

## Governança de TI

O termo "Governança de TI" tem suas origens no conceito de "Governança Corporativa", mas não devemos confundir esses conceitos. Além disso, a "Governança de TI" relaciona-se com a "Gestão/gerenciamento de TI", porém não são a mesma coisa. Para melhor entendermos as semelhanças, as diferenças e o inter-relacionamento do significado desses termos, seguem algumas definições.

### Governança Corporativa

Segundo o Instituto Brasileiro de Governança Corporativa (IBGC):

"Governança Corporativa é o sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre proprietários, Conselho de Administração, Diretoria e órgãos de controle. As boas práticas de Governança Corporativa convertem princípios em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor da organização, facilitando seu acesso a recursos e contribuindo para sua longevidade."

### Sistema de Governança Corporativa



Para o Ministro Aroldo Cedraz, "Governança de TI é o conjunto estruturado de políticas, normas, métodos e procedimentos destinados a permitir à alta administração e aos executivos o planejamento, a direção e o controle da utilização atual e futura de tecnologia da informação, de modo a assegurar, a um nível aceitável de risco, eficiente utilização de recursos, apoio aos processos da organização e alinhamento estratégico com objetivos desta última. Seu objetivo, pois, é garantir que o uso da TI agregue valor ao negócio da organização." (Voto do Ministro Relator – Acórdão 2.308/2010 – Plenário)

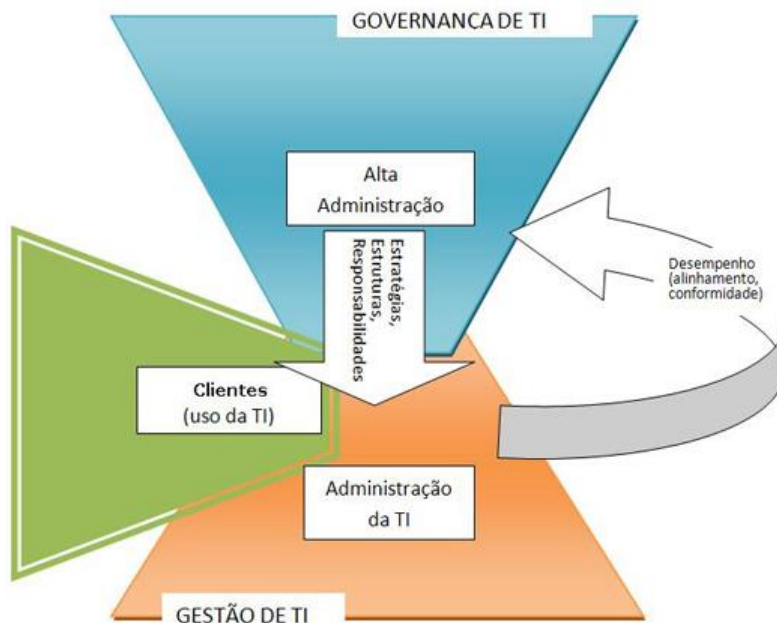
Para o Information Technology Governance Institute (ITGI), "governança de TI é de responsabilidade dos executivos e da alta direção, consistindo em aspectos de liderança, estrutura organizacional e processos que garantam que a área de TI da organização suporte e aprimore os objetivos e as estratégias da organização."

Observa-se, portanto, que a "Governança Corporativa" tem foco no direcionamento e monitoramento da gestão da instituição, e busca permitir a intervenção dos responsáveis finais sempre que houver desvio em relação ao esperado. Em última instância, esses responsáveis são os detentores da propriedade: sócios e acionistas, no caso das organizações privadas, e a sociedade, no caso das organizações públicas federais.

Já a "Governança de TI" tem foco no direcionamento e monitoramento das práticas de gestão e uso da TI de uma organização, tendo como indutor e principal beneficiário a alta administração da instituição.

Um exemplo prático de mecanismo de governança de TI é o estabelecimento de um processo transparente de tomada de decisão sobre a priorização de grandes demandas de TI. Tal processo é necessário para garantir que as ações de TI estejam alinhadas com os objetivos institucionais e para

garantir que as demandas que tenham maior impacto nesses objetivos tenham atendimento prioritário. Esta é uma decisão que não cabe às unidades de TI (embora devam sempre opinar). Portanto, o estabelecimento desse processo, os participantes e suas competências é uma iniciativa de governança de TI a ser liderada pela alta administração.



Conjunto de processos realizados pelas unidades provedoras de TI, visando ao planejamento e à realização das atividades necessárias ao provimento ou entrega de soluções e serviços de TI.

Relação entre os conceitos

Do que vimos, pode-se pensar, erroneamente, que a Governança Corporativa não tem relação com a Governança de TI e que esta não tem relação com a Gestão/Gerenciamento de TI.

Entretanto, o que de fato ocorre é uma dependência entre elas, tal como mostrado na figura abaixo. O gerenciamento de serviços de TI é, de fato, um enabler (facilitador) da governança de TI e esta é um facilitador da governança corporativa. Em resumo, uma organização que faça uso intenso de TI (situação comum, atualmente), não pode afirmar ter uma boa governança corporativa sem ter boa governança de TI. Igualmente, a instituição não pode afirmar ter uma boa governança de TI sem ter um bom gerenciamento de (serviços) de TI. A figura abaixo ilustra essa interdependência.



### Áreas De Foco Da Governança De TI

Na prática, a Governança de TI se traduz em um conjunto de políticas, processos, papéis e responsabilidades associados a estruturas e pessoas da organização, de modo a se estabelecer claramente o processo de tomada de decisões e as diretrizes para o gerenciamento e uso da TI, tudo isso de forma alinhada com a visão, missão e metas estratégicas da organização.

A figura abaixo resume as principais dimensões focalizadas pela Governança de TI.

Áreas de foco da Governança de TI Na prática, a Governança de TI se traduz em um conjunto de políticas, processos, papéis e responsabilidades associados a estruturas e pessoas da organização, de modo a se estabelecer claramente o processo de tomada de decisões e as diretrizes para o gerenciamento e uso da TI, tudo isso de forma alinhada com a visão, missão e metas estratégicas da organização. A figura abaixo resume as principais dimensões focalizadas pela Governança de TI.



**Alinhamento Estratégico** - assegura o alinhamento dos planos da TI com os de negócio e alinha a operação e as entregas da TI com as operações da organização.

**Entrega de Valor** – assegura que os benefícios previstos pela TI estão realmente sendo gerados, dentre eles a otimização de custos e outros valores intrínsecos que a TI pode proporcionar.

**Gestão de Riscos** – Permite que a organização reconheça todos os riscos (e oportunidades) derivados da TI para o negócio e que decida e tenha planos para mitigá-los na medida que julgue necessário.

**Gestão de Recursos** – assegura a gestão dos recursos mais importantes para TI: recursos humanos e recursos tecnológicos (informações, infraestrutura, aplicações). Promove a valorização do conhecimento e da infraestrutura.

**Mensuração de Desempenho** – acompanha e monitora a implementação da estratégia, consumação de projetos, uso dos recursos e entrega dos serviços quanto à sua contribuição para as estratégias e objetivos do negócio, utilizando-se não apenas de critérios financeiros. Resumindo tudo em uma figura:



### Importância De Se Aplicar Governança De TI No TCU

O TCU é uma instituição que depende de informação para a realização de seus trabalhos, e cada vez mais da Tecnologia da Informação (TI) para adequadamente tratar, analisar, fazer uso, disseminar e proteger essas informações. Além disso, é cada vez maior a automação de processos de trabalho do Tribunal, como meio de se assegurar o alcance e a manutenção de padrões de desempenho e qualidade compatíveis com as necessidades da sociedade brasileira.

Entretanto, não é suficiente simplesmente reconhecer a importância da TI e aplicar recursos e esforços em tais iniciativas. No mercado, são incontáveis os exemplos de projetos de TI que fracassaram pela falta ou imaturidade dos mecanismos de governança de TI.

Organizações bem-sucedidas reconhecem os benefícios da tecnologia da informação e a utilizam para adicionar valor ao negócio, valendo-se de mecanismos de governança de TI adequados às estratégias institucionais.

### **Compreendendo Os Principais Conceitos Do COBIT 5**

O COBIT 5 é a mais recente versão do framework de boas práticas de governança e gerenciamento empresarial de TI, que incorpora muitos conceitos e teorias amplamente aceitos.

Nesta série de artigos, vamos explorar os princípios fundamentais do framework, servindo como uma referência para a aplicação do COBIT 5 em sua organização. Acompanhe!

### **A Governança Empresarial De TI E O COBIT 5**

Informação (no sentido mais abrangente da palavra) e tecnologias relacionadas estão se tornando fatores cruciais na sustentabilidade, crescimento e gerenciamento do valor e risco na maioria das empresas. Como resultado, a TI deixou de atuar simplesmente no papel de suporte e passou a assumir uma posição central dentro das empresas.

O papel realçado da TI na criação de valor e gerenciamento de risco empresarial veio acompanhado por uma crescente ênfase na Governança e Gerenciamento Empresarial de TI. Os stakeholders anseiam por assegurar que a TI cumpra as metas empresariais.

A Governança e Gerenciamento Empresarial de TI é parte integral de todo o meio corporativo. Ela endereça a definição e implementação de processos, estruturas e mecanismos relacionais dentro da empresa, que permitem ao pessoal de negócio e da TI executar suas responsabilidades para suportar a criação e sustentabilidade do valor ao negócio.

A Governança e Gerenciamento Empresarial de TI é complexa e multifacetada. Membros do comitê de governança e a alta direção tipicamente precisam de assistência para implementá-la. Através dos anos, frameworks de boas práticas foram desenvolvidos e promovidos para auxiliar neste processo.

Lançado em 2012, o COBIT 5 foi construído e integrado com base em 20 anos de desenvolvimento neste campo de atuação. Desde os seus primórdios, centrado na comunidade de auditoria de TI, o COBIT se tornou um framework de Governança e Gerenciamento de TI mais abrangente, compreensivo e aceito.

O COBIT 5 foi adicionalmente complementado com os frameworks Val IT e Risk IT. Antes do COBIT 5, o Val IT endereçava processos de negócio e responsabilidades na criação de valor empresarial e o Risk IT fornecia uma visão de negócio holística sobre o gerenciamento de riscos. Agora, ambos estão incorporados ao COBIT 5.

O framework COBIT 5 é construído em torno de cinco princípios fundamentais:

Satisfazer necessidades das partes interessadas;

Cobrir a organização de ponta a ponta;

Aplicar um framework integrado e único;

Possibilitar uma visão holística;

Separar Governança do Gerenciamento.

### **Entendendo Os Principais Conceitos Do COBIT**

As boas práticas em destaque na ITIL são tão importantes que viraram um padrão de fato no mundo da TI. Seus fundamentos são usados nos níveis táticos e operacionais, possibilitando que o setor da

Tecnologia da Informação estrutura o ciclo vital de seus serviços de modo geral, a fim de buscar excelência operacional.

No caso do framework do COBIT, tem foco na área estratégica e — por se tratar de um framework voltado para o controle — permite que a TI consiga seu desempenho mensurado e seus riscos devidamente apontados e consertados.

Estudando o framework do COBIT com ampla profundidade, torna-se possível saber que ele aponta os objetivos de controle. Porém, percebe-se que não existe detalhamento de como os processos podem ser definidos.

O COBIT 5 não é um padrão, ele não é um regramento como a ISO 9.001, ISO 20.000 ou ISO 17.799. Ressalta-se que ele não serve também como meio para ampliar as vantagens da TI. Em vez disso, o COBIT auxilia o direcionamento ou a priorização dos recursos e esforços da TI para atender aos requisitos do negócio.

O uso do COBIT não tem como objetivo ter o controle de todos os processos. Sua meta é apenas identificar e compreender quais são os processos da TI que estão gerando um impacto, ou ocasionando possíveis riscos para o negócio, de forma a dar prioridade à gestão desses processos.

O framework de controle do COBIT argumenta que não é possível administrar aquilo que não se mede. Posto isso, ele apresenta uma sequência de metas de controle e seus respectivos indicadores de desempenho.

### **Missão**

O objetivo deve ser a pesquisa, o desenvolvimento, a publicação e a promoção de um conjunto de metas de controle para tecnologia que seja apoiado e admitido em geral para o uso do dia a dia de administradores de negócio e auditores.

### **Comparação**

O framework do COBIT foi produzido tendo como fundamentais aspectos a base do negócio, a orientação a métodos, além de ser apoiado em controles e conduzido por métricas.

Optar pelo COBIT auxilia um empreendimento a colocar em prática boas maneiras de governança de TI, uma vez que ele fornece um guia de melhores métodos e direcionamento.

Sua sustentação classifica os processos em 4 comandos, e apresenta ações em uma estrutura gerenciável e lógica.

Vários modelos, referências e guias de boas práticas podem ser escolhidos para moldar um modelo de governança de TI para as empresas. Cabe aos executivos constatar qual é o modelo ideal para cumprir com as necessidades de negócio de suas empresas, mas é notório que a regulamentação externa (SOX/Basileia II) direciona fortemente a opção do COBIT em seus métodos de governança de TI.

Uma questão bastante significativa é o que o COBIT — devido ao fato de ser um framework de controle de nível altíssimo — indica o que precisa ser controlado, mas não diz a maneira como isso deve ser feito. Ele se encaixa muito bem com os melhores métodos para gestão de serviços de TI descritos na IT(Infrastructure Library -ITIL), que possui foco mais específico e operacional no tocante aos processos internos de TI.

Os frameworks do COBIT e do ITIL se acrescentam e cobrem uma boa área dos aspectos da organização da TI, de modo que, quando as práticas acertadas em cada modelo são adotadas pelas empresas de TI, em seus processos íntimos, o perigo operacional de TI é diminuído de forma significativa. Tudo isso tem o objetivo de fazer com que a TI se torne um aliado estratégico para que os empreendimentos consigam alcançar seus objetivos de negócio.

A Tecnologia da Informação é moderadamente nova se comparada à Medicina, Engenharia, Arquitetura ou Advocacia. Contudo, a reunião de boas práticas vem passando por um ciclo de melhoria contínua cujos resultados positivos são comprovados pelo mercado há pelo menos 10 anos.

Como dito previamente, o framework de controle do COBIT parte da ideia inicial de que não é possível administrar aquilo que não se mede. Diante disso, ele propõe uma série de metas de gestão e seus respectivos indicadores de desempenho.

O modelo também leva em conta que a TI precisa entregar a informação que o empreendimento precisa para atingir os seus objetivos de negócio. Além disso, o COBIT é harmonizável com outros padrões de mercado, visto que ele se posiciona em um nível geral, abrangendo diversos processos de TI, definindo as metas de cada um dos processos e como elas devem ser utilizadas.

O COBIT não mira em como cada processo deve ser executado, sendo exatamente esse o motivo que o torna adaptável a outros modelos existentes.

#### Características

O framework do COBIT foi criado tendo como qualidades fundamentais:

A orientação a processos;

A meta no negócio;

Ser direcionado por métricas;

Ser baseado em controles.

#### Objetivos

Abaixo podemos ver o que o COBIT possui como metas:

Colocar as melhores práticas a partir de uma matriz de atividades, domínios e processos organizados de modo lógico e gerenciável;

Ser um padrão aprovado nas melhores práticas de governança de TI;

Ajudar na associação entre as necessidades de controle, aspectos tecnológicos e riscos do negócio.

Optar pelo COBIT como forma de governança é vantajoso por:

Auxiliar a compreender os requisitos regulatórios;

Ser conciliável tanto com o COSO quanto ao controle do ambiente de TI;

Ser focado nos requisitos de negócio;

Determinar uma linguagem comum entre TI e o negócio;

Ser aceito internacionalmente como framework de modelo para Governança de TI;

Ser suportado por treinamentos e ferramentas;

Mapear os melhores padrões e frameworks de mercado, como o ISO 20.000, ISO 27.001 e ITIL.

Ser orientado a processos;

Estar em crescimento contínuo.

#### O Cubo do COBIT

Como todas as peças do COBIT estão organizados em conjunto, a figura do cubo é usada para abreviar que os recursos de TI são administrados pelos processos de TI. Eles visam conseguir metas que correspondam aos requisitos do negócio. Esse é o princípio vital do framework do COBIT.

No tocante à similaridade com o ITIL, o COBIT resguarda grande parte dos processos ITIL, tanto na opção 2 quanto na opção 3. No entanto, o ITIL possui os processos demonstrados com maior nível de detalhamento.



De modo geral, enquanto o ITIL está mais focado em “como”, o COBIT foca no “o que”. Dessa forma, podemos dizer que o COBIT é um framework de controle que estabelece o que tem que ser realizado, mas não diz como proceder.

### **ISO/IEC 38500**

Esta Norma oferece princípios para orientar os dirigentes das organizações (incluindo proprietários, diretores, parceiros, executivos ou similares) sobre o uso eficaz, eficiente e aceitável da Tecnologia de Informação (TI) dentro de suas organizações.

Aplica-se a organizações de todos os tamanhos (pequenas a grandes), independentemente da extensão de seus usos de TI.

A norma ISO/IEC 38500:2008 define seis princípios para a boa governança de TI:

**Responsabilidade:** Os indivíduos e grupos na organização devem compreender e aceitar as suas responsabilidades no fornecimento de TI. Os indivíduos responsáveis por ações devem ter a autoridade para as desempenharem.

**Estratégia:** A estratégia de negócio da organização tem em conta as capacidades de TI atuais e futuras; os planos estratégicos para as TI satisfazem as necessidades atuais e contínuas da estratégia de negócio da organização.

**Aquisições:** As aquisições de TI são feitas por razões válidas, com base e análise apropriada com decisões claras e transparentes. Há um equilíbrio adequado entre os benefícios, oportunidades, custos e riscos, tanto no curto como no longo prazo.

**Desempenho:** A TI é adequada à finalidade de suporte da organização, à disponibilização de serviços e quanto aos níveis e qualidade dos serviços necessários para responder aos requisitos atuais e futuros do negócio.

**Conformidade:** A TI encontra-se em conformidade com a legislação e regulamentos aplicáveis. As políticas e as práticas estão claramente definidas, encontram-se implementadas e são aplicadas.

**Comportamento Humano:** As políticas, práticas e decisões de TI revelam respeito pelo Comportamento Humano, incluindo as necessidades atuais e a evolução das necessidades de todas as “pessoas no processo”.

A norma preconiza que os dirigentes governem a TI através de três tarefas principais:

Avaliar o uso atual e futuro da TI.

Orientar a preparação e a implementação de planos e políticas para assegurar que o uso da TI atenda aos objetivos do negócio.

Monitorar o cumprimento das políticas e o desempenho em relação aos planos.

Se bem utilizada, a norma assegura que os dirigentes poderão avaliar os riscos da TI para o negócio e aproveitar as oportunidades advindas com o uso da TI.

### **Cobit**

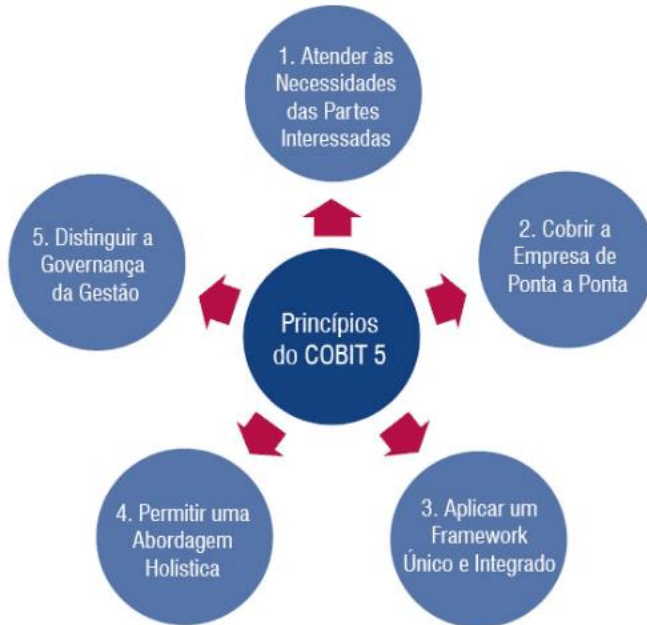
O que é COBIT?

O COBIT fornece um modelo abrangente que auxilia as organizações a atingirem seus objetivos de governança e gestão de TI.

Em termos simples, O COBIT 5 ajuda as organizações a criar valor por meio da TI mantendo o equilíbrio entre a realização de benefícios, a otimização dos níveis de risco e de utilização dos recursos. O COBIT permite que a TI seja governada e gerida de forma holística para toda a organização, abrangendo o negócio de ponta a ponta bem como todas as áreas responsáveis pelas funções de TI, levando em consideração os interesses internos e externos relacionados com TI.

O COBIT é genérico e útil para organizações de todos os portes, sejam comerciais, sem fins lucrativos ou públicas.

O COBIT baseia-se em cinco princípios básicos (demonstrados na figura) para governança e gestão de TI da organização:



### **Por que usar o COBIT 5?**

Novas exigências dos usuários, os regulamentos específicos do setor e cenários de risco surgem a cada dia. Maximizar o valor da propriedade intelectual, gestão do risco e segurança e assegurar a conformidade por meio de governança de TI nunca foi tão importante.

Nenhuma outra estrutura focada em TI corporativa oferece a amplitude ou benefícios do COBIT. Ele ajuda empresas de todos os tamanhos a:

Manter a informação de alta qualidade para apoiar decisões de negócios;

Atingir os objetivos estratégicos através da utilização eficaz e inovadora de TI;

Atingir a excelência operacional através da aplicação confiável, eficiente da tecnologia;

Manter riscos a um nível aceitável;

Otimizar o custo de serviços de TI e tecnologia;

Manter o cumprimento de leis, regulamentos, acordos contratuais e políticas.

O framework COBIT para a governança e gestão de TI empresarial é uma otimização de negócios que utiliza práticas comprovadas, liderança com pensamento global e ferramentas inovadoras para inspirar a inovação em TI e negócios de sucesso.

### **Certificações Relacionadas**

A ISACA oferece três níveis de certificação profissional, relacionados ao conhecimento e a proficiência na utilização do CobiT:

COBIT 5 Foundation: atesta que os profissionais certificados compreendem os problemas de governança e gestão da TI das empresas e sabem como utilizar o CobiT para enfrentar e solucionar esses desafios.



COBIT 5 Implementation: atesta que os profissionais certificados demonstraram conhecimento sobre como o CobiT 5 pode ser adaptado para atender as necessidades específicas de uma empresa, além de domínio da implementação da Governança Corporativa de TI com base em ciclo de melhoria contínua.

COBIT 5 Assessor: direcionado a auditores internos e externos e a consultores de TI, atesta que os profissionais certificados demonstraram domínio sobre como realizar uma avaliação de capacidade de processo formal e sobre como ela pode ser utilizada para habilitar metas de negócio, priorizar iniciativas de melhoria e identificar oportunidades de melhoria da governança e do gerenciamento dos ativos de informação e tecnologia.

[illegible]