

Estrutura de Funções e Responsabilidades de Governança (EFRG)

"Este documento é uma versão simplificada para fins de demonstração de portfólio técnico, focando na estrutura estratégica e alinhamento com os frameworks COBIT e ISO."

Nome da empresa: Apex Financial Solutions

Tipo de documento: Estrutura de Funções e
Responsabilidades de Governança (EFRG)

Framework de Referência: COBIT 2019 (Domínio
EDM - Avaliar, Dirigir e Monitorar)

Versão: 1.0

Data de vigência: 01/01/2026

■ Objetivo

Definir a estrutura de liderança e os comitês necessários para garantir que a TI seja dirigida e monitorada pela alta administração, garantindo a prestação de contas (accountability).



O Comitê Diretor de TI (IT Steering Committee)

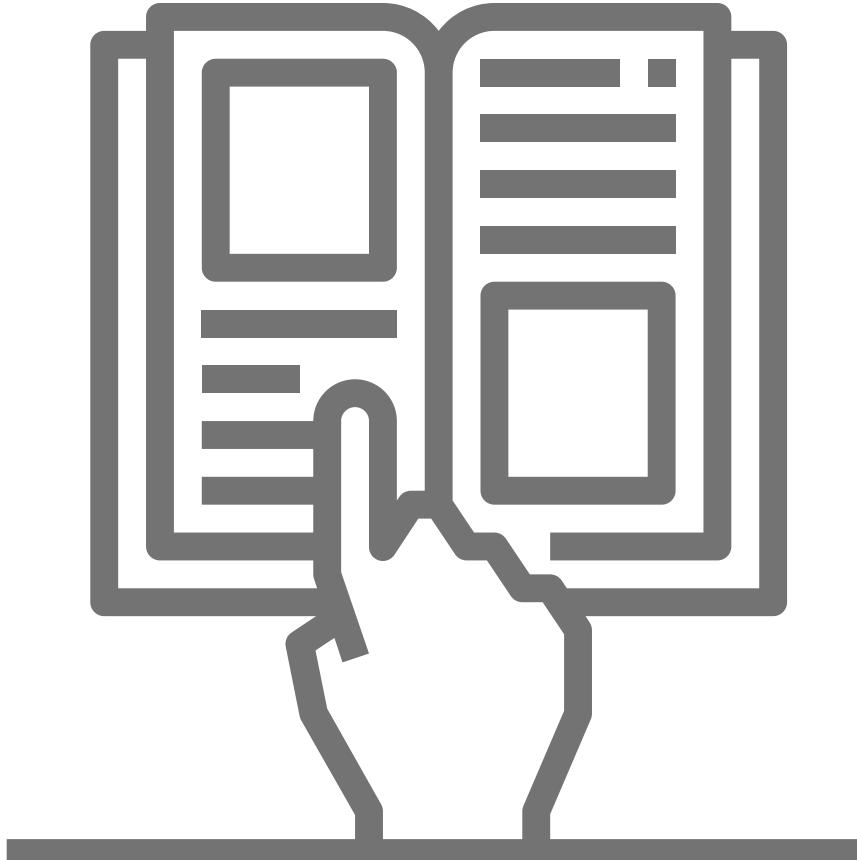
Este é o órgão máximo de decisão para tecnologia na organização.

Composição: CEO (Presidente), CFO, CTO e CISO.

Periodicidade: Reuniões trimestrais.

Responsabilidades:

- Aprovar o Plano Estratégico de TI (PETI).
- Priorizar investimentos em projetos de transformação digital.
- Avaliar se a TI está entregando os benefícios esperados para o negócio.



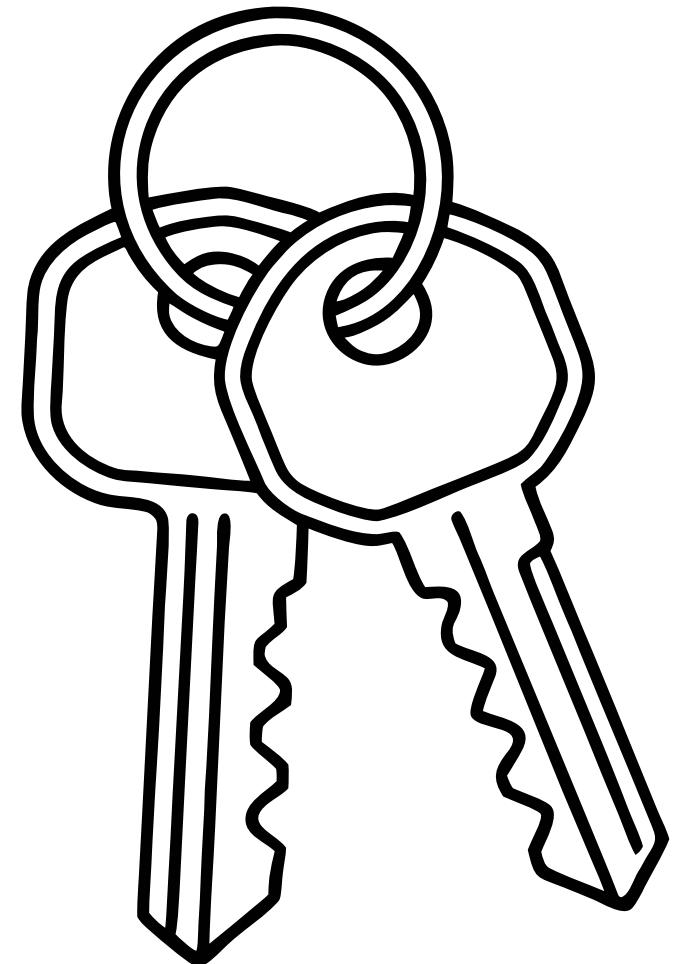
Papéis Chave de Governança

Board Executivo: Responsável por definir o apetite ao risco e garantir o financiamento da estratégia.

CTO (Chief Technology Officer): Garante a entrega dos serviços e a arquitetura tecnológica.

CISO (Chief Information Security Officer): Garante que a segurança e a governança de dados estejam integradas a todos os projetos.

Gestor de Mudanças (Change Manager): Garante que alterações em sistemas não causem impactos negativos na operação.



Fluxo de Decisão (Escalonamento)

Nível Operacional: Decisões diárias e gestão de incidentes simples.

Nível Tático: Decisões sobre infraestrutura e projetos de médio prazo (Liderança de TI).

Nível Estratégico: Mudanças de plataforma, grandes orçamentos e riscos críticos (Comitê Diretor).



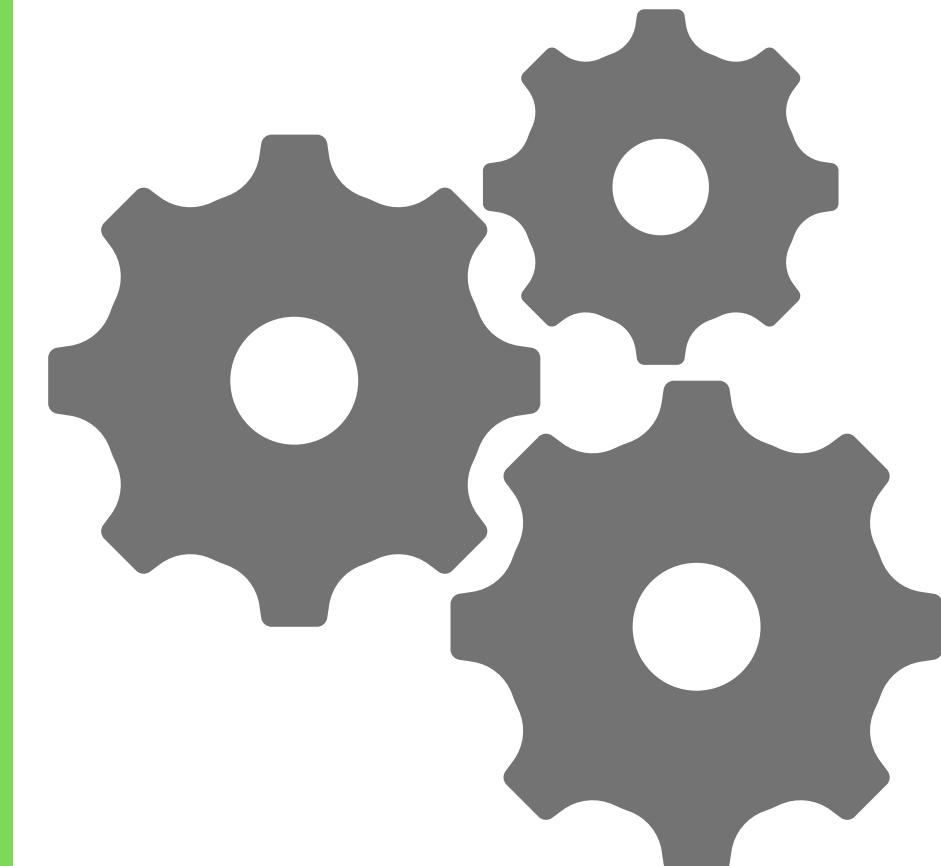
Mecanismos de Prestação de Contas

A Apex adota o modelo de "**Três Linhas de Defesa**":

Gestão Operacional: Gerentes de TI que executam os controles.

Funções de Risco e Compliance (CISO/GRC):
Monitoram a eficácia dos controles.

Auditoria Interna: Avaliação independente de todo o sistema de governança.



■ Isenção de responsabilidade

Este documento representa um caso fictício desenvolvido para fins profissionais e educacionais e não reflete nenhuma organização real.

