

# **Disciplina: Governança em Tecnologia da Informação**

## **Aula 2: Gestão de desempenho em TI**

## Apresentação

Na aula anterior discutimos os conceitos básicos da governança corporativa e de TI, suas motivações, características e a necessidade de controlar as ações da organização. Nesta aula, vamos nos aprofundar nos conceitos de controle de TI e em como os indicadores podem auxiliar e alavancar as ações de governança.

Compreenderemos a importância da implementação de um sistema de medição, confirmando que em uma empresa só é possível gerenciar aquilo que se mede, só se mede aquilo que se define, e só se define aquilo que se compreende. Por isso, os indicadores são grandes aliados para a gestão da organização, pois eles medem a diferença entre a situação desejada pela gestão da organização, a meta e a situação atual, o resultado. Eles apontam o caminho, são um referencial para a gestão e fornecem uma base objetiva para identificar problemas, definem prioridades e identificam os esforços necessários para a melhoria da organização.

Analisaremos como a gestão de riscos auxilia a governança de TI e como utilizá-la em uma abordagem de balanceamento de custos e benefícios das ações de TI, auxiliando a organização na melhoria contínua de seus serviços e resultados. Por fim, abordaremos o conceito de compliance como uma ferramenta para aferição de conformidade da área de TI a regulamentos internos e externos.

---

## Objetivos

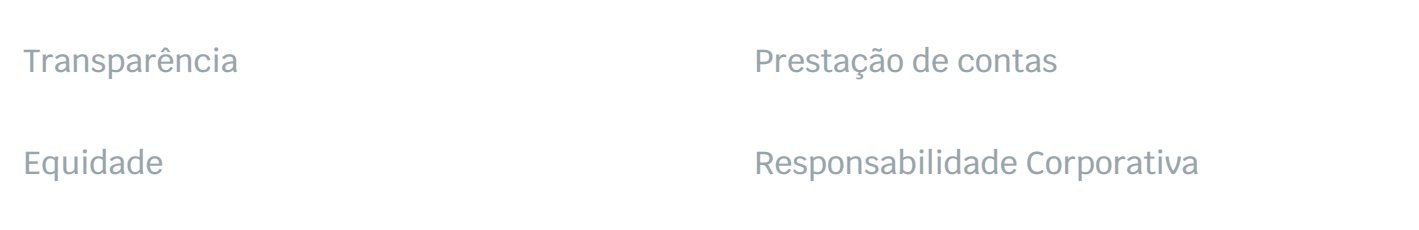
- Identificar a importância da gestão de desempenho da TI;
- Estabelecer a importância da implementação de controles e indicadores de TI;
- Identificar a importância da análise dos riscos e do compliance.

# Gestão de desempenho de TI

Na aula anterior, identificamos as ações que são a base da governança corporativa e que são utilizadas para detectar o cumprimento dos interesses de todos os envolvidos nas organizações:

 (Fonte: Shutterstock)

Analisamos, também, os princípios básicos da boa governança sendo o IBGC:



Entre esses princípios identificamos dois fundamentais e motivadores para a implementação da gestão de desempenho nas organizações:



Para garantir que esses princípios sejam efetivos, as organizações lançam mão de modelos de controle interno e gestão de risco.

## Vamos falar de controle?

O controle está relacionado diretamente com as demais funções do processo administrativo:



Todas as ações de TI independentemente se são resultados da prestação de serviços, de planos estratégicos ou de projetos, só podem ser gerenciadas se tiverem medições e indicadores.


**Atenção!** Aqui existe uma videoaula, acesso pelo conteúdo online

É possível mensurar qualquer atividade que gere números ou valores para a organização. A grande questão é descobrir quais são os indicadores mais importantes para o negócio e para a organização de forma a não perder tempo acompanhando os que são menos relevantes.

**Exemplos de controles de TI:**

- Administrativos e gerenciais
- Segurança e privacidadePreparação e captação de dados
- Entrada de dados
- Processamento
- Saída e de emissão de relatórios
- Gravação e recuperação de dados

A organização deverá adotar um sistema de medição que definirá o desempenho da empresa, baseado em um conjunto de indicadores previamente estabelecidos e que atendam à demanda do negócio.

 (Fonte: Shutterstock)

Medir é importante para que se entenda o que está acontecendo na gestão, quais mudanças devem ser feitas e quais foram os impactos das mudanças já realizadas. Com essas respostas, é possível acompanhar se as metas para a organização estão sendo alcançadas e medir qual a porcentagem de melhoria ou piora em relação às medições anteriores.

Existem diversos tipos de indicadores, cada qual com uma finalidade. Para definir indicadores que sejam relevantes para a área de TI, é necessário compreender qual é a função dessa área na organização e seu direcionamento estratégico. Exemplos de indicadores:

Rentabilidade	▼
Trata da relação entre o lucro e o investimento de uma empresa medido em percentual. Exemplo: Na empresa ABC foram investidos R\$1.000.000,00. Foi obtido um lucro de R\$60.000,00; neste caso, a rentabilidade foi de 6%.	
Capacidade	▼
Trata da relação entre a quantidade e o tempo de produção de uma determinada organização. Exemplo: A empresa ABC tem capacidade de produzir 300 produtos Y por mês.	
Produtividade	▼
Trata da relação entre o produto gerado por uma determinada tarefa e o recurso utilizado para sua execução. Exemplo: Um carpinteiro consegue produzir 30 peças em uma hora e outro profissional, no mesmo período, produz 10 peças.	
Lucratividade	▼
Trata da relação entre o lucro e as vendas totais de uma organização medido em percentual. Exemplo: A empresa ABC vendeu R\$600.000,00 em horas de consultoria e apurou um lucro de R\$60.000,00. Portanto a lucratividade foi de 10%.	
Qualidade	▼
Trata da relação entre todos os itens produzidos de um determinado produto e os itens deste mesmo produto que não apresentaram defeitos ou inconformidades. Exemplo: 4.900 peças adequadas a cada 5.000 produzidas (98% de conformidade).	

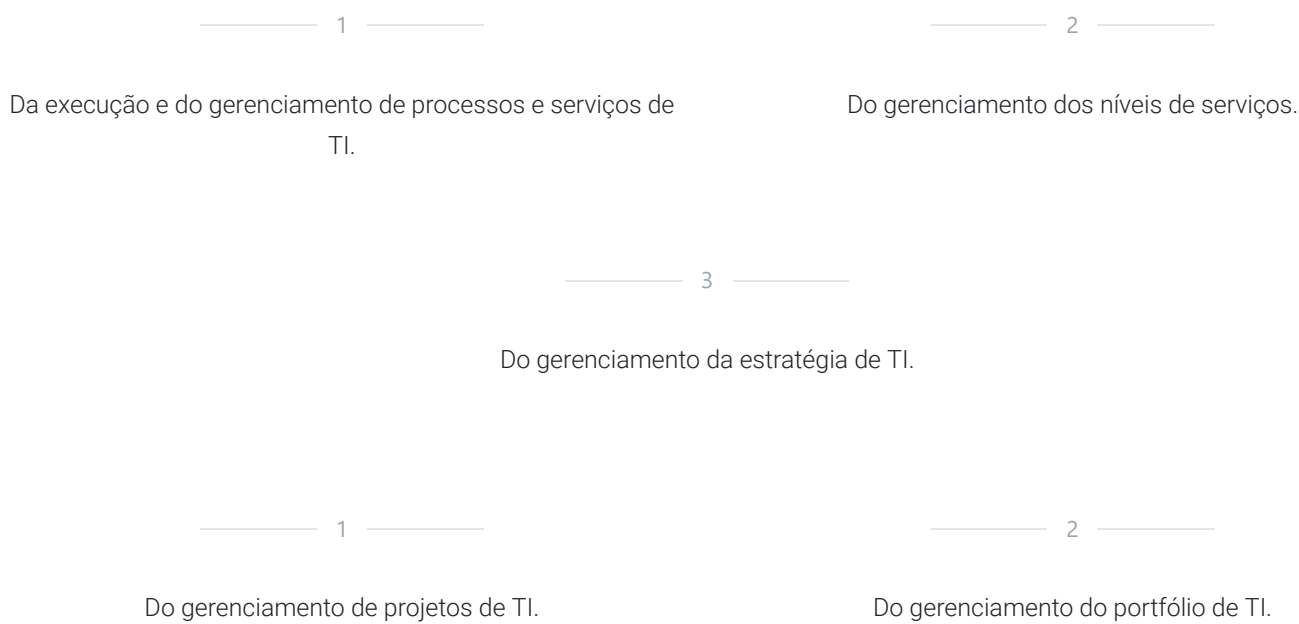
## Gestão de desempenho de TI

A gestão do desempenho de TI tem como objetivos:

- 1
- Verificar se o objetivo de TI foi atendido conforme planejado
- 2
- Entender os motivos da variação positiva ou negativa dos resultados obtidos em comparação com os resultados planejados.

Caso os resultados apresentem variação negativa, ações corretivas, preventivas ou de melhorias no processo devem ser recomendadas, monitoradas e implementadas, e posteriormente monitoradas.

Os resultados de TI são as medições derivadas de toda a prestação de serviços em termos de entrega de projetos e serviços e do atendimento a planos estratégicos e táticos. Esses resultados podem ser avaliados por meio:



Para que esses resultados possam ser efetivamente medidos e monitorados, a organização deverá lançar mão da utilização de indicadores de desempenho.

## Indicadores de desempenho

Um indicador de desempenho, também conhecido como **KPI** (sigla em inglês para *Key Performance Indicator*) é utilizado para:

- Medir e avaliar o desempenho de processos, e gerenciá-los da maneira mais eficaz e eficiente possível.
- Medir e avaliar as metas e objetivos previamente estipulados pelas organizações.

Um indicador é uma informação estruturada que permite comparações, inclusive com indicadores de outras organizações. Serve para comparar a métrica com um valor-base definido previamente (*baseline*) ou com um resultado esperado.

**As funções de um indicador são:**



Fonte: Shutterstock

Mensurar os resultados e gerir o desempenho.



Fonte: Shutterstock

Embasar a análise crítica dos resultados obtidos e do processo de tomada decisão.



Fonte: Shutterstock

Contribuir para a melhoria contínua dos processos organizacionais.



Fonte: Shutterstock

Facilitar o planejamento e o controle do desempenho.



Fonte: Shutterstock

Viabilizar a análise comparativa do desempenho da organização.

**A medição é necessária para confirmar que os esforços dispendidos na melhoria tiveram efeito e, assim, apoiar o sistema de melhoria contínua da organização.**

Os indicadores precisam ser apurados e documentados regularmente. Para que esse controle seja feito, é necessário definir as diretrizes de controle para cada indicador, ou seja, devem estar presentes na documentação de cada indicador:

Indicador (nome do indicador)	
Descrição	Fórmula
O que o indicador mede e qual a sua finalidade.	Como o indicador é calculado e a unidade de medida (número percentual, valor etc.)

Cada organização deve escolher o conjunto de indicadores relevantes para o seu negócio. Os indicadores de desempenho (KPI) devem observar as seguintes características:



A organização deverá definir o objetivo estratégico a ser medido. Todos os objetivos estratégicos de uma determinada área da organização devem ser mensurados individualmente, a partir de indicadores.

Para realizar o monitoramento, a organização poderá criar *dashboards* de gestão, agrupando os indicadores em diferentes níveis:

Clique nos botões para ver as informações.

Indicadores estratégicos

São os indicadores primários da organização, que serão acompanhados pela diretoria. O principal propósito é demonstrar de forma rápida se os objetivos estratégicos estão sendo alcançados.  
Exemplo: Faturamento bruto.

Indicadores táticos

São indicadores secundários, que serão acompanhados pelas gerências de cada departamento. Apesar de não serem estratégicos, seus resultados devem ser ligados aos resultados dos indicadores estratégicos.  
Exemplo: Faturamento por linha de produto ou por canal de vendas.

Indicadores operacionais

Indicadores que serão acompanhados pelos especialistas de cada área. Esses indicadores têm a função de fornecer mais detalhes para entendimento dos resultados dos indicadores táticos e estratégicos.  
Exemplo: Número de vendedores por canal de vendas.



O monitoramento do desempenho ocorre quando o resultado atingido é comparado com os resultados esperados, normalmente a intervalos regulares. Esse monitoramento deve responder as seguintes perguntas:

- Qual é o nosso desempenho atual?
- Existem diferenças entre o realizado e o previsto?
- O que está causando desvios?
- Qual é a tendência do desempenho?
- Como estamos em relação a referenciais de mercado (benchmarking)?
- Quais eventos causam variação positiva ou negativa no desempenho?
- Qual é o padrão de desempenho?

A partir desse monitoramento, a organização deverá estabelecer um plano de ação para atingir corrigir os possíveis desvios encontrados. O plano de ação deve deixar claro tudo o que deverá ser feito para o cumprimento dos objetivos e metas.

## Comunicação

A maneira mais eficiente de comunicação do desempenho organizacional é por meio da criação de dashboard que permita ao executivo consultar e entender, de forma rápida, o desempenho da TI.

No dashboard nem todos os indicadores serão estratégicos, mas todos deverão ter a função de monitorar o desempenho dos processos atuais ou o andamento em relação aos objetivos estratégicos da organização. A partir desse monitoramento, a organização estabelecerá um plano de ação para atingir e corrigir os possíveis desvios encontrados.

**Atenção!** Aqui existe uma videoaula, acesso pelo conteúdo online

### Saiba mais

**Você sabe o que é um *Dashboard*?**

A exibição de relatórios e informações relevantes em uma única tela, permitindo analisar os dados de forma rápida e com maior facilidade de compreensão. Compreendendo a importância e o significado global de um conjunto de informação com maior precisão, há a possibilidade de realizar comparações entre os diferentes tipos de gráficos.

Com a visão global dos dados, é possível identificar tendências e relações, levando o gestor a uma percepção mais profunda da situação, fornecendo uma visão geral do que está acontecendo no ambiente organizacional e permitindo diagnosticar por que algo ocorreu e sua origem.

# Gestão de risco

Você sabe o que é risco?



As organizações de todos os tipos e tamanhos enfrentam influências e fatores internos e externos que tomam incerto se e quando elas atingirão seus objetivos. O efeito que essa incerteza tem sobre os objetivos da organização é chamado de risco.”

ABNT NBR ISO 31000:2009 — Gestão de Risco, Princípios e Diretrizes

É qualquer impacto em potencial nos objetivos da empresa causado por um evento não planejado deve ser identificado, analisado e avaliado.

A organização deve dar uma atenção especial aos riscos de TI, que podem comprometer a operação da organização e gerar impacto nos negócios. Por isso, deve criar e manter uma estrutura de gestão de risco que documente os riscos de TI, as estratégias de mitigação e os [riscos residuais](#)<sup>1</sup>.

Estratégias de mitigação de risco devem ser adotadas para minimizar os riscos residuais a níveis aceitáveis. O resultado da avaliação deve ser entendido pelas partes interessadas, e expresso em termos financeiros, para permitir que as partes interessadas alinhem o risco a níveis de tolerância aceitáveis. Entretanto, precisamos considerar que nem sempre o risco percebido é o risco verdadeiro.

Segundo a norma ISO 31000, o processo de gestão de riscos envolve as seguintes atividades:

A **gestão de riscos** contempla uma série de atividades relacionadas à forma como uma organização lida com o risco. Cobre todo o ciclo de vida de tratamento de risco, desde sua identificação até a comunicação às partes envolvidas.

## 1) A fase de identificação dos riscos

É o processo de busca, reconhecimento e descrição de riscos. Essa busca pode envolver dados históricos, análises teóricas, opiniões de pessoas informadas e especialistas, e as necessidades das partes interessadas. Nessa fase é preciso identificar:

- **Fonte de risco:** É um elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco.
- **Evento:** Representa a ocorrência ou alteração em um conjunto específico de circunstâncias. Um evento pode consistir em uma ou mais ocorrências, podendo ter várias causas.
- **Consequência:** É o resultado de um evento que afeta os objetivos. Um evento pode levar a uma série de consequências. Uma consequência pode ser certa ou incerta e pode ter efeitos positivos ou negativos sobre os objetivos.
- **Probabilidade:** É a chance de algo acontecer.
- **Perfil de risco:** É a descrição de um conjunto qualquer de riscos que dizem respeito a toda a organização, parte da organização, ou referente ao que tiver sido definido.

## 2) A fase de análise dos riscos

Contempla todos os levantamentos em relação às possibilidades de algum objetivo de TI não se concretizar, as causas do problema, ameaças, vulnerabilidades, probabilidades e impacto aos quais os ativos estão sujeitos.

## 3) A fase de avaliação de risco

É o processo de avaliar regularmente a probabilidade e o impacto de todos os riscos identificados, utilizando métodos qualitativos e quantitativos.

## QUALITATIVO

Em vez de usarmos valores numéricos para estimar os componentes do risco, trabalhamos com menções mais subjetivas como alto, médio e baixo. O que torna o processo mais rápido. Os resultados dependem muito do conhecimento do profissional que atribuiu notas aos componentes do risco que foram levantados.



## QUANTITATIVO

A métrica é feita por meio de uma metodologia na qual tentamos quantificar em termos numéricos os componentes associados ao risco. O risco é representando em termos de possíveis perdas financeiras.

Os **critérios de risco** representam os termos de referência contra a qual o significado de um risco é avaliado. Eles são baseados nos objetivos organizacionais e no contexto externo e interno, e podem ser derivados de normas, leis, políticas e outros requisitos.

O **nível de risco** representa a magnitude de um risco, expressa em termos da combinação das consequências e de suas probabilidades.

A **probabilidade** e o **impacto** associado ao risco inerente e residual devem ser determinados individualmente, por categoria, e com base no portfólio da organização.

Na fase de **tratamento dos riscos** diferentes ações podem ser implementadas:

————— 1 —————

### Preventivas

Controles que reduzem a probabilidade do risco se concretizar ou diminuem o grau do impacto de sua ocorrência.

————— 2 —————

### Corretivas

Reduzem o impacto da ocorrência do risco.

————— 3 —————

### Detectivas


Disparam medidas reativas, tentando evitar a concretização do risco.

A **comunicação dos riscos** identificados pelo processo de gestão de risco deverá ser feita para todas as partes envolvidas no processo, que precisem ter conhecimento dos riscos, tenham eles sido tratados ou não.

 Fonte: Shutterstock

**Aceitar um risco é uma das maneiras de tratá-lo. Ocorre quando o custo de proteção contra um determinado risco não vale a pena.**

## Compliance

 Fonte: Shutterstock

Qual a diferença entre ser compliance e estar compliance?

Ser compliance é conhecer as normas da organização, seguir os procedimentos recomendados, agir em conformidade e sentir o quanto é fundamental a ética e a idoneidade em todas as nossas atitudes.



Estar em compliance é estar em conformidade com leis e regulamentos internos e externos.

O compliance vai além das barreiras legais e regulamentares, incorporando princípios de integridade e conduta ética.

Diferença entre **auditoria** e **compliance**:

## AUDITORIA

Realiza seus trabalhos de forma aleatória e temporal, por meio de amostragens, a fim de certificar o cumprimento das normas e processos instituídos pela Alta Administração.

## COMPLIANCE

Realiza suas atividades de forma rotineira e permanente, sendo responsável por monitorar e assegurar de maneira corporativa e tempestiva que as diversas unidades da Instituição estejam respeitando as regras aplicáveis a cada negócio, por meio do cumprimento das regulamentações, dos processos internos, da prevenção e do controle de riscos envolvidos em cada atividade.

- Para que a função de compliance seja eficaz nas organizações, é necessário o comprometimento da alta administração.
- O compliance deve fazer parte da cultura organizacional, contando com o comprometimento de todos os funcionários.
- Todos são responsáveis por compliance.
- Em relação à área de TI, o compliance refere-se à conformidade da área de TI da organização a regulamentos internos e externos impostos às suas atividades.

**Atenção!** Aqui existe uma videoaula, acesso pelo conteúdo online

## Atividade

1. A  tem objetivo verificar se o objetivo de TI foi atendido conforme planejado pela organização e entender os motivos da variação positiva ou negativa dos resultados obtidos em comparação com os resultados planejados.

2. Os  são indicadores primários da organização, que serão acompanhados diretamente pela diretoria e seu principal propósito é demonstrar de forma rápida se os objetivos  estão sendo alcançados.

3. Na avaliação dos riscos existem dois métodos que podem ser aplicados. O método em que trabalhamos com menções mais subjetivas como alto, médio e baixo, chama-se:

### Notas

### Riscos residuais <sup>1</sup>

Riscos que não podem ser completamente eliminados; a porção do risco existente após todas as medidas de tratamento terem sido tomadas.

### Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO 31000:2018**. Gestão de riscos — Princípios e diretrizes. São Paulo: ABNT, 2018.

<sup>1</sup>FERNANDES, A. A.; ABDELVALY, E. M. (coord.). **Compliance em TI**. São Paulo: Editora Atlas, 2015. Disponível em: <http://www.abnt.org.br/abnt/normas/abnt-nbr-31000-2018>. Acesso em: 14 de Maio de 2018.

FERNANDES, A. A.; ABREU, V. F. **Implantando a Governança de TI:** da Estratégia à Gestão dos Processos e Serviços. 4. ed. Rio de Janeiro: Brasport, 2014.

FUNDAÇÃO NACIONAL DA QUALIDADE (FNQ). **Indicadores de desempenho:** estruturação do sistema de indicadores organizacionais. São Paulo: FNQ, 2014.

PARMENTER, D. **Key performance indicators:** Developing, Implementing, and Using Winning KPIs. Nova Jersey, Estados Unidos: Wiley, 2015.

## Próxima aula

---

- Modelo de governança de TI apresentado pela ISO 38500;
- Modelo de governança de TI apresentado pelo COBIT;
- Diferenças entre os dois modelos.

## Explore mais

---

- Assista ao vídeo [Gestão por indicadores <https://www.youtube.com/watch?v=v5aGv9iVZIU&t=13s>](https://www.youtube.com/watch?v=v5aGv9iVZIU&t=13s).
- Baixe o ebook gratuito [Guia completo para ter uma empresa competitiva <http://www.fnq.org.br/informe-se/publicacoes/e-books>](http://www.fnq.org.br/informe-se/publicacoes/e-books).