidentes dentro do planejamento arquitetônico.

DevOps SRE

- Nível de Convergência: Alto
- Racional: O SRE, uma componente chave do DevOps, concentra-se na confiabilidade do serviço e na rápida resolução de incidentes, o que está em completa harmonia com os princípios do Incident & Crisis Management.

NIST

- Nível de Convergência: Médio
- Racional: O NIST fornece diretrizes sobre cibersegurança e resposta a incidentes, que são componentes vitais da gestão de crises e incidentes em TI.

Six Sigma

- Nível de Convergência: Baixo
- Racional: O Six Sigma é uma metodologia de melhoria de qualidade que não aborda diretamente a gestão de incidentes, mas seus princípios de redução de defeitos podem ser aplicados para melhorar a resposta a incidentes.

Lean IT

- Nível de Convergência: Baixo
- Racional: O Lean IT visa a eficiência operacional e a eliminação de desperdícios, que indiretamente pode suportar a capacidade de uma organização de responder eficientemente a incidentes.

Em resumo, a capability Incident & Crisis Management é crítica para a resiliência de TI e a continuidade dos negócios.

Sua eficácia é aumentada quando alinhada com as práticas recomendadas dos frameworks de mercado, o que pode variar dependendo do foco e aplicação específica de cada framework.

A implementação desta capability deve ser feita com atenção às melhores práticas de mercado, antecipando-se às tendências futuras, e com foco na otimização contínua para enfrentar desafios emergentes no cenário de TI.

A mensuração do sucesso pode ser realizada por meio de KPIs e OKRs que refletem a eficiência na gestão de incidentes e crises, assim como na maturidade alcançada em conformidade com a escala inspirada no CMMI.

Processos e Atividades

Develop Incident Management Plans

Desenvolver planos de gestão de incidentes é essencial para assegurar que a

organização esteja preparada para responder de maneira eficaz a qualquer evento não planejado que possa interromper os serviços de TI.

Este processo envolve a criação de um plano detalhado que inclui políticas, procedimentos e responsabilidades claramente definidos para a gestão de incidentes.

As atividades incluem a identificação dos tipos de incidentes que podem ocorrer, a definição de critérios para classificação e priorização de incidentes e a elaboração de procedimentos de resposta.

O plano deve também delinear as etapas para a comunicação interna e externa durante um incidente, assegurando que todas as partes interessadas estejam informadas.

A documentação do plano é fundamental para garantir que todos os membros da equipe de TI estejam cientes de suas responsabilidades e saibam como agir em caso de um incidente.

A colaboração entre diversas áreas de TI e de negócios é crucial para o desenvolvimento de um plano abrangente e eficaz.

- PDCA focus: Plan
- Periodicidade: Anual

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Identify Incident Types	Identificar os tipos de incidentes que podem ocorrer.	Dados históricos, feedback dos stakeholders	Tipos de incidentes identificados	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Cybersecurity; Informed: IT Governance & Transformation	Decider: IT Infrastructure & Operation; Advisor: Cybersecurity; Recommender: IT Governance & Transformation; Executer: IT Infrastructure & Operation

2	Define Classification Criteria	Definir critérios para classificação e priorização de incidentes.	Tipos de incidentes, melhores práticas	Critérios de classificação definidos	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Data, AI & New Technology; Informed: Solution Engineering & Development	Decider: IT Infrastructure & Operation; Advisor: Data, AI & New Technology; Recommender: Solution Engineering & Development; Executer: IT Infrastructure & Operation
3	Develop Response Procedures	Desenvolver procedimentos de resposta para cada tipo de incidente identificado.	Critérios de classificação, melhores práticas	Procedimentos de resposta desenvolvidos	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Solution Engineering & Development; Informed: Architecture & Technology Visioning	Decider: IT Infrastructure & Operation; Advisor: Solution Engineering & Development; Recommender: Architecture & Technology Visioning; Executer: IT Infrastructure & Operation
4	Establish Communication Plan	Estabelecer um plano de comunicação para incidentes.	Procedimentos de resposta, melhores práticas	Plano de comunicação estabelecido	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Cybersecurity; Informed: IT Governance & Transformation	Decider: IT Infrastructure & Operation; Advisor: Cybersecurity; Recommender: IT Governance & Transformation; Executer: IT Infrastructure & Operation

5	Document and Approve Plan	Documentar e obter aprovação do plano de gestão de incidentes.	Plano de comunicação, procedimentos de resposta	Plano de gestão de incidentes aprovado	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: IT Governance & Transformation; Informed: Solution Engineering & Development	Decider: IT Infrastructure & Operation; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: IT Infrastructure & Operation

Identify Incident Requirements

Identificar os requisitos para gestão de incidentes é um passo crucial para garantir que a organização esteja adequadamente preparada para responder a qualquer evento adverso.

Este processo envolve a coleta e análise de dados para determinar as necessidades específicas da organização em termos de recursos, ferramentas e procedimentos para a gestão de incidentes.

As atividades incluem a avaliação dos sistemas e serviços críticos, a identificação de vulnerabilidades potenciais e a definição dos níveis de serviço esperados durante e após um incidente.

A colaboração com várias áreas de TI e de negócios é essencial para garantir que todos os requisitos sejam identificados e compreendidos.

A documentação desses requisitos é fundamental para a elaboração de um plano de gestão de incidentes eficaz e para a definição de métricas de desempenho que serão usadas para monitorar e avaliar a eficácia das atividades de resposta a incidentes.

- PDCA focus: Plan
- Periodicidade: Anual

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE

1	Assess Critical Systems	Avaliar os sistemas e serviços críticos da organização.	Inventário de TI, dados de desempenho	Lista de sistemas críticos	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Cybersecurity; Informed: IT Governance & Transformation	Decider: IT Infrastructure & Operation; Advisor: Cybersecurity; Recommender: IT Governance & Transformation; Executer: IT Infrastructure & Operation
2	Identify Potential Vulnerabilities	Identificar vulnerabilidades potenciais nos sistemas e serviços críticos.	Avaliação de sistemas críticos, auditorias de segurança	Vulnerabilidades identificadas	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Cybersecurity; Informed: IT Governance & Transformation	Decider: IT Infrastructure & Operation; Advisor: Cybersecurity; Recommender: IT Governance & Transformation; Executer: IT Infrastructure & Operation
3	Define Service Levels	Definir níveis de serviço esperados durante e após um incidente.	Análise de vulnerabilidades, metas de negócio	Níveis de serviço definidos	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Architecture & Technology Visioning; Informed: Solution Engineering & Development	Decider: IT Infrastructure & Operation; Advisor: Architecture & Technology Visioning; Recommender: Solution Engineering & Development; Executer: IT Infrastructure & Operation

4	Determine Resource Needs	Determinar as necessidades de recursos para a gestão de incidentes.	Níveis de serviço definidos, inventário de recursos	Necessidades de recursos determinadas	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Data, AI & New Technology; Informed: Cybersecurity	Decider: IT Infrastructure & Operation; Advisor: Data, AI & New Technology; Recommender: Cybersecurity; Executer: IT Infrastructure & Operation
5	Document Requirements	Documentar todos os requisitos de gestão de incidentes.	Necessidades de recursos, níveis de serviço definidos	Requisitos de gestão de incidentes documentados	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: IT Governance & Transformation; Informed: Solution Engineering & Development	Decider: IT Infrastructure & Operation; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: IT Infrastructure & Operation

Execute Incident Management Activities

Executar as atividades de gestão de incidentes conforme planejado é crucial para garantir uma resposta rápida e eficaz a qualquer evento que possa interromper os serviços de TI.

Este processo envolve a implementação dos procedimentos de resposta a incidentes, conforme definido no plano de gestão de incidentes, e a coordenação das equipes de resposta.

As atividades incluem a identificação e registro de incidentes, a análise e classificação dos mesmos, a execução de ações corretivas e a comunicação constante com todas as partes interessadas.

A utilização de ferramentas e tecnologias adequadas é essencial para a identificação rápida e precisa de incidentes e para a implementação eficaz das ações de resposta.

A documentação de todas as atividades é fundamental para garantir a rastreabilidade e a transparência, além de fornecer informações valiosas para a análise pós-incidente e a melhoria contínua dos processos de gestão de incidentes.

- PDCA focus: Do
- Periodicidade: Contínua

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Identify and Log Incidents	Identificar e registrar incidentes de TI.	Alertas de monitoramento, feedback dos usuários	Incidentes registrados	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Cybersecurity; Informed: IT Governance & Transformation	Decider: IT Infrastructure & Operation; Advisor: Cybersecurity; Recommender: IT Governance & Transformation; Executer: IT Infrastructure & Operation
2	Analyze and Classify Incidents	Analisar e classificar incidentes com base em sua criticidade.	Incidentes registrados, critérios de classificação	Incidentes classificados	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Solution Engineering & Development; Informed: Architecture & Technology Visioning	Decider: IT Infrastructure & Operation; Advisor: Solution Engineering & Development; Recommender: Architecture & Technology Visioning; Executer: IT Infrastructure & Operation
3	Execute Corrective Actions	Executar ações corretivas para resolver incidentes.	Incidentes classificados, plano de resposta	Incidentes resolvidos	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Data, AI & New Technology; Informed: Cybersecurity	Decider: IT Infrastructure & Operation; Advisor: Data, AI & New Technology; Recommender: Cybersecurity; Executer: IT Infrastructure & Operation

4	Communicate with Stakeholders	Comunicar-se com as partes interessadas sobre o status dos incidentes.	Status dos incidentes, plano de comunicação	Comunicação de status	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: IT Governance & Transformation; Informed: Solution Engineering & Development	Decider: IT Infrastructure & Operation; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: IT Infrastructure & Operation
5	Document Incident Activities	Documentar todas as atividades de gestão de incidentes.	Incidentes resolvidos, feedback dos stakeholders	Atividades de incidentes documentadas	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Cybersecurity; Informed: IT Governance & Transformation	Decider: IT Infrastructure & Operation; Advisor: Cybersecurity; Recommender: IT Governance & Transformation; Executer: IT Infrastructure & Operation

Monitor Incident Performance

Monitorar continuamente o desempenho da gestão de incidentes é fundamental para garantir que a resposta a incidentes seja eficaz e que os processos sejam aprimorados continuamente.

Este processo envolve a coleta e análise de dados sobre a performance das atividades de gestão de incidentes, utilizando ferramentas de monitoramento para identificar áreas de melhoria.

As atividades incluem a definição de métricas de desempenho, o monitoramento em tempo real das atividades de resposta a incidentes, a geração de relatórios de desempenho e a realização de revisões periódicas.

A análise dos dados coletados ajuda a identificar tendências e padrões que podem ser usados para melhorar os processos e aumentar a eficácia da gestão de incidentes.

A documentação e a comunicação dos resultados do monitoramento são essenciais para garantir que as partes interessadas estejam cientes do desempenho atual e das

melhorias necessárias.

- PDCA focus: Check
- Periodicidade: Contínua

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Define Performance Metrics	Definir métricas de desempenho para a gestão de incidentes.	Plano de gestão de incidentes, melhores práticas	Métricas de desempenho definidas	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: IT Governance & Transformation; Informed: Cybersecurity	Decider: IT Infrastructure & Operation; Advisor: IT Governance & Transformation; Recommender: Cybersecurity; Executer: IT Infrastructure & Operation
2	Monitor Incident Response	Monitorar a resposta a incidentes em tempo real.	Incidentes registrados, ferramentas de monitoramento	Dados de monitoramento coletados	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Data, AI & New Technology; Informed: Solution Engineering & Development	Decider: IT Infrastructure & Operation; Advisor: Data, AI & New Technology; Recommender: Solution Engineering & Development; Executer: IT Infrastructure & Operation
3	Analyze Performance Data	Analisar os dados de desempenho das atividades de gestão de incidentes.	Dados de monitoramento, métricas de desempenho	Relatório de análise de desempenho	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Cybersecurity; Informed: IT Governance & Transformation	Decider: IT Infrastructure & Operation; Advisor: Cybersecurity; Recommender: IT Governance & Transformation; Executer: IT Infrastructure & Operation

4	Generate Performance Reports	Gerar relatórios de desempenho periódicos para as partes interessadas.	Relatório de análise de desempenho, feedback dos stakeholders	Relatórios de desempenho gerados	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: IT Governance & Transformation; Informed: Solution Engineering & Development	Decider: IT Infrastructure & Operation; Advisor: IT Governance & Transformation; Recommender: Solution Engineering & Development; Executer: IT Infrastructure & Operation
5	Conduct Performance Reviews	Conduzir revisões periódicas de desempenho com as partes interessadas.	Relatórios de desempenho, feedback dos stakeholders	Revisões de desempenho realizadas	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Cybersecurity; Informed: IT Governance & Transformation	Decider: IT Infrastructure & Operation; Advisor: Cybersecurity; Recommender: IT Governance & Transformation; Executer: IT Infrastructure & Operation

Review and Optimize Incident Processes

Revisar e otimizar os processos de gestão de incidentes com base nos resultados obtidos é essencial para garantir a melhoria contínua e a eficácia das atividades de resposta a incidentes.

Este processo envolve a análise detalhada dos dados de desempenho e feedbacks coletados, a identificação de áreas de melhoria e a implementação de mudanças nos processos de gestão de incidentes.

As atividades incluem a realização de análises pós-incidente, a revisão das políticas e procedimentos existentes, a identificação de melhores práticas e a integração das lições aprendidas nos processos atualizados.

A documentação das mudanças e a comunicação eficaz com todas as partes interessadas são essenciais para garantir que as melhorias sejam compreendidas e implementadas de maneira eficiente.

Este processo assegura que as atividades de gestão de incidentes continuem a

proporcionar valor significativo à organização, permitindo uma resposta proativa e eficaz a eventos futuros.

- PDCA focus: Act
- Periodicidade: Trimestral

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Evaluate Incident Performance	Avaliar o desempenho das atividades de gestão de incidentes.	Dados de desempenho, feedback dos stakeholders	Relatório de avaliação	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Solution Engineering & Development; Informed: IT Governance & Transformation	Decider: IT Infrastructure & Operation; Advisor: Solution Engineering & Development; Recommender: IT Governance & Transformation; Executer: IT Infrastructure & Operation
2	Identify Improvement Areas	Identificar áreas de melhoria com base na avaliação dos resultados.	Relatório de avaliação, feedback dos stakeholders	Lista de áreas de melhoria	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Architecture & Technology Visioning; Informed: Cybersecurity	Decider: IT Infrastructure & Operation; Advisor: Architecture & Technology Visioning; Recommender: Cybersecurity; Executer: IT Infrastructure & Operation

3	Update Incident Processes	Atualizar os processos de gestão de incidentes para incorporar as melhorias identificadas.	Lista de áreas de melhoria, melhores práticas	Processos de incidentes atualizados	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Data, AI & New Technology; Informed: Solution Engineering & Development	Decider: IT Infrastructure & Operation; Advisor: Data, AI & New Technology; Recommender: Solution Engineering & Development; Executer: IT Infrastructure & Operation
4	Document Changes	Documentar as mudanças nos processos de gestão de incidentes.	Processos de incidentes atualizados, feedback dos stakeholders	Documentação de mudanças	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Cybersecurity; Informed: IT Governance & Transformation	Decider: IT Infrastructure & Operation; Advisor: Cybersecurity; Recommender: IT Governance & Transformation; Executer: IT Infrastructure & Operation
5	Communicate Updates	Comunicar as atualizações dos processos aos stakeholders relevantes.	Documentação de mudanças, plano de comunicação	Comunicação de atualizações	Responsible: IT Infrastructure & Operation; Accountable: IT Infrastructure & Operation; Consulted: Architecture & Technology Visioning; Informed: Cybersecurity	Decider: IT Infrastructure & Operation; Advisor: Architecture & Technology Visioning; Recommender: Cybersecurity; Executer: IT Infrastructure & Operation