

Propósito e Objetivos



The IT Framework
www.ciocodex.com

Propósito e Objetivos

A IT Risk Management desempenha um papel fundamental na governança de TI, concentrando-se na identificação, análise e mitigação de riscos associados às operações de Tecnologia da Informação.

Seu propósito central é assegurar que as ameaças sejam identificadas e tratadas de forma proativa, minimizando o impacto negativo nas operações de TI e, conseqüentemente, na organização como um todo.

Objetivos

Dentro do contexto do CIO Codex Capability Framework, os objetivos da IT Risk Management são:

- **Identificar Riscos de TI:** Realizar uma análise detalhada para identificar os diversos tipos de riscos que podem afetar as operações de TI, tais como riscos de segurança cibernética, riscos operacionais e riscos de conformidade.
- **Avaliar a Severidade e Probabilidade:** Avaliar a gravidade potencial e a probabilidade de ocorrência de cada risco identificado, atribuindo uma classificação que orienta o tratamento adequado.
- **Mitigar Riscos:** Desenvolver e implementar estratégias de mitigação de riscos, que podem incluir a definição de controles de segurança, processos de contingência e planos de resposta a incidentes.
- **Monitorar e Relatar Riscos:** Estabelecer um sistema contínuo de monitoramento de riscos e incidentes, bem como relatórios regulares para a alta administração e partes interessadas.
- **Integrar a Gestão de Riscos:** Integre a gestão de riscos de TI com a gestão de riscos corporativos, garantindo que os riscos de TI estejam alinhados com os objetivos estratégicos da organização.

Impacto na Tecnologia

A IT Risk Management influencia diversas dimensões da tecnologia:

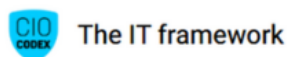
- **Infraestrutura:** Influencia a seleção de infraestrutura de segurança, como firewalls, sistemas de detecção de intrusão e sistemas de prevenção de ameaças, para mitigar os riscos de segurança cibernética.

- **Arquitetura:** Define padrões de arquitetura que incorporam medidas de segurança e resiliência para proteger a infraestrutura contra ameaças e vulnerabilidades.
- **Sistemas:** Inclui a implementação de sistemas de monitoramento de segurança e a definição de políticas de acesso para proteger os sistemas contra ameaças internas e externas.
- **Modelo Operacional:** Define processos de gerenciamento de incidentes, planos de continuidade de negócios e práticas de resposta a incidentes para manter a continuidade das operações de TI em caso de ameaças.
- **Cybersecurity:** A gestão de riscos avalia e prioriza ameaças, permitindo a alocação eficaz de recursos de segurança.



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.



O conteúdo apresentado neste website, incluindo o framework, é protegido por direitos autorais e é de propriedade exclusiva do CIO Codex. Isso inclui, mas não se limita a, textos, gráficos, marcas, logotipos, imagens, vídeos e demais materiais disponíveis no site. Qualquer reprodução, distribuição, ou utilização não autorizada desse conteúdo é estritamente proibida e sujeita às penalidades previstas na legislação aplicável