Ajuda da Pesquisa sobre Perfil de Governança de TI 2010
Objetivos das Questões

ÍNDICE

Ajuda da Pesquisa sobre Perfil de Governança de TI 2010

Objetivos das Questões

Este documento descreve os objetivos e destaca aspectos relevantes de cada questão formulada no questionário sobre o Perfil de Governança de TI 2010, além de referenciar a legislação, normas técnicas ou boas práticas que fundamentam tais proposições.

As questões estão agrupadas conforme os seguintes critérios, definidos no "Modelo de Excelência em Gestão Pública": Liderança, Estratégias e Planos, Cidadãos, Sociedade, Informações e Conhecimento, Pessoas, Processos.[1]

1. LIDERANÇA

1.1 Em relação à estrutura de governança, a Alta Administração da instituição:

- ☐ se responsabiliza pelo estabelecimento e pelo cumprimento das políticas de gestão e uso corporativos de TI.
- ☐ designou formalmente um Comitê de TI para **auxiliá-la nas decisões** relativas à gestão e ao uso corporativos de TI.
- ☐ designou representantes de todas as áreas relevantes para o negócio institucional para compor o Comitê de TI.
- ☐ monitora regularmente o funcionamento do Comitê de TI.
- ☐ nenhuma das opções anteriores descreve a situação desta instituição.

Esta questão busca verificar se o processo decisório relativo à gestão e uso de TI na organização é realizado com auxílio de um comitê formalmente designado, do qual participem representantes das diversas áreas de negócio da instituição, conforme recomendado pelas melhores práticas. [2]

1.2 Em relação ao desempenho organizacional na gestão e no uso de TI, a Alta Administração da instituição:

- ☐ estabeleceu objetivos (diretrizes) de desempenho de gestão e de uso corporativos de TI.
- ☐ estabeleceu indicadores de desempenho de gestão e de uso corporativos de TI.
- ☐ recebe e avalia regularmente informações sobre o desempenho relativo à gestão e ao uso corporativos de TI.
- ☐ acompanha os indicadores de benefício dos principais sistemas de informação e toma decisões a respeito quando as metas de benefício não são atingidas.
- ☐ nenhuma das opções anteriores descreve a situação desta instituição.

Esta questão busca verificar se, nos processos de planejamento, são definidos os objetivos de negócio e os indicadores de desempenho associados, e se esses indicadores são monitorados e avaliados periodicamente pela Alta Administração, tanto para os processos de gestão de TI quanto para os processos relacionados ao uso de TI na organização. [3]

1.3 Em relação ao desenvolvimento interno de gestores de TI, a Alta Administração da instituição:

- ☐ provê política de desenvolvimento de gestores de TI.
- ☐ prioriza (>75%) o preenchimento das funções gerenciais com pessoas do quadro efetivo permanente da própria instituição.
- ☐ implementa programa de acompanhamento de desempenho gerencial.
- ☐ escolhe os gestores de TI fundamentalmente com base em suas competências (p.ex. desempenho profissional, experiência, formação acadêmica etc.)
- ☐ nenhuma das opções anteriores descreve a situação desta instituição.

Esta questão busca verificar certos aspectos de como a Alta Administração gerencia sua equipe de gestão de TI e se há políticas que suportam esse esforço de gerenciamento.[4]

1.4 Foi realizada alguma auditoria de TI por iniciativa da própria instituição nos últimos três anos? Em que áreas?

- ☐ não foi realizada auditoria de iniciativa da própria instituição nos últimos três anos.
- ☐ auditoria de dados.
- ☐ auditoria de segurança da informação.
- ☐ auditoria de contratos de TI.
- ☐ auditoria de sistemas de informação.
- ☐ auditoria de governança de TI.
- ☐ outra(s). Qual(is)? _____

Esta questão busca verificar se houve mudança no quadro identificado no levantamento de governança realizado em 2007, bem como identificar se a organização monitora e avalia seus controles internos de TI por meio de auditorias específicas. [5]

2. ESTRATÉGIAS E PLANOS

2.1 Em relação ao processo de planejamento estratégico institucional, marque a opção que melhor descreve a sua instituição:

- ○ a instituição não executa um processo de planejamento estratégico institucional.
- ○ a instituição desenvolve planos estratégicos, mas não de maneira periódica.
- ○ a instituição executa um processo periódico de planejamento, embora este não esteja formalmente instituído.
- ○ o processo de planejamento estratégico institucional é formalmente (aprovado e publicado) instituído.
- ○ o processo de planejamento estratégico institucional formal é acompanhado segundo indicadores e metas estabelecidos.
- ○ o processo de planejamento estratégico institucional formal é aperfeiçoado continuamente com base na análise de seus indicadores.

Esta questão busca obter informações sobre o nível de maturidade do processo de planejamento estratégico institucional da organização. [6]

2.2 Em relação ao processo de planejamento estratégico de TI, marque a opção que melhor descreve a sua instituição:

- ○ a instituição não executa um processo de planejamento estratégico de TI.
- ○ a instituição desenvolve alguns planos estratégicos de TI, mas não de maneira periódica.
- ○ a instituição executa um processo periódico de planejamento, embora este não esteja formalmente instituído.
- ○ o processo de planejamento estratégico de TI é formalmente (aprovado e publicado) instituído.
- ○ o processo de planejamento estratégico de TI formal é acompanhado segundo indicadores e metas estabelecidos.
- ○ o processo de planejamento estratégico de TI formal é aperfeiçoado continuamente com base na análise de seus indicadores.

Esta questão busca obter informações sobre o nível de maturidade do processo de planejamento estratégico de TI da organização. [7]

2.3 Em relação ao PDTI (Plano Diretor de Tecnologia da Informação):

- ☐ a instituição não aprovou e nem publicou PDTI interna ou externamente.
- ☐ o PDTI vincula as ações de TI a indicadores e metas de negócio.
- ☐ o PDTI vincula os custos de TI a atividades e projetos de TI.
- ☐ o PDTI é publicado na internet para acesso livre.
- ☐ o PDTI vincula as ações de TI a indicadores e metas de serviços ao cidadão.

Esta questão busca identificar algumas características do documento resultante do processo de planejamento estratégico de TI. [8]

2.4 Em relação ao processo decisório de priorização das ações e gastos de TI, assinale a opção que melhor descreve sua instituição:

- ○ As decisões acerca da priorização das ações e gastos de TI são tomadas pela área de TI.
- ○ As decisões acerca da priorização das ações e gastos de TI são tomadas pelo Comitê de TI.
- ○ As decisões acerca da priorização das ações e gastos de TI são tomadas pela Alta Administração da instituição, sem apoio de Comitê de TI ou da área de TI.
- ○ As decisões acerca da priorização das ações e gastos de TI são tomadas pela Alta Administração da instituição, com apoio da área de TI como instância consultiva.
- ○ As decisões acerca da priorização das ações e gastos de TI são tomadas pela Alta Administração da instituição, com apoio do Comitê de TI como instância consultiva.

Esta questão busca verificar o papel da Alta Administração, do Comitê de TI (se houver) e da área de TI no processo decisório de priorização das ações e gastos de TI da organização. [9]

3. CIDADÃOS

3.1 Em relação ao atendimento ao Decreto nº 6.932/2009:

- ○ não é aplicável a esta instituição.
- ○ a instituição ainda não publicou a sua Carta de Serviços ao Cidadão.
- ○ a instituição está providenciando a publicação da sua Carta de Serviços ao Cidadão para 2010, sem incluir serviços de TI.
- ○ a instituição está providenciando a publicação da sua Carta de Serviços ao Cidadão para 2010 e incluirá serviços de TI.
- ○ a instituição já publicou a sua Carta de Serviços ao Cidadão, mas não incluiu serviços de TI.
- ○ a instituição já publicou a sua Carta de Serviços ao Cidadão e incluiu serviços de TI.

Esta questão busca verificar a situação da organização em relação ao Decreto 6.932/2009, que dispõe sobre a simplificação do atendimento público prestado ao cidadão e, entre outras providências, determina a obrigatoriedade de elaboração e divulgação da "Carta de Serviços ao Cidadão", que tem por objetivo informar o cidadão dos serviços prestados pelo órgão ou entidade, das formas de acesso a esses serviços e dos respectivos compromissos e padrões de qualidade de atendimento ao público. [10]

4. SOCIEDADE

4.1 Em relação ao atendimento aos interesses da sociedade, a instituição:

☐ adota política formal de TI para conservação de recursos não renováveis, preservação dos ecossistemas e a otimização do uso dos recursos renováveis (p. ex. economia de insumos físicos, de energia elétrica etc.)

Esta questão busca verificar se há política de TI em relação a temas ambientais e, no caso de organização integrante do SISP, a sua situação em relação à Instrução Normativa SLTI/MPOG nº 01, de 19 de janeiro de 2010, que dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal. [11]

5. INFORMAÇÕES E CONHECIMENTO

5.1 Preencha a primeira coluna com as três ações orçamentárias institucionais finalísticas de maior valor (portanto, exclui-se qualquer ação pertencente ao programa "0750.Apoio Administrativo", como p.ex. "2000.Administração da Unidade"). A seguir, elenque os sistemas de informação de maior relevância no suporte de cada ação finalística.

Programa e ação orçamentária (LOA)	Sigla e breve descrição do sistema (no formato "sigla: descrição")	CN[1]	BM?[2]
Programa.Ação (1) _____._____			
Programa.Ação (2) _____._____			
Programa.Ação (3) _____._____			

[1] CN (Criticidade para o negócio):
se o sistema parar: (1) o negócio para imediatamente; (2) o negócio para em uma semana; (3) o negócio para em um mês; (4) o negócio é afetado, mas não para; (5) o negócio não é afetado.

[2] BM? (O benefício de negócio é mensurado?):
o benefício (valor agregado) que o sistema traz para o alcance do(s) objetivo(s) da ação orçamentária é mensurado por meio de indicadores de negócio?

Esta questão busca identificar quais são os sistemas informatizados mais críticos para o negócio da organização, aos quais deveriam estar dirigidos os maiores esforços e os mais rigorosos controles de risco. A mensuração de benefícios é a forma de mensurar a importância do sistema informatizado para o negócio e dá a base econômica para avaliação de alternativas de investimento e a aceitabilidade dos custos de controle. [12]

6. PESSOAS

6.1 Qual o quantitativo de funções comissionadas voltadas à gestão de TI?

Obs: o valor da primeira resposta deve equivaler à soma das demais respostas

_____ quantitativo total de funções comissionadas de gerenciamento e assessoramento específicas para gestão de TI.
_____ funções preenchidas por servidores públicos efetivos oriundos de outras instituições.
_____ funções preenchidas por servidores efetivos da instituição.
_____ funções preenchidas por pessoas que não são servidores efetivos.
_____ outra(s) situação(ões). Quais ?

Esta questão busca identificar a composição da força de trabalho que detém funções comissionadas gerenciais ou de assessoramento na área de TI ou ainda que contribuem significativamente em processos decisórios de TI, discriminando-se: servidores públicos efetivos da própria instituição, servidores públicos cedidos de outras instituições ou servidores não efetivos em cargos de livre nomeação. [13]

6.2 Qual o quantitativo de pessoas que compõem a força de trabalho em TI?

Obs: o valor da primeira resposta deve equivaler à soma das demais respostas

_____ quantitativo total da força de trabalho em TI.
_____ servidores públicos efetivos da carreira de TI da própria instituição.
_____ servidores públicos efetivos de outras carreiras (que não TI) da própria instituição.
_____ servidores públicos cedidos de outras instituições públicas.
_____ servidores públicos não efetivos em cargos de livre nomeação.
_____ estagiários.
_____ terceirizados que trabalham regularmente no ambiente da instituição (contratos de serviços continuados com cessão de mão de obra).
_____ terceirizados que trabalham no ambiente da instituição para execução de projetos de tempo determinado.
_____ outros. Quais ? _____

Esta questão busca identificar a composição da força de trabalho **total** cujo foco seja o funcionamento da TI organizacional. Em algumas instituições a TI está descentralizada em pequenas áreas de TI. Em outras, as áreas de negócio possuem funções de TI. Em todos esses casos deve-se lançar o número de pessoas cujo foco principal de trabalho é a própria TI, mesmo que não seja dentro de uma área de TI. [14]

6.3 Em relação ao plano de capacitação de pessoal para gestão TI, assinale a opção que melhor descreve sua instituição:

- ○ Não há critério definido para avaliação e atendimento aos pedidos de capacitação.
- ○ É realizada capacitação do pessoal recém-ingresso, que a partir de então recebe capacitação quando necessário.
- ○ A instituição elabora e executa um plano de capacitação para atender às necessidades de capacitação em gestão de TI.
- ○ A instituição mede o cumprimento do plano de capacitação e consegue identificar e corrigir desvios na sua execução.
- A instituição avalia e melhora o plano da capacitação dos gestores de TI de acordo com as melhores práticas da Administração Pública e da iniciativa privada.

Esta questão busca obter informações sobre o nível de maturidade do processo de capacitação dos gestores de TI da organização. [15]

6.4 Em relação à qualificação do atual principal dirigente responsável pela gestão de TI na instituição, quais dos elementos abaixo ele possui:

Obs: A lista abaixo não é exaustiva e não corresponde necessariamente a requisitos mínimos para o exercício do papel em foco

- ☐ experiência em gestão de TI. Quantos anos? _____.
- ☐ curso superior (em qualquer área não relacionada à TI).
- ☐ curso superior (em qualquer área relacionada à TI).
- ☐ pós-graduação *lato sensu* (especialização) não relacionada à TI.
- ☐ pós-graduação *lato sensu* (especialização) em TI, exceto gestão ou governança de TI.
- ☐ pós-graduação *lato sensu* (especialização) em gestão ou governança de TI.
- ☐ pós-graduação *stricto sensu* (mestrado/doutorado/pós-doutorado) não relacionada à TI.
- ☐ pós-graduação *stricto sensu* (mestrado/doutorado/pós-doutorado) em TI, exceto gestão ou governança de TI.
- ☐ pós-graduação *stricto sensu* (mestrado/doutorado/pós-doutorado) em gestão ou governança de TI.
- ☐ certificados profissionais (CGEIT, CobiT, PMP, ITIL, CISM, CISA etc.).
  Quais? _____.
- ☐ outros elementos de qualificação considerados relevantes.
  Quais? _____.

Esta questão busca identificar os elementos relevantes na formação do principal gestor de TI da organização (também conhecido na literatura como “Chief Information Officer – CIO”). [16]

7. PROCESSOS

7.1 A instituição implementou formalmente (aprovou e publicou) os processos corporativos de segurança da informação abaixo relacionados?

- ☐ Inventariar todos os ativos de informação (dados, hardware, software e instalações).
- ☐ Classificar a informação para o negócio (p.ex. divulgação ostensiva ou restrita).
- ☐ Analisar os riscos aos quais a informação crítica para o negócio está submetida, considerando, pelo menos, confidencialidade, integridade e disponibilidade.
- ☐ Gerenciar os incidentes de segurança da informação.

Esta questão busca identificar processos relativos à Segurança da Informação implantados na organização. [17]

7.2 A instituição formalizou (aprovou e publicou):

- ☐ a política corporativa de segurança da informação.
- ☐ a designação de responsável(is) por implantar e acompanhar a política corporativa de segurança da informação.

Esta questão busca verificar se a organização possui Política de Segurança da Informação formalmente instituída e com responsabilidades pela execução definidas. [18]

7.3 Em que nível de capacidade/maturidade melhor se enquadra o seu atual processo de software?

Obs: com base na ABNT NBR ISO/IEC 15.504

- ○ ***Ad hoc*** (não há processo e nem conceito de qualidade do processo).
- ○ Inicial (não há processo nem seu controle, mas já há conceitos de qualidade de processo em implantação).
- ○ Gerenciado (há um processo informal repetido várias vezes e que implementa conceitos de qualidade de processo).
- ○ Definido (há um processo formal – aprovado e publicado – e obrigatório).
- ○ Mensurado (o processo é controlado por meio de mensurações e há metas de processo a cumprir).
- ○ Em otimização (o processo é periodicamente revisado e melhorado com base nas suas mensurações)

Esta questão busca obter informações sobre o nível de maturidade do processo de software da organização. [19]

7.4 Em relação ao processo de gerenciamento de projetos:

- ○ A instituição não pratica o gerenciamento de projetos.
- ○ A instituição pratica o gerenciamento de projetos, mas não adota qualquer padrão interno ou de mercado.
- ○ A instituição formalizou (aprovou e publicou) um padrão interno ou de mercado para gerenciamento de projetos.
- ○ A instituição acompanha e mede o processo de gerenciamento de projetos.
- ○ A instituição melhora o processo de gerenciamento de projetos com base nas mensurações internas e nas melhores práticas de mercado.

Esta questão busca obter informações sobre o nível de maturidade do processo de gerenciamento de projetos da organização. [20]

7.5 Quais os cinco projetos de TI de maior valor orçamentário alocado em 2010?

Nome	Valor total Previsto (em R$)	Data de conclusão prevista	Breve descrição	Programa e ação orçamentária

Esta questão busca identificar os principais projetos de TI da organização e o respectivo volume de recursos alocados. [21]

7.6 A instituição implementou corporativamente os processos de gestão de serviços de TI abaixo relacionados?

Obs: conceitos baseados na biblioteca ITIL v.3

- ☐ gestão de mudanças — ☐ se sim, constituiu um comitê técnico de gestão de mudanças
- ☐ gestão de capacidade
- ☐ gestão de nível de serviço
- ☐ gestão de problemas — ☐ se sim, tem base de conhecimento de apoio à gestão de problemas e incidentes
- ☐ gestão de incidentes
- ☐ gestão de configuração — ☐ se sim, tem base de dados de gestão da configuração do ambiente computacional
- ☐ gestão financeira
- ☐ gestão de disponibilidade
- ☐ gestão de continuidade — ☐ se sim, tem plano de continuidade de negócio em vigor (aprovado e publicado)
- ☐ gestão de liberação

Esta questão busca identificar processos de gestão de serviços de TI implantados na organização. Os processos enumerados acima baseiam-se nas melhores práticas da biblioteca "Information Technology Infrastructure Library – ITIL". [22]

7.7 Em relação à gestão de nível de serviço de TI:

- ○ Não há um portfólio formal (aprovado e publicado) dos serviços oferecidos aos clientes.
- ○ Há um portfólio formal e atualizado dos serviços oferecidos aos clientes.
- ○ Além do item anterior, os níveis dos serviços oferecidos nesse portfólio são monitorados pela área de TI.
- ○ Além do item anterior, são feitos Acordos de Nível de Serviço (ANS) formais com as áreas de negócio clientes.
- ○ Além do item anterior, os ANS são monitorados formalmente e seus resultados relatados periodicamente aos clientes.
- ○ Além do item anterior, os resultados do monitoramento são usados para melhorar os ANS.

Esta questão busca obter informações sobre o nível de maturidade do processo de gestão de Nível de Serviço praticado com os clientes internos da organização. [23]

7.8 Em relação às contratações de serviços de TI:

Use a seguinte escala: (1) nunca; (2) às vezes; (3) usualmente; (4) sempre.

_____ nos autos são explicitadas as necessidades de negócio que se pretende atender com a contratação.
_____ nos autos são explicitados os indicadores dos benefícios de negócio que serão alcançados.
_____ nos autos são feitos estudos técnicos preliminares para avaliar a viabilidade da contratação.
_____ a análise dos benefícios reais já obtidos é usado como critério para prorrogar ou não o contrato.

Esta questão busca verificar a frequência em que são realizados levantamentos prévios das necessidades de negócio, de benefícios resultantes e de análises de viabilidade nas contratações de TI. [24]

7.9 Em relação às licitações de TI publicadas em 2009:

_____ número total de licitações de TI.
_____ número de licitações por pregão presencial.
_____ número de licitações por pregão eletrônico.
_____ número de adesões (em 2009) a atas de registro de preço licitadas (em 2009 ou 2008) e gerenciadas por outras instituições ("carona").
_____ número de participações (desde o planejamento) em registro de preço licitadas (em 2009) e gerenciados por outras instituições (participante).
_____ número de licitações para registro de preço que licitou (em 2009) e gerenciou e nas quais havia outras instituições participantes desde o planejamento da licitação ("RP conjunto").
_____ número de licitações para registro de preço que licitou (em 2009) e gerenciou e nas quais NÃO havia outras instituições participantes desde o planejamento da licitação ("RP solitário"), com ou sem "caronas".

☐ houve licitação em que a empresa mais bem classificada era estrangeira e veio a perder o certame por causa do exercício do direito de preferência em favor de licitante concorrente (art. 5º do Decreto nº 1.070/1994).

Esta questão busca verificar de que forma a organização tem contratado bens e serviços de TI, em especial no que se refere a licitações por pregão e registro de preços.

7.10 Em relação à fase de planejamento da contratação em TI, em qual das descrições abaixo a instituição se encaixa melhor?

- ○ As contratações de TI são feitas conforme os procedimentos legais e à medida que as demandas vão surgindo.
- ○ Além dos procedimentos legais, há alguns procedimentos internos que auxiliam na padronização do processo de planejamento das contratações.
- ○ Além dos procedimentos legais, há um processo de trabalho para planejar as contratações de TI, publicado como norma própria e de cumprimento obrigatório.
- ○ Além do item anterior, o cumprimento do processo de planejamento da contratação é medido e controlado.
- ○ Além do item anterior, o processo de planejamento é melhorado com base nas mensurações obtidas.

Esta questão busca obter informações sobre o nível de maturidade do processo de contratação de bens e serviços de TI da organização. [25]

7.11 Em relação à fase de gestão dos contratos de TI, em qual das descrições abaixo a instituição se encaixa melhor?

- ○ As diretrizes legais são observadas, mas há grande variação nos procedimentos adotados.
- ○ As diretrizes legais são observadas e os procedimentos reconhecidos como boas práticas são disseminados internamente e praticados.
- ○ Além do item anterior, o processo de gestão de contratos é formalizado (aprovado e publicado) em norma própria e de cumprimento obrigatório.
- ○ Além do item anterior, o cumprimento do processo de gestão de contratos publicado é medido e controlado.
- ○ Além do item anterior, o processo de gestão de contratos é melhorado com base nas mensurações obtidas.

Esta questão busca obter informações sobre o nível de maturidade do processo de **gestão de contratos** de TI da organização. [26]

7.12 Em relação aos papéis “gestor de contrato” e “fiscal de contrato” de serviços de TI:

- ○ esses papéis são distintos um do outro
- ○ esses papéis são considerados equivalentes

Questão	Gestor	Fiscal
Há norma interna que define as atribuições do papel?	☐	☐
É designado formalmente?	☐	☐
São designadas somente pessoas treinadas para o papel?	☐	☐
Há programa de capacitação específico para o exercício do papel?	☐	☐
Há algum tipo de compensação financeira adicional pelo exercício do papel?	☐	☐

Esta questão busca verificar como a instituição interpreta e trata os papéis “gestor de contrato” e “fiscal de contrato” de serviços de TI. [27]

7.13 Em relação à gestão de contratos de serviços de TI, de quem é a responsabilidade por:

Questão	Área de negócio	Área adminis-trativa	Área de TI	Outro
monitorar a execução contratual do ponto de vista de resultados de negócio?	☐	☐	☐	☐
monitorar o cumprimento das cláusulas contratuais e das obrigações fiscais, comerciais, trabalhistas e previdenciárias?	☐	☐	☐	☐
monitorar a execução técnica dos serviços contratados?	☐	☐	☐	☐
gerir o contrato com base em resultados (Decreto nº 2.271/1997, art. 6º)?	☐	☐	☐	☐
acompanhar e fiscalizar o contrato (Lei nº 8.666/1993, art. 67)?	☐	☐	☐	☐

Esta questão busca identificar qual área da organização é responsável por monitorar diferentes aspectos da execução contratual de serviços de TI. Como exemplo de monitoramento negocial, temos: quais módulos de um sistema devem ter a implementação priorizada? Como exemplo de monitoramento técnico temos: contagem de pontos de função de módulos de sistema desenvolvidos. [28]

7.14 Quais fontes de informação sobre preços a instituição utiliza?

Use a seguinte escala: (1) nunca; (2) às vezes; (3) usualmente; (4)sempre

Fontes		Em contratações	Em prorrogações	Em repactuações
Cotação de preços junto aos fornecedores		____	____	____
Preços em contratações similares de outras instituições públicas		____	____	____
Tabelas de preços divulgadas na mídia especializada		____	____	____
Pesquisa em sítios de compras eletrônicas governamentais		____	____	____
Atas de registro de preço em vigor		____	____	____
Consulta a sítios de fornecedores na Internet		____	____	____
Outras.Quais?	_____	____	____	____
	_____	____	____	____
	_____	____	____	____

Esta questão busca identificar quais fontes de informação são utilizadas pelo órgão/entidade para realizar estimativas de preços na contratação de bens e serviços de TI, bem como nas prorrogações e repactuações contratuais. [29]

7.15 Em relação à orçamentação e à execução da despesa de TI:

- ☐ A solicitação de orçamento de TI é feita com base na estimativa dos custos das contratações previstas.
- ☐ Há alocação de custos de TI por área de negócio.
- ☐ A execução da despesa de TI é acompanhada pela área de TI.
- ☐ A execução da despesa de TI é acompanhada pela Alta Administração da instituição.
- ☐ A classificação da despesa de TI é de responsabilidade da área TI.
- ☐ A classificação da despesa de TI é de responsabilidade da área contábil/orçamentária da instituição.
- ☐ A gestão do orçamento de TI é centralizada na área de TI.

Esta questão busca verificar como a organização trata o orçamento, a classificação e execução de despesas relacionadas com TI, bem como identificar a área organizacional responsável por tais atividades. [30]

FUNDAMENTAÇÃO

1

BRASIL. **Decreto nº 5.378, de 23 de fevereiro de 2005.**
Art. 1º Fica instituído o Programa Nacional de Gestão Pública e Desburocratização – GESPÚBLICA, com a finalidade de contribuir para a melhoria da qualidade dos serviços públicos prestados aos cidadãos e para o aumento da competitividade do País. Art. 4o Os critérios para avaliação da gestão de que trata este Decreto serão estabelecidos em consonância com o modelo de excelência em gestão pública.

Brasil. Ministério do Planejamento, Orçamento e Gestão. Secretaria de Gestão. Programa Nacional de Gestão Pública e Desburocratização – GesPública; Prêmio Nacional da Gestão Pública – PQGF; **Instruções para Avaliação da Gestão Pública – 2010**.

2

BRASIL. Tribunal de Contas da União. **Questionário de Governança de TI - 2007.**
Q3. Há comitê que decida sobre a priorização das ações e investimentos de TI? Sim: 32,5%

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. **COBIT - Control Objectives for Information and related Technology. COBIT 4.1.**
p.43. PO4 Definir os processos, organização e os relacionamentos de TI - Uma organização de TI é definida considerando os requisitos de pessoal, habilidades, funções, autoridade, papéis e responsabilidades, rastreabilidade e supervisão. Essa organização deve fazer parte de uma estrutura de processos de TI que assegure transparência e controle, assim como o envolvimento de executivos sênior e a Direção do negócio. Um comitê estratégico deve assegurar a supervisão da Direção de TI, e um ou mais comitês dos quais as áreas de negócio e TI participem devem definir a priorização dos recursos de TI em linha com as necessidades do negócio. Os processos, as políticas administrativas e os procedimentos precisam estar estabelecidos para todas as funções, com especial atenção às de controle, garantia da qualidade, gestão de risco, segurança da informação, propriedade de sistemas e dados e segregação de funções. Para assegurar o rápido atendimento das exigências do negócio, a TI deve ser envolvida nos processos de decisão relevantes.

3

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. **COBIT - Control Objectives for Information and related Technology. COBIT 4.1.**
p.167. ME4 Prover a governança de TI - O estabelecimento de uma efetiva estrutura de governança envolve a definição das estruturas organizacionais, dos processos, da liderança, dos papéis e respectivas responsabilidades para assegurar que os investimentos corporativos em TI estejam alinhados e sejam entregues em conformidade com as estratégias e os objetivos da organização.
p. 155. ME1 Monitorar e Avaliar o Desempenho de TI - A gestão eficaz de desempenho de TI exige um processo de monitoramento. Esse processo inclui a definição de indicadores de desempenho relevantes, informes de desempenho sistemáticos e oportunos e uma pronta ação em relação aos desvios encontrados. O monitoramento é necessário para assegurar que as atividades corretas estejam sendo feitas e que estejam em alinhamento com as políticas e diretrizes estabelecidas.

4

BRASIL. Tribunal de Contas da União. **Questionário de Governança de TI - 2007.**
Q5. Há funções comissionadas de direção e assessoramento na área de TI? Sim: 88,6%
Q6. Esse Órgão/Entidade conhece o grau de formação das pessoas que atuam na área de TI? Sim: 94,9%
Q7. Há carreiras específicas para a área de TI no plano de cargos do Órgão/Entidade? Sim: 43,1%
Q8. São consideradas as competências gerenciais, técnicas e resultados produzidos anteriormente na seleção de pessoas para funções comissionadas na área de TI? Sim: 40,0%

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. **COBIT - Control Objectives for Information and related Technology. COBIT 4.1.**
p.58. PO7 Gerenciar os Recursos Humanos de TI. PO7.2 Competências Pessoais - Verificar regularmente se o pessoal tem as competências necessárias para exercer suas funções com base na formação, no treinamento e/ou na experiência. Definir os requisitos centrais de competência em TI e verificar se estão sendo mantidos através de programas de

qualificação e certificação onde apropriado. PO7.4 Treinamento do Pessoal - Prover ao pessoal de TI treinamento apropriado para manter conhecimento, especializações, habilidades, conscientização sobre controles internos e segurança no nível exigido para atingir os objetivos organizacionais.

5

BRASIL. Tribunal de Contas da União. **Questionário de Governança de TI - 2007.**
Q38. O Órgão/Entidade possui equipe própria para realizar auditorias de TI? Sim: 18,8%
Q39. Foi realizada alguma auditoria de TI nos últimos cinco anos no Órgão/Entidade? Sim: 39,6%

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. **COBIT - Control Objectives for Information and related Technology. COBIT 4.1.**
p.159. ME2 Monitorar e avaliar os controles internos - Estabelecer um programa eficaz de controles internos de TI requer um processo de monitoramento bem definido. Esse processo inclui o monitoramento e reporte das exceções de controle, dos resultados de autoavaliação e avaliação de terceiros. Um benefício importante do monitoramento dos controles internos é assegurar uma operação eficaz e eficiente e a conformidade com as leis e os regulamentos aplicáveis.
p.163. ME3 Assegurar a conformidade com requisitos externos - A supervisão eficaz da conformidade requer o estabelecimento de um processo de revisão para assegurar a conformidade com as leis e regulamentações e os requisitos contratuais. Esse processo inclui identificar os requisitos de conformidade, otimizar e avaliar a resposta, assegurar que os requisitos sejam atendidos e integrar os relatórios de conformidade de TI com os das áreas de negócios.

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. **ABNT NBR ISO/IEC 27002:2005 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação**
p. 112. Conformidade com normas e políticas de segurança da informação e conformidade técnica: convém que a segurança dos sistemas de informação seja analisada criticamente a intervalos regulares;

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. **ABNT NBR ISO/IEC 27002:2005 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação**
p.14. Análise crítica independente de segurança da informação: convém que o enfoque da organização para gerenciar a segurança da informação e a sua implementação (...) seja analisado criticamente, de forma independente, a intervalos planejados, ou quando ocorrerem mudanças significativas relativas à implementação da segurança da informação.

6

BRASIL. Tribunal de Contas da União. **Questionário de Governança de TI - 2007.**
Q1. Há planejamento institucional em vigor? Sim: 52,9%

7

BRASIL. Tribunal de Contas da União. **Questionário de Governança de TI - 2007.**
Q2. Há Planejamento Estratégico para a área de TI em vigor? Sim: 40,8%

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. **COBIT - Control Objectives for Information and related Technology. COBIT 4.1.**
p. 32. PO1 Definir um Plano Estratégico de TI - O planejamento estratégico de TI é necessário para gerenciar todos os recursos de TI em alinhamento com as prioridades e estratégias de negócio. A função de TI e as partes interessadas pelo negócio são responsáveis por garantir a otimização do valor a ser obtido do portfólio de projetos e serviços. O plano estratégico deve melhorar o entendimento das partes interessadas no que diz respeito a oportunidades e limitações da TI, avaliar o desempenho atual e esclarecer o nível de investimento requerido. A estratégia e as prioridades de negócio devem ser reletidas nos portfólios e executadas por meio de planos táticos de TI que estabeleçam objetivos concisos, tarefas e planos bem deinidos e aceitos por ambos, negócio e TI.

8

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. **COBIT - Control Objectives for Information and related Technology. COBIT 4.1.**
p. 32. PO1.4 Plano Estratégico de TI - Criar um plano estratégico que defina, em cooperação com as partes interessadas relevantes, como a TI contribuirá com os objetivos estratégicos da organização (metas) e quais os custos e riscos relacionados. Esse plano estratégico deve contemplar como a TI aplicará os programas de investimentos e como dará sustentação à entrega operacional de serviços. O plano deve definir como os objetivos serão atingidos e medidos e deve ser formalmente liberado para implementação pelas partes interessadas. O plano estratégico de TI deve contemplar o orçamento operacional e de investimento, as fontes de recursos financeiros, a estratégia d fornecimento, a estratégia de aquisição e requisitos legais e regulamentares. O plano estratégico deve ser suficientemente detalhado para possibilitar a definição dos planos táticos de TI.
p. 32. PO1.5 Planos Táticos de TI - Criar um portfólio de planos táticos de TI derivados do plano estratégico de TI. Esses planos táticos devem descrever quais são as iniciativas de TI requeridas, quais os recursos necessários e como o uso de recursos e os benefícios alcançados serão monitorados e administrados. Os planos táticos devem ser suficientemente detalhados de forma a permitir o desenvolvimento de planos de projetos. Gerenciar ativamente o conjunto de planos e iniciativas táticas de TI através de análise do portfólio de projetos e serviços. Isso contempla o acompanhamento frequente de requisitos e recursos, comparando-os ao alcance de metas estratégicas e táticas e os benefícios esperados, e tomando-se as ações apropriadas em caso de desvios.

9

BRASIL. Tribunal de Contas da União. **Questionário de Governança de TI - 2007.**
Q3. Há comitê que decida sobre a priorização das ações e investimentos de TI? (Sim: 32,5%)

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. **COBIT - Control Objectives for Information and related Technology. COBIT 4.1.**
p.43. PO4 Definir os processos, organização e os relacionamentos de TI - Uma organização de TI é definida considerando os requisitos de pessoal, habilidades, funções, autoridade, papéis e responsabilidades, rastreabilidade e supervisão. Essa organização deve fazer parte de uma estrutura de processos de TI que assegure transparência e controle, assim como o envolvimento de executivos sênior e a Direção do negócio. Um comitê estratégico deve assegurar a supervisão da Direção de TI, e um ou mais comitês dos quais as áreas de negócio e TI participem devem definir a priorização dos recursos de TI em linha com as necessidades do negócio. Os processos, as políticas administrativas e os procedimentos precisam estar estabelecidos para todas as funções, com especial atenção às de controle, garantia da qualidade, gestão de risco, segurança da informação, propriedade de sistemas e dados e segregação de funções. Para assegurar o rápido atendimento das exigências do negócio, a TI deve ser envolvida nos processos de decisão relevantes.
p. 49. PO5 Gerenciar o Investimento de TI - Estabelecer e manter uma estrutura para gerenciar os programas de investimentos em TI que contemple custos, benefícios, prioridade dentro do orçamento, um processo formal de definição orçamentária e gerenciamento de acordo com o orçamento. As partes interessadas são consultadas para identiicar e controlar os custos totais e os benefícios dentro dos contextos estratégicos e táticos da TI e iniciar ações de correção quando necessário. O processo promove a parceria entre a TI e as partes interessadas do negócio, permite o uso eficaz e eficiente dos recursos de TI, provê transparência, atribui responsabilidade pelo custo total de propriedade (TCO, Total Cost of Ownership), realização dos benefícios do negócio e do retorno sobre os investimentos em TI.p.167. ME4 Prover a governança de TI - O estabelecimento de uma efetiva estrutura de governança envolve a definição das estruturas organizacionais, dos processos, da liderança, dos papéis e respectivas responsabilidades para assegurar que os investimentos corporativos em TI estejam alinhados e sejam entregues em conformidade com as estratégias e os objetivos da organização.

10

BRASIL. **Decreto nº 6.932, de 11 de agosto de 2009.**
Art. 11. Os órgãos e entidades do Poder Executivo Federal que prestam serviços diretamente ao cidadão deverão elaborar e divulgar "Carta de Serviços ao Cidadão", no âmbito de sua esfera de competência. § 1o A Carta de Serviços ao Cidadão tem por objetivo informar o cidadão dos serviços prestados pelo órgão ou entidade, das formas de acesso a esses serviços e dos respectivos compromissos e padrões de qualidade de atendimento ao público.

Brasil. Ministério do Planejamento, Orçamento e Gestão. Secretaria de Gestão. Programa Nacional de Gestão Pública e Desburocratização – **GESPÚBLICA; Prêmio Nacional da Gestão Pública – PQGF; Carta de Serviços ao Cidadão**; Brasília; MP, SEGES, 2009. Versão 1/2009.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. Secretaria de Gestão**. Instrução Normativa nº 1, de 6 de janeiro de 2010**.
Art. 5º A elaboração das Cartas de Serviços ao Cidadão ocorrerá em articulação com o planejamento estratégico do órgão ou entidade, com mobilização, sensibilização e capacitação dos servidores para sua adequada implementação e desenvolvimento das ferramentas logísticas e de tecnologia da informação.

11

BRASIL. Ministério do Planejamento, Orçamento e Gestão. **Instrução Normativa SLTI/MPOG nº 01, de 19 DE JANEIRO DE 2010.** Publicada no DOU de 20/01/2010.
Art. 5º Os órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional, quando da aquisição de bens, poderão exigir os seguintes critérios de sustentabilidade ambiental: I - que os bens sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme ABNT NBR - 15448-1 e 15448-2; II - que sejam observados os requisitos ambientais para a obtenção de certificação do Instituto Nacional de Metrologia, Normalização e Qualidade Industrial - INMETRO como produtos sustentáveis ou de menor impacto ambiental em relação aos seus similares; III - que os bens devam ser, preferencialmente, acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento; e IV - que os bens não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenil-polibromados (PBBs), éteres difenilpolibromados (PBDEs).

Art. 6º Os editais para a contratação de serviços deverão prever que as empresas contratadas adotarão as seguintes práticas de sustentabilidade na execução dos serviços, quando couber: I - use produtos de limpeza e conservação de superfícies e objetos inanimados que obedeçam às classificações e especificações determinadas pela ANVISA; II - adote medidas para evitar o desperdício de água tratada, conforme instituído no Decreto nº 48.138, de 8 de outubro de 2003; III - Observe a Resolução CONAMA nº 20, de 7 de dezembro de 1994, quanto aos equipamentos de limpeza que gerem ruído no seu funcionamento; IV - forneça aos empregados os equipamentos de segurança que se fizerem necessários, para a execução de serviços; V - realize um programa interno de treinamento de seus empregados, nos três primeiros meses de execução contratual, para redução de consumo de energia elétrica, de consumo de água e redução de produção de resíduos sólidos, observadas as normas ambientais vigentes; VI - realize a separação dos resíduos recicláveis descartados pelos órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional, na fonte geradora, e a sua destinação às associações e cooperativas dos catadores de materiais recicláveis, que será procedida pela coleta seletiva do papel para reciclagem, quando couber, nos termos da IN/MARE nº 6, de 3 de novembro de 1995 e do Decreto nº 5.940, de 25 de outubro de 2006; VII - respeite as Normas Brasileiras - NBR publicadas pela Associação Brasileira de Normas Técnicas sobre resíduos sólidos; e VIII - preveja a destinação ambiental adequada das pilhas e baterias usadas ouinservíveis, segundo disposto na Resolução CONAMA nº 257, de 30 de junho de 1999.

12

BRASIL. Tribunal de Contas da União. **Questionário de Governança de TI - 2007.**
Q20. O Órgão/Entidade possui e mantém inventário dos principais sistemas informatizados e suas bases de dados? (Sim: 85,9%).

13

BRASIL. Tribunal de Contas da União. **Questionário de Governança de TI - 2007.**
Q5. Há funções comissionadas de direção e assessoramento na área de TI? Sim: 88,6%
Q7. Há carreiras específicas para a área de TI no plano de cargos do Órgão/Entidade? Sim: 43,1%

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. **COBIT - Control Objectives for Information and related Technology. COBIT 4.1.**

p.57. PO7 Gerenciar os recursos humanos de TI - Adquirir, manter e motivar uma força de trabalho competente para criar e entregar serviços de TI para o negócio. Isso é alcançado seguindo práticas definidas e acordadas de recrutamento, treinamento, avaliação de desempenho, promoção e desligamento. Esse processo é crítico porque as pessoas são ativos importantes e a governança e o ambiente de controle de dados são altamente dependentes da motivação e da competência dessas pessoas.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. SLTI. **Instrução Normativa nº 4, de 19 de maio de 2008.**
Art. 5º Não poderão ser objeto de contratação:
(...) III - gestão de processos de Tecnologia da Informação, incluindo gestão de segurança da informação.

14

BRASIL. Tribunal de Contas da União. **Questionário de Governança de TI - 2007.**
Q7. Há carreiras específicas para a área de TI no plano de cargos do Órgão/Entidade? Sim: 43,1%

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. **COBIT - Control Objectives for Information and related Technology. COBIT 4.1.**
p.57. PO7 Gerenciar os recursos humanos de TI - Adquirir, manter e motivar uma força de trabalho competente para criar e entregar serviços de TI para o negócio. Isso é alcançado seguindo práticas definidas e acordadas de recrutamento, treinamento, avaliação de desempenho, promoção e desligamento. Esse processo é crítico porque as pessoas são ativos importantes e a governança e o ambiente de controle de dados são altamente dependentes da motivação e da competência dessas pessoas.

15

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. **COBIT - Control Objectives for Information and related Technology. COBIT 4.1.**
p.57 PO7 Gerenciar os recursos humanos de TI (Adquirir, manter e motivar uma força de trabalho competente para criar e entregar serviços de TI para o negócio. Isso é alcançado seguindo práticas definidas e acordadas de recrutamento, treinamento, avaliação de desempenho, promoção e desligamento. Esse processo é crítico porque as pessoas são ativos importantes e a governança e o ambiente de controle de dados são altamente dependentes da motivação e da competência dessas pessoas.)

16

BRASIL. Tribunal de Contas da União. **Questionário de Governança de TI - 2007.**
Q5. Há funções comissionadas de direção e assessoramento na área de TI? Sim: 88,6%
Q6. Esse Órgão/Entidade conhece o grau de formação das pessoas que atuam na área de TI? Sim: 94,9%
Q8. São consideradas as competências gerenciais, técnicas e resultados produzidos anteriormente na seleção de pessoas para funções comissionadas na área de TI? Sim: 40,0%

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. **COBIT - Control Objectives for Information and related Technology. COBIT 4.1.**
p.57. PO7 Gerenciar os recursos humanos de TI - Adquirir, manter e motivar uma força de trabalho competente para criar e entregar serviços de TI para o negócio. Isso é alcançado seguindo práticas definidas e acordadas de recrutamento, treinamento, avaliação de desempenho, promoção e desligamento. Esse processo é crítico porque as pessoas são ativos importantes e a governança e o ambiente de controle de dados são altamente dependentes da motivação e da competência dessas pessoas.

17

BRASIL. Tribunal de Contas da União. **Questionário de Governança de TI - 2007.**
Q12. É feita classificação de informações? (Sim: 20,0%)
Q13. É efetuada Análise de Riscos na área de TI? (Sim: 24,7%)
Q15. Existe uma área específica para gerência de incidentes de segurança? (Sim: 24,3%)
Q20. O Órgão/Entidade possui e mantém inventário dos principais sistemas informatizados e suas bases de dados? (Sim: 85,9%)

BRASIL. Associação Brasileira de Normas Técnicas - **ABNT. ABNT NBR ISO/IEC 27002:2005 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação**
p.21. Inventário dos ativos - Convém que todos os ativos sejam claramente identificados e um inventário de todos os ativos importantes seja estruturado e mantido.
p.23. Convém que a informação seja classificada para indicar a necessidade, prioridades e o nível esperado de proteção quando do tratamento da informação. A informação possui vários níveis de sensibilidade e criticidade. Alguns itens podem necessitar um nível adicional de proteção ou tratamento especial. Convém que um sistema de classificação da informação seja usado para definir um conjunto apropriado de níveis de proteção e determinar a necessidade de medidas especiais de tratamento.
p.6. Convém que as análises/avaliações de riscos identifiquem, quantifiquem e priorizem os riscos com base em critérios para aceitação dos riscos e dos objetivos relevantes para a organização. Convém que os resultados orientem e determinem as ações de gestão apropriadas e as prioridades para o gerenciamento dos riscos de segurança da informação, e para a implementação dos controles selecionados, de maneira a proteger contra estes riscos.
p.98. Convém que os eventos de segurança da informação sejam relatados através dos canais apropriados da direção, o mais rapidamente possível. Convém que um procedimento de notificação formal seja estabelecido para relatar os eventos de segurança da informação, junto com um procedimento de resposta a incidente e escalonamento, estabelecendo a ação a ser tomada ao se receber a notificação de um evento de segurança da informação. Convém que um ponto de contato seja estabelecido para receber as notificações dos eventos de segurança da informação. Convém que este ponto de contato seja de conhecimento de toda a organização e esteja sempre disponível e em condições de assegurar uma resposta adequada e oportuna.

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. **ABNT NBR ISO/IEC 27001:2006 - Tecnologia da Informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos**
p.3. integridade - propriedade de salvaguarda da exatidão e completeza de ativos.
p.2. Confidencialidade - propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.
p.2. Disponibilidade - propriedade [da informação] *de estar acessível e utilizável sob demanda por uma entidade autorizada.*

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. **ABNT NBR ISO/IEC 27002:2005 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação**
p.2. incidente de segurança da informação - um incidente de segurança da informação é indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação

18

BRASIL. Tribunal de Contas da União. **Questionário de Governança de TI - 2007.**
Q11. Existe Política de Segurança da Informação (PSI) em vigor? ? (Sim: 36,1%)
Q10. Existe Plano de Continuidade de Negócios em vigor? (Sim: 12,2%)

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. **ABNT NBR ISO/IEC 27002:2005 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação**
p.8. Política de Segurança da Informação - Documento que declara o comprometimento da direção e estabeleça o enfoque da organização para gerenciar a segurança da informação (...) Convém que um documento da política de segurança da informação seja aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes.
p.10. Convém que uma estrutura de gerenciamento seja estabelecida para iniciar e controlar a implementação da segurança da informação dentro da organização. Convém que a direção aprove a política de segurança da informação, atribua as funções da segurança, coordene e analise criticamente a implementação da segurança da informação por toda a organização

19

BRASIL. Tribunal de Contas da União. **Questionário de Governança de TI - 2007.**
Q19. O desenvolvimento de sistemas segue alguma metodologia? (Sim: 49,0%)

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. **ABNT NBR ISO/IEC 15504-2:2008 - Tecnologia da Informação - Avaliação de Processo - Parte 2: Realização de uma Avaliação**
p.6 a 9. Uma Estrutura de Medição para a Capacidade de processo - Esta seção da ABNT NBR ISO/IEC 15504-2 define uma estrutura de medição para a avaliação da capacidade de processo. A capacidade de processo é definida em uma escala ordinal de seis pontos (...) Nível 0: Processo incompleto - O processo não está implementado ou não atinge o seu propósito. Nível 1: Processo executado - O processo implementado atinge o seu propósito. Nível 2: Processo gerenciado - O processo executado, descrito anteriormente, agora é implementado de forma gerenciada, monitorada e ajustada e seus produtos de trabalho são estabelecidos, controlados e mantidos apropriadamente. Nível 3: Processo estabelecido - O Processo Gerenciado, descrito anteriormente, agora é implementado utilizando um processo definido capaz de atingir seus resultados. Nível 4: Processo previsível - O processo estabelecido, descrito anteriormente, agora opera dentro de limites definidos para atingir seus resultados. Nível 5: Processo em otimização - O processo previsível, descrito anteriormente, é melhorado continuamente para atingir metas de negócio relevantes, atuais e projetadas.

BRASIL. Softex. MPS.BR - **Melhoria de Processo do Software Brasileiro - Guia Geral**. 2009.
p. 6. O modelo MPS baseia-se nos conceitos de maturidade e capacidade de processo para a avaliação e melhoria da qualidade e produtividade de produtos de software e serviços correlatos.
p. 16. Os níveis de maturidade estabelecem patamares de evolução de processos, caracterizando estágios de melhoria da implementação de processos na organização. O nível de maturidade em que se encontra uma organização permite prever o seu desempenho futuro ao executar um ou mais processos. O MR-MPS define sete níveis de maturidade: A (Em Otimização), B (Gerenciado Quantitativamente), C (Definido), D (Largamente Definido), E (Parcialmente Definido), F (Gerenciado) e G (Parcialmente Gerenciado). A escala de maturidade se inicia no nível G e progride até o nível A.

WIKIPEDIA.**Capability Maturity Model.**
The Capability Maturity Model (CMM) was originally developed as a tool for objectively assessing the ability of government contractors' processes to perform a contracted software project. (…) There are five levels defined along the continuum of the CMM (…) 1. Initial (chaotic, ad hoc, individual heroics) - the starting point for use of a new process. 2. Managed - the process is managed according to the metrics described in the Defined stage. 3. Defined - the process is defined/confirmed as a standard business process, and decomposed to levels 0, 1 and 2 (the latter being Work Instructions). 4. Quantitatively managed. 5. Optimized - process management includes deliberate process optimization/improvement.

20

WIKIPEDIA. **Projeto.**
Um projeto é um esforço temporário empreendido para criar um produto, serviço ou resultado exclusivo. Os projetos e as operações diferem, principalmente, no fato de que os projetos são temporários e exclusivos, enquanto as operações são contínuas e repetitivas.

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. **COBIT - Control Objectives for Information and related Technology. COBIT 4.1.**
p.69. PO10 Gerenciar projetos - Estabelecer um programa e uma estrutura de gestão de projeto para o gerenciamento de todos os projetos de TI. Essa estrutura deve assegurar a correta priorização e a coordenação de todos os projetos. A estrutura deve incluir um plano mestre, atribuição de recursos, definição dos resultados a serem entregues, aprovação dos usuários, uma divisão por fases de entrega, garantia da qualidade, um plano de teste formal e uma revisão pós-implementação para assegurar a gestão de risco do projeto e a entrega de valor para o negócio. Esta abordagem reduz o risco de custos inesperados e de cancelamentos de projeto, aperfeiçoa a comunicação, melhora o envolvimento das áreas de negócio e dos usuários finais, assegura o valor e a qualidade dos resultados do projeto e maximiza a contribuição para os programas de investimentos em TI.

PMI. **A Guide to the Project Management Body of Knowledge (PMBOK Guide).**

21

BRASIL. Tribunal de Contas da União. **Questionário de Governança de TI - 2007.**
Q37. Ao longo do exercício financeiro há controle dos gastos e da disponibilização orçamentária? (Sim: 82,0%)

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. **COBIT - Control Objectives for Information and related Technology. COBIT 4.1.**
p.123. DS6 Identificar e alocar custos - A necessidade de um sistema justo e equitativo de alocação de custo de TI para o negócio requer avaliação precisa dos custos de TI e acordo com os usuários do negócio sobre uma alocação razoável. Este processo contempla a construção e a operação de um sistema para capturar, alocar e reportar os custos de TI aos usuários dos serviços. Um sistema de alocação justo permite à empresa tomar decisões mais embasadas sobre o uso dos serviços.

22

BRASIL. Tribunal de Contas da União. **Questionário de Governança de TI - 2007.**
Q10. Existe Plano de Continuidade de Negócios em vigor? (Sim: 12,2%)
Q13. É efetuada Análise de Riscos na área de TI? (Sim: 24,7%)
Q14. Existem procedimentos definidos que disciplinem o controle de acesso (lógico e físico) a recursos computacionais? (Caso a resposta seja "Sim", anexar procedimento) (Sim: 51,8%)
Q15. Existe uma área específica para gerência de incidentes de segurança? (Sim: 24,3%)
Q17. É efetuada a gestão de mudanças? (Sim: 12,2%)
Q18. É efetuada a gestão de capacidade e compatibilidade das soluções de TI do Órgão/Entidade? (Sim: 15,7%)
Q21. É efetuada a gestão de acordos de níveis de serviço das soluções de TI do Órgão/Entidade oferecidas aos seus clientes? (Sim: 10,6%)
Q22. É efetuada a gestão dos níveis de serviço acordados para os serviços de TI prestados ao Órgão/Entidade? (Sim: 25,9%)
Q24. Na elaboração do projeto básico das contratações de TI é feita análise de custo/benefício da solução a ser contratada? (Sim: 52,5%)
Q25. Na elaboração do projeto básico das contratações de TI são explicitados os benefícios da contratação em termos de negócio do Órgão/Entidade e não somente em termos de TI? (Sim: 60,0%)
Q37. Ao longo do exercício financeiro há controle dos gastos e da disponibilização orçamentária? (Sim: 82,0%)

itSMF. The IT Service Managent Forum. **An Introductory Overview of ITIL V3.**

WIKIPEDIA. **Information Technology Infrastructure Library.**

23

BRASIL. Tribunal de Contas da União. **Questionário de Governança de TI - 2007.**
Q21. É efetuada a gestão de acordos de níveis de serviço das soluções de TI do Órgão/Entidade oferecidas aos seus clientes? (Sim: 10,6%)

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. **COBIT - Control Objectives for Information and related Technology. COBIT 4.1.**
p.32. PO1.1 Gerenciamento de Valor da TI - Trabalhar com a Direção do Negócio para assegurar que o portfólio de investimentos em TI da empresa contenha programas baseados em sólidos estudos de caso de negócio. Reconhecer que há investimentos obrigatórios, sustentáveis e discricionários que diferem em complexidade e grau de liberdade na alocação de fundos. Os processos de TI devem prover a entrega eficaz e eficiente dos componentes de TI e prévia advertência de qualquer desvio do plano, incluindo custo, cronograma ou funcionalidade, que possa afetar os resultados esperados dos programas. Os serviços de TI devem ser executados em conformidade com acordos de níveis de serviço (service level agreeement, SLA) equilibrados e controláveis. A responsabilidade pelo alcance dos benefícios e o controle dos custos deve ser claramente atribuída e monitorada. Estabelecer avaliação adequada, transparente, repetível e comparável de estudos de caso de negócio, incluindo valor financeiro, o risco de não fornecer uma capacidade e o risco de não atingir os benefícios esperados.
p.32. PO1.6 Gerenciamento do Portfólio de TI - Gerenciar ativamente com as áreas de negócio o portfólio dos programas de investimentos de TI necessários para atingir os objetivos estratégicos específicos de negócio, através de identificação,

definição, avaliação, priorização, seleção, início, gerenciamento e controle de programas. Isso inclui esclarecer os resultados de negócio desejados, assegurar que os objetivos do programa sustentem o alcance dos resultados, entender o escopo completo do esforço necessário para atingir os resultados, atribuir responsabilidades com medidas de suporte, definir projetos dentro do programa, alocar recursos e fundos, delegar autoridade e atribuir responsabilidades pelos projetos no lançamento do programa.
p.103. DS1 Definir e Gerenciar Níveis de Serviço - A comunicação eficaz entre a Direção de TI e os clientes de negócio sobre os serviços necessários é possibilitada por um acordo definido e documentado que aborda os serviços de TI e os níveis de serviço esperados. Este processo também inclui monitoramento e relatório oportuno às partes interessadas quanto ao atendimento dos níveis de serviço. Este processo permite o alinhamento entre os serviços de TI e os respectivos requisitos do negócio.

24

BRASIL. Tribunal de Contas da União. **Questionário de Governança de TI - 2007.**
Q24. Na elaboração do projeto básico das contratações de TI é feita análise de custo/benefício da solução a ser contratada? (Sim: 52,5%)
Q25. Na elaboração do projeto básico das contratações de TI são explicitados os benefícios da contratação em termos de negócio do Órgão/Entidade e não somente em termos de TI? (Sim: 60,0%)

BRASIL. Ministério do Planejamento, Orçamento e Gestão. SLTI. **Instrução Normativa nº 4, de 19 de maio de 2008.**
Art. 3º As contratações de que trata esta Instrução Normativa deverão ser precedidas de planejamento, elaborado em harmonia com o Plano Diretor de Tecnologia da Informação - PDTI, alinhado à estratégia do órgão ou entidade.
Art. 9º A fase de Planejamento da Contratação consiste nas seguintes etapas: I - Análise de Viabilidade da Contratação; II - Plano de Sustentação; III - Estratégia de Contratação; e IV - Análise de Riscos.
Art. 16. A Análise de Riscos deverá ser elaborada pelo Gestor do Contrato, com o apoio da Área de Tecnologia da Informação e do Requisitante do Serviço, observando o seguinte(...)

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. **COBIT - Control Objectives for Information and related Technology. COBIT 4.1.**
p.75. AI1 Identificar Soluções Automatizadas - A necessidade de uma nova aplicação ou função requer uma análise prévia à aquisição ou ao desenvolvimento para assegurar que os requisitos de negócio sejam atendidos através de uma abordagem eficaz e eficiente. Este processo contempla a definição das necessidades, considera fontes alternativas, a revisão de viabilidade econômica e tecnológica, a execução das análises de risco e de custo-benefício e a obtenção de uma decisão final por "desenvolver" ou "comprar". Todos esses passos permitem às organizações minimizar os custos de aquisição e implementação de soluções e permitem ao negócio alcançar seus objetivos.
p.79. AI2 Adquirir e manter software aplicativo - As aplicações devem ser disponibilizadas em alinhamento com os requisitos do negócio. Este processo contempla o projeto das aplicações, a inclusão de controles e requisitos de segurança apropriados, o desenvolvimento e a configuração de acordo com padrões. Isso permite às organizações apoiarem de forma adequada as operações do negócio com as aplicações corretas.

25

BRASIL. Tribunal de Contas da União. **Questionário de Governança de TI - 2007.**
Q23. O Órgão/Entidade adota processo de trabalho formal na contratação de bens e serviços de TI ? (Sim: 54,1%)

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. **COBIT - Control Objectives for Information and related Technology. COBIT 4.1.**
p.83. AI3 Adquirir e manter infraestrutura de tecnologia - As organizações devem ter processos de aquisição, implementação e atualização da infraestrutura de tecnologia. Isso requer uma abordagem planejada de aquisição, manutenção e proteção da infraestrutura em alinhamento com as estratégias tecnológicas acordadas e o fornecimento de ambientes de desenvolvimento e teste. Isso assegura um apoio tecnológico contínuo às aplicações de negócio.
p.91. AI5 Adquirir recursos de TI - Recursos de TI, incluindo pessoas, hardware, software e serviços precisam ser adquiridos. Isso requer a definição e a aplicação de procedimentos de aquisição, a seleção de fornecedores, o estabelecimento de arranjos contratuais e a aquisição propriamente dita. Assim assegura-se que a organização tenha todos os recursos de TI necessários a tempo e com boa relação custo-benefício.

26

BRASIL. Tribunal de Contas da União. **Questionário de Governança de TI - 2007.**
Q28. O Órgão/Entidade adota processo de trabalho formal na gestão de contratos de bens e serviços de TI ? (Sim: 45,1%)
Q29. Há designação formal do gestor de cada contrato relativo a bens e serviços de TI? (Sim: 77,6%)
Q30. Há realização de reunião periódica com o contratado para avaliar o andamento de cada contrato relativo a bens e serviços de TI? (Sim: 35,3%)
Q32. A monitoração administrativa dos contratos relativos a bens e serviços de TI é feita pela Área de TI? (Sim: 55,3%)
Q33 É feita monitoração técnica dos contratos relativos a bens e serviços de TI? Quantos funcionários realizam esta atividade? Quantos contratos relativos de bens e serviços de TI estão em vigor? (Sim: 89,8%)
Q34 Há transferência de conhecimento para servidores do Órgão/Entidade referente a produtos e serviços de TI terceirizados? (Sim: 42,7%)

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. **COBIT - Control Objectives for Information and related Technology. COBIT 4.1.**
p.107. DS2 Gerenciar serviços de terceiros - A necessidade de assegurar que os serviços prestados por fornecedores satisfaçam aos requisitos do negócio requer um processo efetivo de gestão da terceirização. Esse processo é realizado definindo-se claramente os papéis, responsabilidades e expectativas nos acordos de terceirização bem como revisando e monitorando tais acordos quanto à efetividade e à conformidade. A gestão eficaz dos serviços terceirizados minimiza os riscos de negócio associados aos fornecedores que não cumprem seu papel.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. SLTI. **Instrução Normativa nº 4, de 19 de maio de 2008.**
Art. 20. A fase de Gerenciamento do Contrato visa acompanhar e garantir a adequada prestação dos serviços durante todo o período de execução do contrato e envolve as seguintes tarefas(...)

27

BRASIL. Tribunal de Contas da União. **Questionário de Governança de TI - 2007.**
Q28. O Órgão/Entidade adota processo de trabalho formal na gestão de contratos de bens e serviços de TI ? (Sim: 45,1%)
Q29. Há designação formal do gestor de cada contrato relativo a bens e serviços de TI? (Sim: 77,6%)
Q30. Há realização de reunião periódica com o contratado para avaliar o andamento de cada contrato relativo a bens e serviços de TI? (Sim: 35,3%)
Q34 Há transferência de conhecimento para servidores do Órgão/Entidade referente a produtos e serviços de TI terceirizados? (Sim: 42,7%)

28

BRASIL. Tribunal de Contas da União. **Questionário de Governança de TI - 2007.**
Q32. A monitoração administrativa dos contratos relativos a bens e serviços de TI é feita pela Área de TI? (Sim: 55,3%)
Q33 É feita monitoração técnica dos contratos relativos a bens e serviços de TI? Quantos funcionários realizam esta atividade? Quantos contratos relativos de bens e serviços de TI estão em vigor? (Sim: 89,8%)

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. **COBIT - Control Objectives for Information and related Technology. COBIT 4.1.**
p.107. DS2 Gerenciar serviços de terceiros - A necessidade de assegurar que os serviços prestados por fornecedores satisfaçam aos requisitos do negócio requer um processo efetivo de gestão da terceirização. Esse processo é realizado definindo-se claramente os papéis, responsabilidades e expectativas nos acordos de terceirização bem como revisando e monitorando tais acordos quanto à efetividade e à conformidade. A gestão eficaz dos serviços terceirizados minimiza os riscos de negócio associados aos fornecedores que não cumprem seu papel.

BRASIL. **Lei nº 8.666, de 21 de junho de 1993**.
Art. 67. A execução do contrato deverá ser acompanhada e fiscalizada por um representante da Administração especialmente designado, permitida a contratação de terceiros para assisti-lo e subsidiá-lo de informações pertinentes a essa atribuição.

BRASIL. **Decreto nº 2.271, de 07 de julho de 1997**.
Art . 6º A administração indicará um gestor do contrato, que será responsável pelo acompanhamento e fiscalização da sua execução, procedendo ao registro das ocorrências e adotando as providências necessárias ao seu fiel cumprimento, tendo por parâmetro os resultados previstos no contrato.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. SLTI. **Instrução Normativa nº 4, de 19 de maio de 2008.**
Art. 20. A fase de Gerenciamento do Contrato visa acompanhar e garantir a adequada prestação dos serviços durante todo o período de execução do contrato e envolve as seguintes tarefas(...)

29

BRASIL. Tribunal de Contas da União. **Questionário de Governança de TI - 2007.**
Q26. O Órgão/Entidade utiliza mais de uma fonte na elaboração da estimativa de preços das licitações de TI? (Sim: 85,1%)

BRASIL. Ministério do Planejamento, Orçamento e Gestão. SLTI. **Instrução Normativa nº 4, de 19 de maio de 2008.**
Art. 14, inc. VI - elaboração, pela área competente, com apoio da Área de Tecnologia da Informação, do orçamento detalhado, fundamentado em pesquisa no mercado, a exemplo de: contratações similares, valores oficiais de referência, pesquisa junto a fornecedores ou tarifas públicas;

30

BRASIL. Tribunal de Contas da União. **Questionário de Governança de TI - 2007.**
Q35. A solicitação do orçamento para a área de TI, encaminhada em 2006, foi feita com base nas ações da área de TI planejada para 2007? (Sim: 61,2%)
Q36. No 1° trimestre de 2007 foi feita a alocação orçamentária às ações constantes do planejamento de TI? (Sim: 49,0%)
Q37. Ao longo do exercício financeiro há controle dos gastos e da disponibilização orçamentária? (Sim: 82,0%)