

NORMA ISO/IEC 38500

RESUMO

AVISO GERAL

Este é um Resumo da **Norma ISO/IEC 38500:2008** e da equivalente Norma Brasileira publicada em língua portuguesa no ano de 2009 pela Associação Brasileira de Normas Técnicas (ABNT). Trata-se de um material para revisão rápida e não, um material completo. Maiores detalhes sobre este material e informações sobre o curso completo podem ser obtidos através do link:

<http://www.provasdeti.com.br/mdl-govo1lc-iso-iec-38500-governanca-corporativa-de-ti-prof-luis-claudio.html>

A QUEM SE DESTINA

Este material se destina às pessoas que já estudaram a Norma ISO/IEC 38500:2008 e querem fazer uma revisão rápida de seus principais pontos ou àqueles que não conhecem a Norma e querem ter uma visão geral sobre ela.

PROFESSORES RESPONSÁVEIS

A confecção deste material foi realizada e coordenada pelo Prof. **Luis Claudio**, M.Sc. Os materias mais recentes e as novidades trazidas pelo Prof. LC podem ser vistos em nosso site através do link

<http://www.provasdeti.com.br/landing-professor-luis-claudio>

Ou em nosso site (ProvasdeTI.com.br) no menu "Por Professor" > "Luis Claudio"

Bons estudos.

Provas de TI, tudo para você passar!

INTRODUÇÃO AO CURSO

A ISO/IEC 38500:2008 é uma Norma internacional para a **Governança Corporativa de Tecnologia da Informação** publicada conjuntamente pela *International Organization for Standardization* (ISO) e pela *International Electrotechnical Commission* (IEC).

Atualmente, ela está na versão 2015 e pode ser acessada através do link http://www.iso.org/iso/catalogue_detail.htm?csnumber=62816 (acesso realizado em 27/02/2016). O custo da Norma em inglês é de CFH 58,00, o que dá aproximadamente R\$ 232,42 (câmbio de 27/02/2016) após a conversão. Aqui no Brasil, a versão antiga traduzida (ABNT NBR ISO/IEC 38500:2009) pode ser obtida por R\$ 88,00 através do site da ABNT.

Este conteúdo passou a ser cobrado de forma mais recorrente a partir de 2015 por bancas como FCC, CESPE, ESAF, entre outras. Por ora, a maior parte cobrou apenas a versão mais antiga, de 2008 (publicada no Brasil em 2009 pela ABNT), até porque não existe ainda uma versão em português da Norma mais recente (a que foi revisada em 2015).

De qualquer modo, não houve muita mudança na ISO/IEC 38500. Isso porque ela está dando origem a uma família. Assim, a tendência é que ela permaneça menor e os detalhes sejam esmiuçados noutras Normas. Atualmente já temos a ISO/IEC 38502 (Governance of IT — Framework and model), já publicada em 2014, e a ISO/IEC 38501 (Corporate governance of IT implementation guide), esta ainda em fase de acabamento e aprovações finais para publicação.

A ISO/IEC 38500:2008 é uma Norma rápida de ser estudada. Ela possui só 15 páginas de conteúdo na versão de 2008 (a versão de 2015 foi reduzida para 12). O conteúdo que mais se destaca são os **princípios** e também o **modelo** da boa Governança Corporativa de TI!

Segue abaixo resumo das seções desta Norma.

INTRODUÇÃO

As **despesas com TI** podem representar uma proporção significativa dos gastos com pessoas, infraestrutura, aplicativos e processos de trabalho. Entretanto, o **ROI** nem sempre é totalmente obtido e percebido pela organização.

A principal razão para isso é a **ênfase nos aspectos técnicos**, financeiros e de programação das atividades de TI, ao invés da ênfase no **contexto geral do negócio**.

Lembre-se sempre de que “**governança** é diferente de **gestão**”. Governança tem mais a ver com diretores (determinam objetivos e metas estratégicas) e gestão tem mais a ver com gerentes (que gerenciam recursos para atingir os objetivos e metas estratégicas estabelecidos pela direção).

SEÇÃO 1 – ESCOPO, APLICAÇÃO E OBJETIVOS

O escopo principal da Norma é oferecer princípios para **orientar os dirigentes** das organizações (proprietários, membros do conselho de administração, diretores, executivos seniores ou similares) sobre o uso eficaz, eficiente e aceitável da Tecnologia da Informação. Mas, adicionalmente, ela também fornece orientações para aqueles que aconselham, informam ou assessoram os dirigentes (gerentes seniores, especialistas internos e externos, auditores de TI etc.)

A Norma se aplica a **todas as organizações**, independente do porte, setor e dependência do uso da TI.

O propósito desta Norma é...:

- a) informar e orientar os dirigentes quanto ao uso eficaz, eficiente e aceitável da TI;
- b) garantir que se a Norma for seguida, pode-se confiar na Governança Corporativa de TI;
- c) fornecer uma base para avaliação objetiva da Governança Corporativa de TI.

Com relação à **conformidade**, a Governança Corporativa de TI ajuda os dirigentes a garantirem o cumprimento de obrigações (legais, regulamentares, contratuais etc.). Note que há países onde os dirigentes podem ser responsabilizados se um sistema inadequado resultar em não cumprimento de obrigações (pagamento de impostos, respeito a propriedade intelectual, licenças de softwares etc.).

Quanto ao **desempenho**, a Governança Corporativa de TI ajuda os dirigentes a garantir que o uso da TI contribua positivamente para o bom desempenho da organização. Note que a correta implementação e operação dos ativos de TI gera maior grau de continuidade e sustentabilidade do negócio, mais alinhamento da TI com o negócio, alocação mais eficiente de recursos e até redução de custos.

Algumas definições importantes da Norma são:

- o **Aceitável** é atender às necessidades das partes interessadas;
- o **Comportamento humano** é a compreensão das interações entre os seres humanos e demais elementos de um sistema, com a intenção de garantir o bem-estar das pessoas e o desempenho dos sistemas;
- o **Governança Corporativa** é o sistema pelo qual a organização é dirigida e controlada (Cadbury 1992 e OECD 1999);
- o **Governança Corporativa de TI** é o sistema pelo qual o uso atual e futuro da TI é dirigido e controlado;
- o **Gerenciamento** é o sistema de controles e processos necessários para alcançar objetivos estratégicos estabelecidos pela direção da organização;
- o **Política** são instruções claras que condicionem as decisões;
- o **Recursos** são pessoas, procedimentos, informações, software e infra, capital e tempo;
- o **Uso da TI** é o planejamento, projeto, desenvolvimento, distribuição, operação, gerenciamento e aplicação da TI para atender às necessidades do negócio.

SEÇÃO 2 – ESTRUTURA PARA UMA BOA GOVERNANÇA CORPORATIVA DE TI

Os princípios expressam o comportamento preferido para **orientar uma tomada de decisão**. Eles referem-se ao **que** convém acontecer, mas não descrevem como, quando e por quem os princípios seriam implementados.

Os dirigentes **devem exigir a aplicação de SEIS princípios**.

- Seção 2.1.1 – **Responsabilidade** - Todos compreendem e aceitam suas responsabilidades com respeito ao fornecimento e demanda da TI. Os responsáveis pelas ações também devem ter autoridade para desempenhar tais ações.
- Seção 2.1.2 – **Estratégia** - A estratégia de negócio da organização leva em conta as capacidades atuais e futuras da TI. Os planos estratégicos de TI satisfazem as necessidades atuais e contínuas da estratégia de negócio da organização.
- Seção 2.1.3 – **Aquisição** - Existe um equilíbrio apropriado entre benefícios, oportunidades, custos e riscos.
- Seção 2.1.4 – **Desempenho** - A TI é adequada ao propósito de apoiar a organização, fornecendo serviços de forma apropriada (nível, qualidade, capacidade, sustentabilidade etc.) necessários para atender a seus requisitos atuais e futuros.
- Seção 2.1.5 – **Conformidade** - A TI cumpre com toda a legislação e regulamentos obrigatórios. As políticas e práticas são claramente definidas, implementadas e fiscalizadas.
- Seção 2.1.6 – **Comportamento Humano** - As políticas, práticas e decisões de TI demonstram respeito pelo Comportamento Humano, incluindo as necessidades atuais e futuras de todas as “pessoas no processo”.



DICA: Tente usar o mnemônico **READ CC**

O modelo para Governança Corporativa de TI envolve **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.

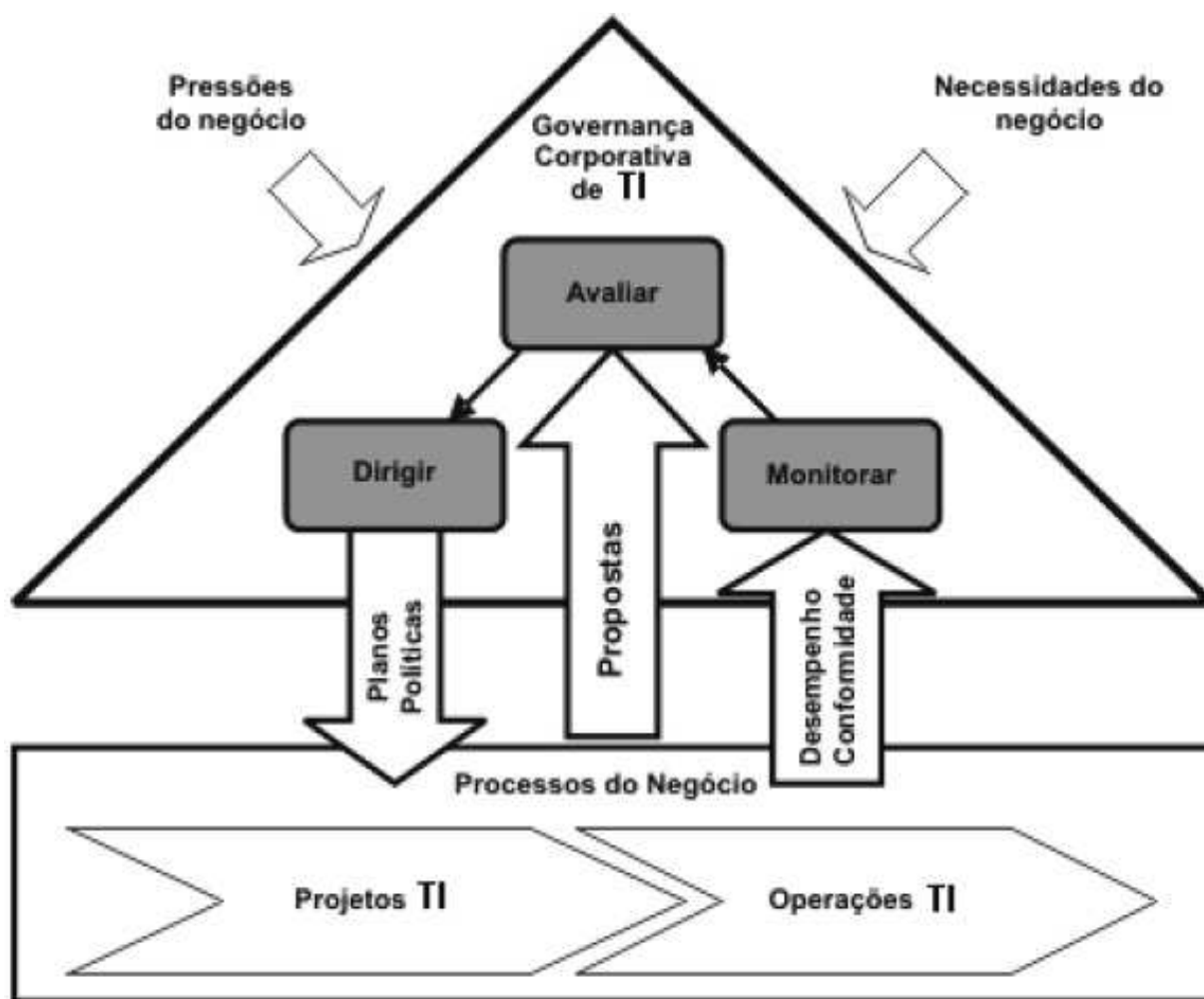
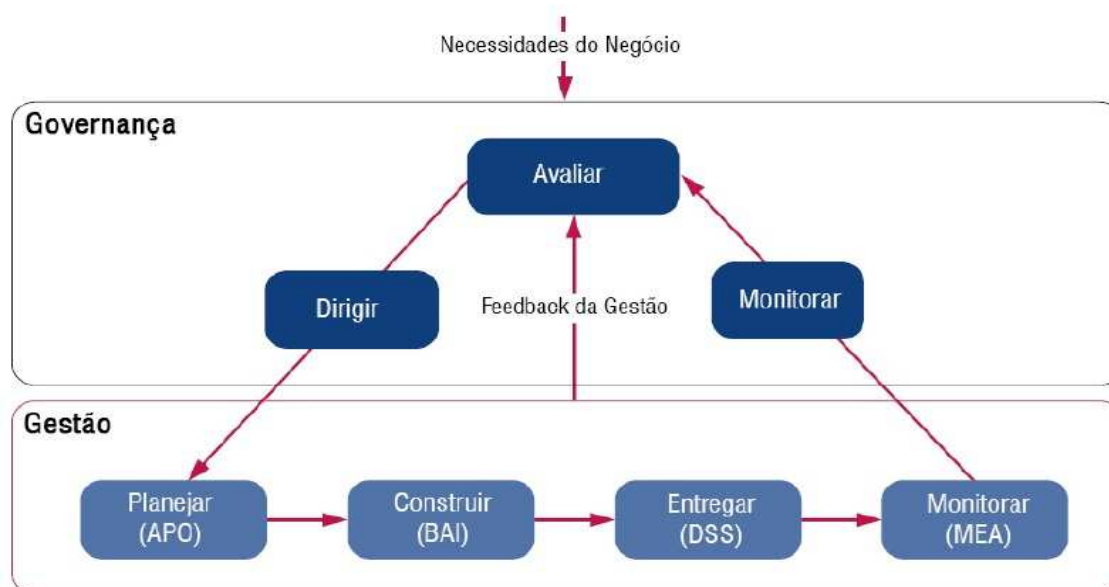


Figura 1: Modelo para Governança Corporativa de TI segundo a Norma ABNT NBR ISO/IEC 38500:2009.

Obs.: Embora a imagem abaixo não esteja na ISO/IEC 38500:2008, é importante comparar ambas e ver como esta Norma influenciou o Cobit v.5.



Segundo a ISO/IEC 38500:2008, **avaliar** envolve considerar as pressões externas e internas que influenciam o negócio, tais como mudanças tecnológicas, tendências econômicas e sociais e influências políticas.

Segundo a ISO/IEC 38500:2008, **dirigir** envolve exigir a preparação e implementação de planos e políticas. Os dirigentes devem assegurar que a transição dos projetos para a entrada em operação seja corretamente planejada e gerenciadas. Convém que os dirigentes encorajem uma cultura de boa governança de TI em suas organizações, exigindo que os gerentes forneçam as informações em tempo adequado, cumprindo as orientações e em conformidade com os seis princípios da boa governança.

Segundo a ISO/IEC 38500:2008, **monitorar** envolve determinar sistemas de mensuração apropriados. Convém certificar-se de que o desempenho está de acordo com os planos, principalmente no que diz respeito aos objetivos do negócio. A responsabilidade pelo uso e entrega aceitável, eficaz e eficiente da TI permanece sempre com os dirigentes, embora alguns aspectos específicos da TI possam ser delegados aos gerentes.

Nota: Para indicar erros ortográficos, necessidade de atualizações ou sugerir mudança e melhorias, envie-nos um e-mail para faleconosco@provasdeti.com.br. Ficamos felizes em melhorar sempre!