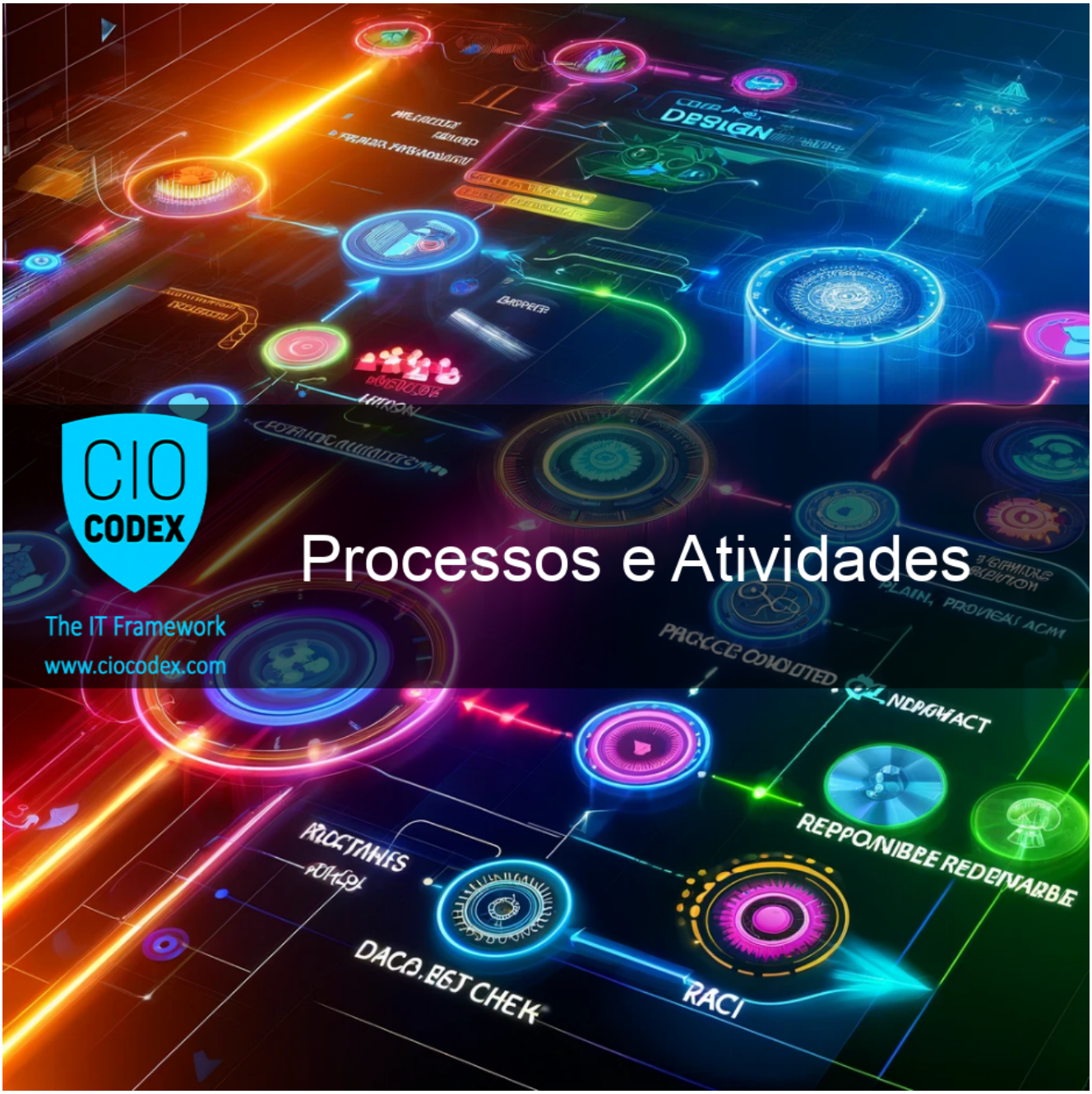
Processos e Atividades



Develop Risk Management Strategy

Desenvolver uma estratégia de gestão de riscos para TI alinhada com os objetivos do negócio é fundamental para identificar, analisar e mitigar os riscos que possam

impactar as operações de TI.

Este processo envolve a definição de uma abordagem sistemática para identificar ameaças potenciais, avaliar suas probabilidades e impactos, e implementar controles eficazes.

A estratégia deve considerar as melhores práticas de mercado e estar alinhada com a estratégia corporativa, garantindo que os riscos de TI sejam gerenciados de maneira integrada.

A comunicação da estratégia para todas as partes interessadas é crucial para assegurar o engajamento e a adesão aos processos de gestão de riscos estabelecidos.

- PDCA focus: Plan
- Periodicidade: Anual

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Assess Risk Landscape	Avaliar o panorama de riscos relevantes para a organização.	Informações de risco, benchmarks	Relatório de avaliação de riscos	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: Cybersecurity; Informed: All areas	Decider: IT Governance & Transformation; Advisor: Cybersecurity; Recommender: Architecture & Technology Visioning; Executer: IT Governance & Transformation

2	Define Risk Objectives	Definir os objetivos de gestão de riscos alinhados com os objetivos do negócio.	Feedback de stakeholders, análise de riscos	Objetivos de gestão de riscos definidos	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: All areas; Recommender: Solution Engineering & Development; Executer: IT Governance & Transformation
3	Develop Risk Policies	Desenvolver políticas de gestão de riscos detalhadas e alinhadas com os objetivos definidos.	Objetivos de gestão de riscos, benchmark de políticas	Políticas de gestão de riscos desenvolvidas	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: All areas; Recommender: Data, AI & New Technology; Executer: IT Governance & Transformation
4	Establish Risk Framework	Estabelecer um framework de gestão de riscos que suporte a implementação das políticas.	Políticas de gestão de riscos, frameworks de referência	Framework de gestão de riscos estabelecido	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: All areas; Recommender: Architecture & Technology Visioning; Executer: IT Governance & Transformation

5	Communicate Risk Strategy	Comunicar a estratégia de gestão de riscos para todas as partes interessadas.	Framework de gestão de riscos, políticas de gestão de riscos	Estratégia de gestão de riscos comunicada	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: All areas; Recommender: Solution Engineering & Development; Executer: IT Governance & Transformation

Identify Potential Risks

Identificar os riscos potenciais que possam impactar a organização é um processo crítico para assegurar que todas as operações de TI estejam preparadas para mitigar ameaças.

Este processo envolve a realização de uma análise detalhada para identificar riscos em várias áreas, como segurança cibernética, operacionais, conformidade e tecnológicos.

A identificação de riscos inclui a coleta de dados através de entrevistas, workshops e revisões de documentação.

A colaboração com diferentes áreas internas e externas é fundamental para garantir uma visão abrangente dos riscos potenciais.

Os riscos identificados devem ser documentados e categorizados para facilitar a análise e priorização subsequente.

- PDCA focus: Plan
- Periodicidade: Anual

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE

1	Conduct Risk Assessments	Realizar avaliações de risco para identificar ameaças potenciais.	Dados de riscos, entrevistas	Relatório de avaliação de riscos	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: Cybersecurity; Informed: All areas	Decider: IT Governance & Transformation; Advisor: Cybersecurity; Recommender: Architecture & Technology Visioning; Executer: IT Governance & Transformation
2	Gather Risk Data	Coletar dados de risco de várias fontes, incluindo entrevistas e workshops.	Informações de risco, dados de entrevistas	Dados de risco coletados	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: All areas; Recommender: Solution Engineering & Development; Executer: IT Governance & Transformation
3	Analyze Risk Data	Analisar os dados coletados para identificar e categorizar riscos potenciais.	Dados de risco coletados	Análise de riscos realizada	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: All areas; Recommender: Data, AI & New Technology; Executer: IT Governance & Transformation

4	Document Identified Risks	Documentar os riscos identificados e categorizá-los para priorização.	Análise de riscos realizada	Riscos identificados documentados	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: All areas; Recommender: Architecture & Technology Visioning; Executer: IT Governance & Transformation
5	Communicate Identified Risks	Comunicar os riscos identificados para as partes interessadas relevantes.	Riscos identificados documentados	Riscos comunicados	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: All areas; Recommender: Solution Engineering & Development; Executer: IT Governance & Transformation

Implement Risk Mitigation Plans

Implementar planos de mitigação de riscos é crucial para minimizar os impactos negativos dos riscos identificados.

Este processo envolve a criação e execução de estratégias para reduzir a probabilidade de ocorrência e/ou o impacto dos riscos.

A implementação deve incluir a designação de responsáveis por cada plano de mitigação, a criação de processos claros para monitorar a eficácia das ações e a integração de tecnologias que facilitem a mitigação.

Além disso, a comunicação e o treinamento são fundamentais para garantir que todos os colaboradores compreendam suas responsabilidades e estejam preparados para executar os planos de mitigação quando necessário.

- PDCA focus: Do

- Periodicidade: Contínua

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Develop Mitigation Plans	Desenvolver planos detalhados de mitigação de riscos para os riscos identificados.	Riscos identificados, políticas de gestão de riscos	Planos de mitigação desenvolvidos	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: Cybersecurity; Recommender: Architecture & Technology Visioning; Executer: IT Governance & Transformation
2	Assign Mitigation Responsibilities	Designar responsáveis por cada aspecto dos planos de mitigação de riscos.	Planos de mitigação desenvolvidos	Responsáveis designados	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: All areas; Recommender: Solution Engineering & Development; Executer: IT Governance & Transformation
3	Implement Mitigation Actions	Implementar as ações de mitigação conforme os planos desenvolvidos.	Planos de mitigação, ferramentas de monitoramento	Ações de mitigação implementadas	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: Cybersecurity; Informed: All areas	Decider: IT Governance & Transformation; Advisor: Cybersecurity; Recommender: Data, AI & New Technology; Executer: IT Governance & Transformation

4	Monitor Mitigation Effectiveness	Monitorar a eficácia das ações de mitigação implementadas.	Ações de mitigação implementadas	Relatórios de eficácia de mitigação	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: Cybersecurity; Informed: All areas	Decider: IT Governance & Transformation; Advisor: Cybersecurity; Recommender: Architecture & Technology Visioning; Executer: IT Governance & Transformation
5	Communicate Mitigation Status	Comunicar o status das ações de mitigação para as partes interessadas.	Relatórios de eficácia de mitigação	Status de mitigação comunicado	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: All areas; Recommender: Solution Engineering & Development; Executer: IT Governance & Transformation

Monitor Risk Management Performance

Monitorar continuamente o desempenho da gestão de riscos utilizando indicadores-chave de desempenho (KPIs) é essencial para assegurar que as estratégias e ações de mitigação sejam eficazes.

Este processo inclui a coleta e análise de dados de desempenho, a revisão de incidentes de risco e a avaliação contínua dos controles de risco implementados.

O uso de KPIs permite uma avaliação objetiva e mensurável do sucesso das estratégias de gestão de riscos.

A comunicação dos resultados para as partes interessadas e a revisão periódica dos KPIs garantem que as ações corretivas possam ser tomadas rapidamente para manter a eficácia do programa de gestão de riscos.

- PDCA focus: Check
- Periodicidade: Trimestral

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Define Risk KPIs	Definir indicadores-chave de desempenho para monitorar a gestão de riscos.	Objetivos de gestão de riscos, benchmarks	KPIs definidos	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: Cybersecurity; Informed: All areas	Decider: IT Governance & Transformation; Advisor: Cybersecurity; Recommender: Architecture & Technology Visioning; Executer: IT Governance & Transformation
2	Collect Risk Data	Coletar dados de desempenho relacionados aos riscos.	Ferramentas de monitoramento, relatórios de riscos	Dados de risco coletados	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: Cybersecurity; Recommender: Solution Engineering & Development; Executer: IT Governance & Transformation
3	Analyze Risk Performance	Analisar os dados coletados para avaliar a eficácia da gestão de riscos.	Dados de risco coletados	Análise de desempenho de riscos	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: Cybersecurity; Recommender: Data, AI & New Technology; Executer: IT Governance & Transformation

4	Review Risk Incidents	Revisar incidentes de risco ocorridos e sua gestão.	Dados de risco, relatórios de incidentes	Relatório de revisão de incidentes	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: Cybersecurity; Informed: All areas	Decider: IT Governance & Transformation; Advisor: Cybersecurity; Recommender: Architecture & Technology Visioning; Executer: IT Governance & Transformation
5	Report Risk Performance	Relatar o desempenho da gestão de riscos para as partes interessadas.	Análise de desempenho de riscos	Relatório de desempenho de riscos	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: All areas; Recommender: Solution Engineering & Development; Executer: IT Governance & Transformation

Review and Improve Risk Management Processes

Revisar e melhorar continuamente os processos de gestão de riscos com base nos resultados obtidos e feedbacks recebidos é essencial para assegurar que a organização se mantenha resiliente frente a novos desafios.

Este processo envolve a análise dos resultados das auditorias, a identificação de oportunidades de melhoria, e a implementação de ajustes necessários nos processos e controles de riscos.

A revisão deve considerar as melhores práticas do mercado e as lições aprendidas de ciclos anteriores para garantir que os processos estejam atualizados e eficazes.

A comunicação das melhorias implementadas é crucial para garantir a adesão e o entendimento por parte de todas as partes interessadas.

- PDCA focus: Act

- Periodicidade: Semestral

#	Nome da Atividade	Descrição	Inputs	Outputs	RACI	DARE
1	Evaluate Risk Management Results	Avaliar os resultados da gestão de riscos com base em auditorias e KPIs.	Relatórios de auditoria, KPIs	Relatório de avaliação de riscos	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: Cybersecurity; Informed: All areas	Decider: IT Governance & Transformation; Advisor: Cybersecurity; Recommender: Architecture & Technology Visioning; Executer: IT Governance & Transformation
2	Identify Improvement Areas	Identificar áreas de melhoria nos processos de gestão de riscos.	Relatório de avaliação de riscos	Áreas de melhoria identificadas	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: Cybersecurity; Recommender: Solution Engineering & Development; Executer: IT Governance & Transformation
3	Develop Improvement Plan	Desenvolver um plano detalhado para melhorar os processos de gestão de riscos.	Áreas de melhoria identificadas	Plano de melhoria desenvolvido	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: Cybersecurity; Recommender: Data, AI & New Technology; Executer: IT Governance & Transformation

4	Implement Process Improvements	Implementar as melhorias conforme o plano desenvolvido.	Plano de melhoria desenvolvido	Melhorias implementadas	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: Cybersecurity; Recommender: Architecture & Technology Visioning; Executer: IT Governance & Transformation
5	Communicate Process Updates	Comunicar as atualizações dos processos de gestão de riscos para as partes interessadas.	Melhorias implementadas	Atualizações comunicadas	Responsible: IT Governance & Transformation; Accountable: IT Governance & Transformation; Consulted: All areas; Informed: All areas	Decider: IT Governance & Transformation; Advisor: All areas; Recommender: Solution Engineering & Development; Executer: IT Governance & Transformation

CIO Codex

Com o advento da era digital, a Tecnologia da Informação assumiu um papel de destaque dentro das estratégias corporativas das empresas dos mais diversos portes e setores de atuação. O CIO Codex Framework foi concebido com o propósito de oferecer uma visão integrada dos conceitos de uma área de tecnologia pronta para a era digital.