Referências do Questionário de Governança de TI 2014

ÍNDICE

Objetivo

Este documento apresenta as referências que balizam o questionário de governança de TI 2014, tendo em vista auxiliar nas respostas das organizações e, na medida do possível, orientá-las acerca das atividades que caracterizam a adoção dessas práticas. Essas referências dizem respeito a leis, decretos, resoluções, jurisprudência do TCU, normas técnicas e modelos de boas práticas de governança de TI.

1. Liderança da alta administração

1.1. Com relação à estrutura de governança corporativa:

a. a organização define e comunica formalmente papéis e responsabilidades para a governança corporativa.

b. a organização dispõe de um comitê de direção estratégica formalmente instituído, que auxilia nas decisões relativas às diretrizes, estratégias, políticas e no acompanhamento da gestão institucional.

c. a organização realiza avaliações sobre a definição e compreensão dos papéis e das responsabilidades organizacionais.

d. a organização dispõe de um código de ética formalmente instituído, bem como divulga e monitora o seu cumprimento.

e. a organização dispõe de uma política corporativa de gestão de riscos formalmente instituída, como norma de cumprimento obrigatório.

f. a organização dispõe de uma política corporativa de gestão de continuidade do negócio formalmente instituída, como norma de cumprimento obrigatório.

Referências

BRASIL. Tribunal de Contas da União. Referencial Básico de Governança

p.35 ***COMPONENTE E4. Estrutura de governança*** - ***Prática E4.1****. Estabelecer e manter política de delegação e de reserva de poderes, de forma a assegurar a capacidade de avaliar, dirigir e monitorar a organização.* ***Prática E4.2.*** *Definir os papéis e distribuir as responsabilidades entre os conselhos, a alta administração e a gestão operacional, de modo a garantir o balanceamento de poder e a segregação de funções críticas.* ***Prática E4.3****. Definir, de forma clara, procedimentos e regulamentos afetos a gestão da estrutura interna de governança, bem como os seguintes processos: elaboração, implementação e revisão de políticas; tomada de decisão, monitoramento e controle.* ***Prática E4.4.*** *Definir instâncias internas de apoio à governança e indicar como elas se relacionam com as demais estruturas de governança.*

p.29 ***COMPONENTE L3. Liderança organizacional - Prática L3.1.*** *Avaliar, direcionar e monitorar a gestão da organização, especialmente o alcance de metas institucionais e o comportamento dos membros da alta administração e dos gerentes.* ***Prática L3.2.*** *Definir os papéis e distribuir as responsabilidades entre os membros dos conselhos, da alta administração e os gerentes, de modo a garantir o balanceamento de poder e a segregação de funções críticas.* ***Prática L3.3.*** *Responsabilizar-se, perante as estruturas de governança (internas e externas), pelo estabelecimento de políticas e diretrizes para a gestão da organização e pelo alcance dos resultados previstos.* ***Prática L3.4.*** *Avaliar os resultados das atividades de controle e dos trabalhos de auditoria e garantir que sejam adotadas as providências cabíveis.*

p.36 ***COMPONENTE C1. Gestão de riscos e controle interno - Prática C1.2.*** *Estabelecer política e estrutura integrada de gestão de riscos e controle interno.*

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. ABNT NBR ISO 15999-1:2008 – Gestão de continuidade de negócios – Parte 1: Código de Prática

p.13 ***5.3 Política*** *- A Alta Direção deve definir uma política de continuidade de negócios que a) esteja alinhada com o propósito da organização, b) forneça uma estrutura que estabeleça os objetivos de continuidade de negócios,c) inclua o compromisso de atender aos requisitos aplicáveis, d) inclua o compromisso da melhoria contínua do SGCN [Sistema de Gestão de Continuidade de .*

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. ABNT NBR ISO 31000:2009 – Gestão de riscos – Princípios e diretrizes

p.9 ***4.2 Mandato e comprometimento*** *– [...] Convém que a administração defina e aprove a política de gestão de riscos.*

1.2. Com relação ao sistema de governança de TI:

a. a organização define e comunica formalmente papéis e responsabilidades mais relevantes para a governança e gestão de TI.

b. a organização dispõe de um comitê de TI, formalmente instituído, composto por representantes de áreas relevantes da organização.

c. o comitê de TI realiza as atividades previstas em seu ato constitutivo.

d. a organização prioriza as ações de TI com apoio do comitê de TI (ou colegiado equivalente), que atua como instância consultiva da alta administração.

Referências

Brasil. Tribunal de Contas da União. Acórdão 1.233/2012-TCU-Plenário.

9.2. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, à Secretaria de Logística e Tecnologia da Informação (SLTI/MP) que:

9.2.1 normatize a obrigatoriedade de que os entes sob sua jurisdição estabeleçam comitês de TI, observando as boas práticas sobre o tema, a exemplo do Cobit 4.1, PO4.2 - comitê estratégico de TI e PO4.3 - comitê diretor de TI (subitem II.3);

9.2.9. em atenção ao Decreto-Lei 200/1967, art. 6º, V, estabeleça, normativamente para todos os entes sob sua jurisdição, a obrigatoriedade de a alta administração implantar uma estrutura de controles internos mediante a definição de atividades de controle em todos os níveis da organização para mitigar os riscos de suas atividades, pelo menos nos seguintes processos (subitem II.11):

9.2.9.2. funcionamento dos comitês de TI;

9.11. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, à Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União (CGPAR) que:

9.11.1 normatize a obrigatoriedade de que os entes sob sua jurisdição estabeleçam comitês de TI, observando as boas práticas sobre o tema, a exemplo do Cobit 4.1, PO4.2 - comitê estratégico de TI e PO4.3 - comitê diretor de TI (subitem II.3);

9.11.12. em atenção ao Decreto-Lei 200/1967, art. 6º, V, estabeleça, normativamente para todos os entes sob sua jurisdição, a obrigatoriedade de a alta administração implantar uma estrutura de controles internos mediante a definição de atividades de controle em todos os níveis da organização para mitigar os riscos de suas atividades, pelo menos nos seguintes processos (subitem II.11):

9.11.12.3. funcionamento dos comitês de TI;

9.13. Recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Conselho Nacional da Justiça (CNJ) que:

9.13.14. em atenção ao Decreto-Lei 200/1967, art. 6º, V, estabeleça, normativamente para todos os entes sob sua jurisdição, a obrigatoriedade de a alta administração implantar uma estrutura de controles internos mediante a definição de atividades de controle em todos os níveis da organização para mitigar os riscos de suas atividades, pelo menos nos seguintes processos (subitem II.11):

9.13.14. 3. funcionamento dos comitês de TI;

9.15. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Conselho Nacional do Ministério Público (CNMP) que:

9.15.3. normatize a obrigatoriedade de que os entes sob sua jurisdição estabeleçam comitês de TI, observando as boas práticas sobre o tema, a exemplo do Cobit 4.1, PO4.2 - comitê estratégico de TI e PO4.3 - comitê diretor de TI (subitem II.3);

9.15.18. em atenção ao Decreto-Lei 200/1967, art. 6º, V, estabeleça, normativamente para todos os entes sob sua jurisdição, a obrigatoriedade de a alta administração implantar uma estrutura de controles internos mediante a definição de atividades de controle em todos os níveis da organização para mitigar os riscos de suas atividades, pelo menos, nos seguintes processos (subitem II.11):

9.15.18.3. funcionamento dos comitês de TI.

BRASIL. Associação Brasileira de Normas Técnicas – ABNT. ABNT NBR ISO/IEC 38500:2009 – Governança corporativa de tecnologia da informação.

p.8-9 ***2. ESTRUTURA PARA UMA BOA GOVERNANÇA CORPORATIVA DE TI. 2.2 Modelo. Avaliar –*** *Convém que os dirigentes designem responsabilidade e exijam preparação e implementação dos planos e políticas.*

p.32 ***EDM01.02 Dirigir o sistema de governança. Atividade 2 –*** *Estabelecer ou delegar o estabelecimento de estruturas, processos e práticas de governança em consonância com os princípios acordados.* ***Atividade 3 –*** *Alocar*

responsabilidade, autoridade e obrigação de prestar contas em consonância com os princípios de governança, os modelos de tomada de decisão e as delegações (tradução livre).

1.3. Com relação à entrega de resultado da TI:

a. a organização define formalmente diretrizes para o planejamento de TI.

b. a organização define formalmente diretrizes para gestão do portfólio de projetos e serviços de TI, inclusive para definição de critérios de priorização e de alocação orçamentária.

c. a organização define formalmente diretrizes para contratação de bens e serviços de TI.

d. a organização define formalmente diretrizes para avaliação do desempenho dos serviços de TI.

Referências

Brasil. Tribunal de Contas da União. Acórdão 1.603/2008-TCU-Plenário.

9.1. recomendar ao Conselho Nacional de Justiça - CNJ e ao Conselho Nacional do Ministério Público - CNMP que, nos órgãos integrantes da estrutura do Poder Judiciário Federal e do Ministério Público da União, respectivamente:

9.1.1. promovam ações com o objetivo de disseminar a importância do planejamento estratégico, procedendo, inclusive mediante orientação normativa, ações voltadas à implantação e/ou aperfeiçoamento de planejamento estratégico institucional, planejamento estratégico de TI e comitê diretivo de TI, com vistas a propiciar a alocação dos recursos públicos conforme as necessidades e prioridades da organização;

9.4. recomendar ao Ministério do Planejamento, Orçamento e Gestão - MPOG que, nos órgãos/entidades da Administração Pública Federal:

9.4.1. promova ações com o objetivo de disseminar a importância do planejamento estratégico, procedendo, inclusive mediante orientação normativa, à execução de ações voltadas à implantação e/ou aperfeiçoamento de planejamento estratégico institucional, planejamento estratégico de TI e comitê diretivo de TI, com vistas a propiciar a alocação dos recursos públicos conforme as necessidades e prioridades da organização.

Brasil. Tribunal de Contas da União. Acórdão 2.308/2010-TCU-Plenário.

9.1. recomendar ao Conselho Nacional de Justiça - CNJ, ao Departamento de Coordenação e Controle das Empresas Estatais - Dest, à Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão - SLTI/MPOG, ao Conselho Nacional do Ministério Público - CNMP, à Secretaria Geral da Presidência do Tribunal de Contas da União - Segepres/TCU, à Diretoria Geral da Câmara dos Deputados e à Diretoria Geral do Senado Federal que, no âmbito de suas respectivas áreas de atuação:

9.1.1. orientem as unidades sob sua jurisdição, supervisão ou estrutura acerca da necessidade de estabelecer formalmente: (iv) mecanismos para que a alta administração acompanhe o desempenho da TI da instituição.

Brasil. Tribunal de Contas da União. Acórdão 1.233/2012-TCU-Plenário.

9.1. recomendar, com fundamento no art. 43, inciso I, da Lei 8.443/1992, c/c o art. 250, inciso III do Regimento Interno do TCU, à Câmara de Políticas de Gestão, Desempenho e Competitividade (CGDC) do Conselho de Governo que:

9.1.2. em atenção Decreto-Lei 200/1967, art. 6º, inciso I, e art. 7º, normatize a obrigatoriedade de que todos os entes sob sua jurisdição estabeleçam processo de planejamento estratégico de TI, observando as boas práticas sobre o tema, a exemplo do processo "PO1 - Planejamento Estratégico de TI" do Cobit 4.1, contemplando, pelo menos (subitem II.2):

9.1.2.1. elaboração, com participação de representantes dos diversos setores da organização, de um documento que materialize o plano estratégico de TI, contemplando, pelo menos:

9.1.2.1.1. objetivos, indicadores e metas para a TI organizacional, sendo que os objetivos devem estar explicitamente alinhados aos objetivos de negócio constantes do plano estratégico institucional;

9.1.2.1.2. alocação de recursos (financeiros, humanos, materiais etc);

9.1.2.1.3. estratégia de terceirização;

9.1.2.2. aprovação, pela mais alta autoridade da organização, do plano estratégico de TI;

9.1.2.3. desdobramento do plano estratégico de TI pelas unidades executoras;

9.1.2.4. divulgação do plano estratégico de TI para conhecimento dos cidadãos brasileiros, exceto nos aspectos formalmente declarados sigilosos ou restritos;

9.1.2.5. acompanhamento periódico do alcance das metas estabelecidas, para correção de desvios;

9.1.2.6. divulgação interna e externa do alcance das metas, ou os motivos de não as ter alcançado;

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. ABNT NBR ISO/IEC 38500:2009 – Governança corporativa de tecnologia da informação.

p.11 ***3.3. Princípio 2: Estratégia. Dirigir –*** *Convém que os dirigentes liderem a preparação e o uso de planos e políticas que assegurem que a organização seja beneficiada pelos desenvolvimentos de TI.* ***Monitorar –*** *Convém que os dirigentes monitorem o uso da TI para assegurar que os benefícios pretendidos estão sendo alcançados.*

p.12 ***3.4 Princípio 3: Aquisição. Dirigir –*** *Convém que os dirigentes deem a devida orientação para que os ativos de TI (sistemas e infraestrutura) sejam adquiridos de forma apropriada, incluindo a preparação de documentação adequada que assegure o fornecimento de capacidades necessárias.* ***Monitorar –*** *Convém que os dirigentes monitorem os investimentos de TI para assegurar que eles forneçam as capacidades requeridas.*

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. COBIT - Control Objectives for Information and related Technology. COBIT 5 – Enabling Process.

p.36 ***EDM02.02 Dirigir a otimização de valor. Atividade 1 –*** *Definir e comunicar o portfólio, tipos, categorias, critérios dos investimentos e pesos relativos aos critérios de pontuação.* ***Atividade 6 –*** *Dirigir quaisquer mudanças necessárias ao portfólio de investimentos e serviços para realinhar com os objetivos corporativos (e/ou restrições) esperados e atuais (tradução livre).*

1.4. Com relação aos riscos de TI:

a. organização define formalmente as diretrizes para gestão dos riscos de TI aos quais o negócio está exposto.

b. a organização define e comunica formalmente papéis e responsabilidades pela gestão de riscos de TI.

c. a organização define formalmente os níveis de risco de TI aceitáveis na consecução de seus objetivos (apetite a risco).

d. a organização toma decisões estratégicas considerando os níveis de risco de TI definidos.

Referências

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. ABNT NBR ISO 31000:2009 – Gestão de riscos – Princípios e diretrizes

p.7 **3. Princípios. c) A gestão de riscos é parte da tomada de decisão –** A gestão de riscos auxilia os tomadores de decisão a fazer escolhas conscientes, priorizar ações e distinguir enre formas alternativas de ação.

p.9 ***4.2 Mandato e comprometimento*** *– [...] Convém que a administração defina e aprove a política de gestão de riscos.*

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. COBIT - Control Objectives for Information and related Technology. COBIT 5 – Enabling Process.

p.36 ***EDM03.02 Dirigir a gestão de risco –*** *Dirigir o estabelecimento das práticas de gestão de risco, a fim de garantir que o risco de TI não exceda o apetite ao risco da organização (tradução livre).*

1.5. Com relação ao pessoal de TI:

a. a organização define formalmente diretrizes para garantir o desenvolvimento de competências e a retenção de gestores de TI.

b. a organização define formalmente diretrizes para garantir o desenvolvimento de competências e a retenção de pessoal técnico de TI.

c. a organização define formalmente diretrizes para avaliação e incentivo ao desempenho de gestores de TI.

d. a organização define formalmente diretrizes para avaliação e incentivo ao desempenho de pessoal técnico de TI.

e. a organização define formalmente diretrizes para escolha dos líderes da área de TI, ocupantes dos cargos de chefia e de assessoramento.

Referências

Brasil. Tribunal de Contas da União. Acórdão 1.233/2012-TCU-Plenário.

9.2. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, à Secretaria de Logística e Tecnologia da Informação (SLTI/MP) que:

9.2.9. em atenção ao Decreto-Lei 200/1967, art. 6º, V, estabeleça, normativamente para todos os entes sob sua jurisdição, a obrigatoriedade de a alta administração implantar uma estrutura de controles internos mediante a definição de atividades de controle em todos os níveis da organização para mitigar os riscos de suas atividades, pelo menos nos seguintes processos (subitem II.11):

9.2.9.8. gestão de pessoal de TI;

9.4. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Ministério do Planejamento, Orçamento e Gestão que:

9.4.1. em atenção ao Decreto 5.707/2006, art. 5º, § 2º, c/c o art. 1º, III, discipline a forma de acesso às funções de liderança nos setores de Tecnologia da Informação, considerando as competências multidisciplinares necessárias para estas funções, que incluem, mas não se limitam a conhecimentos em TI (subitem II.3).

9.11. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, à Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União (CGPAR) que:

9.11.3. discipline a forma de acesso às funções de liderança nos setores de Tecnologia da Informação, considerando as competências multidisciplinares necessárias para estas funções, que incluem, mas não se limitam a conhecimentos em TI (subitem II.3);

9.11.12. em atenção ao Decreto-Lei 200/1967, art. 6º, V, estabeleça, normativamente para todos os entes sob sua jurisdição, a obrigatoriedade de a alta administração implantar uma estrutura de controles internos mediante a definição de atividades de controle em todos os níveis da organização para mitigar os riscos de suas atividades, pelo menos nos seguintes processos (subitem II.11):

9.11.12. 9. gestão de pessoal de TI;

9.13. Recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Conselho Nacional da Justiça (CNJ) que:

9.13.2. discipline a forma de acesso às funções de liderança nos setores de Tecnologia da Informação, considerando as competências multidisciplinares necessárias para estas funções, que incluem, mas não se limitam a conhecimentos em TI (subitem II.3);

9.13.14. em atenção ao Decreto-Lei 200/1967, art. 6º, V, estabeleça, normativamente para todos os entes sob sua jurisdição, a obrigatoriedade de a alta administração implantar uma estrutura de controles internos mediante a definição de atividades de controle em todos os níveis da organização para mitigar os riscos de suas atividades, pelo menos nos seguintes processos (subitem II.11):

9.13.14.9. gestão de pessoal de TI;

9.15. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Conselho Nacional do Ministério Público (CNMP) que:

9.15.5. discipline a forma de acesso às funções de liderança nos setores de Tecnologia da Informação, considerando as competências multidisciplinares necessárias para estas funções, que incluem, mas não se limitam a conhecimentos em TI (subitem II.3);

9.15.18. em atenção ao Decreto-Lei 200/1967, art. 6º, V, estabeleça, normativamente para todos os entes sob sua jurisdição, a obrigatoriedade de a alta administração implantar uma estrutura de controles internos mediante a definição de atividades de controle em todos os níveis da organização para mitigar os riscos de suas atividades, pelo menos, nos seguintes processos (subitem II.11):

9.15.18.9. gestão de pessoal de TI;

Brasil. Tribunal de Contas da União. Acórdão 2.585/2012-TCU-Plenário.

9.3. recomendar à Secretaria de Logística e Tecnologia da Informação, do Ministério do Planejamento, Orçamento e Gestão (MP), com fundamento na Lei nº 11.907/2009, arts. 81 e 287, e no princípio do comportamento humano, previsto na ABNT NBR ISO/IEC 38500, que, em conjunto coma Secretaria de Gestão Pública/MP, elabore plano de gestão de recursos humanos para o Sistema de Administração dos Recursos de Informação e Informática;

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. ABNT NBR ISO/IEC 38500:2009 – Governança corporativa de tecnologia da informação.

p. 21 ***3.7 Princípio 6: Comportamento Humano. Avaliar*** *– Convém que os dirigentes avaliem as atividades de TI para garantir que os comportamento humanos sejam identificados e apropriadamente considerados.* ***Dirigir*** *– Convém que os dirigentes exijam que as atividades de TI sejam compatíveis com as diferenças de comportamento humano.* ***Monitorar*** *– Convém que os dirigentes monitorem atividades de TI para garantir que os comportamentos humanos permaneçam relevantes e que lhes sejam dadas a devida atenção. Convém que os dirigentes monitorem as práticas de trabalho para garantir que são consistentes com o uso apropriado da TI.*

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. COBIT - Control Objectives for Information and related Technology. COBIT 5 – Enabling Process.

p. 32 ***EDM01.02 Dirigir o sistema de governança. Atividade 2*** *– Estabelecer ou delegar o estabelecimento de estruturas, processos e práticas de governança em conformidade com os princípios acordados.* ***Atividade 3 –*** *Alocar responsabilidade, autoridade e obrigação de prestar contas em consonância com os princípios de governança, os modelos de tomada de decisão e as delegações.* ***Atividade 5 –*** *Dirigir a equipe para seguir diretrizes de comportamento ético e profissional e assegurar que consequências de desconformidade sejam conhecidas e aplicadas.* ***Atividade 6 –*** *Dirigir o estabelecimento de um sistema de recompensa para promover a mudança cultural desejável* (tradução livre).

p. 43 ***EDM04 Assegurar otimização de recursos*** *– Assegurar que capacidades de TI (pessoas, processos e tecnologia) adequadas e suficientes estejam disponíveis para suportar os objetivos da organização de forma efetiva e com custo otimizado*.

p. 44 ***EDM04.01 Avaliar o gerenciamento de recursos. Atividade 1*** *– Com base nas estratégias atual e futura, examinar e fazer juízo sobre as opções para fornecimento de recursos de TI e o desenvolvimento de capacidades para atender as necessidades atuais e as futuras.* ***Atividade 2 –*** *Definir os princípios para orientar a alocação e o gerenciamento de recursos e capacidades para que a TI possa atender às necessidades da organização.* ***Atividade 3 –*** *Revisar e aprovar o plano de recursos e as estratégias da organização para entrega de valor e mitigação de riscos com os recursos alocados* (tradução livre). ***EDM04.02 Direcionar o gerenciamento de recursos. Atividade 1 –*** *Comunicar e conduzir a adoção de estratégias e princípios de gestão de recursos* (tradução livre). ***Atividade 2*** *– Atribuir responsabilidades para gerenciamento de recursos* (tradução livre). ***Atividade 3 –*** *Definir métricas e metas para gestão de recursos* (tradução livre). ***Atividade 5 –*** *Alinhar gestão de recursos com os planejamentos de recursos humanos e financeiro da organização* (tradução livre). ***EDM04.03 Monitorar o gerenciamento de recursos. Atividade 1 –*** *Monitorar a alocação e a otimização de recursos em conformidade com objetivos e prioridades da organização, usando metas e métricas acordadas.* ***Atividade 2*** *– Monitorar as capacidades e recursos de TI para assegurar que as necessidades atual e futura da organização possam ser atendidas* (tradução livre). ***Atividade 3 –*** *Monitorar o desempenho dos recursos em relação aos objetivos e analisar e tratar as causas de desvios* (tradução livre).

1.6. Com relação à transparência da gestão e uso de TI:

a. a organização define formalmente diretrizes para comunicação com as partes interessadas (público interno e externo) sobre os resultados da gestão e do uso de TI, contemplando o meio de divulgação, o conteúdo, a frequência e o formato das comunicações.

Referências

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. ABNT NBR ISO/IEC 38500:2009 – Governança corporativa de tecnologia da informação.

p. 9 ***3.2 Princípio 1: Responsabilidade. Dirigir*** *– Convém que os dirigentes exijam o recebimento de informações que eles necessitam para atender às suas responsabilidades e compromissos.*

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. COBIT - Control Objectives for Information and related Technology. COBIT 5 – Enabling Process.

p. 47 ***EDM05 Assegurar transparência para as partes interessadas*** *– Objetivo: Ter certeza de que a comunicação com as partes interessadas é efetiva e tempestiva e a base para a comunicação é estabelecida para aumentar o desempenho, identificar áreas de melhoria, e confirmar que os objetivos e estratégias de TI estão alinhados com a estratégia da organização* (tradução livre).

p. 48 ***EDM05.01 Avaliar as necessidades de comunicação com as partes interessadas*** *– Continuamente examinar e fazer juízo sobre as necessidades atuais e futuras para comunicação com as partes interessadas* (...). *Estabelecer os princípios para a comunicação* (tradução livre). ***EDM05.02 Dirigir a comunicação com as partes interessadas*** *– Assegurar o estabelecimento de comunicação efetiva com as partes interessadas, incluindo mecanismos para assegurar a qualidade e a integridade das informações, a fiscalização de comunicações obrigatórias, e a criação de uma estratégia de comunicação com as partes interessadas* (tradução livre). ***EDM05.03 Monitorar a comunicação com as partes interessadas*** *– Monitorar a efetividade da comunicação com as partes interessadas. Avaliar os mecanismos para assegurar precisão, confiabilidade e efetividade, e verificar se as necessidades das diferentes partes interessadas estão sendo atendidas* (tradução livre).

1.7. Com relação ao monitoramento da governança e da gestão de TI:

a. a organização define formalmente diretrizes para avaliação da governança e da gestão de TI.

b. a organização realiza avaliação periódica de governança e de gestão de TI.

c. a organização realiza avaliação periódica de sistemas de informação.

d. a organização realiza avaliação periódica de segurança da informação.

e. a organização realiza avaliação periódica de contratos de TI.

Referências

Brasil. Tribunal de Contas da União. Acórdão 1.233/2012-TCU-Plenário.

9.10. Recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, à Controladoria-Geral da União (CGU/PR) que:

9.10.1. considere os temas governança de TI, riscos de TI e controles de TI na seleção dos objetos a auditar, consoante o previsto nas boas práticas internacionais para que a atividade de auditoria interna seja mais efetiva (e.g., IPPF 2110.A2, 2120.A1 e 2130.A1; subitem II.11).

9.10.2. oriente as unidades de auditoria interna sob sua orientação normativa a considerar os temas governança de TI, riscos de TI e controles de TI na seleção dos objetos a auditar, consoante o previsto nas boas práticas internacionais para que a atividade de auditoria interna seja mais efetiva (e.g., IPPF 2110.A2, 2120.A1 e 2130.A1; subitem II.11).

9.13. Recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Conselho Nacional da Justiça (CNJ) que:

9.13.15. oriente as unidades de auditoria interna sob sua orientação normativa a considerar os temas governança de TI, riscos de TI e controles de TI na seleção dos objetos a auditar, consoante o previsto nas boas práticas internacionais para que a atividade de auditoria interna seja mais efetiva (e.g., IPPF 2110.A2, 2120.A1 e 2130.A1; subitem II.11);

9.15. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Conselho Nacional do Ministério Público (CNMP) que:

9.15.19. oriente as unidades de auditoria interna sob sua orientação normativa a considerar os temas governança de TI, riscos de TI e controles de TI na seleção dos objetos a auditar, consoante o previsto nas boas práticas internacionais para que a atividade de auditoria interna seja mais efetiva (e.g., IPPF 2110.A2, 2120.A1 e 2130.A1; subitem II.11);

Brasil. Tribunal de Contas da União. Acórdão 2.308/2010-TCU-Plenário.

9.1. recomendar ao Conselho Nacional de Justiça - CNJ, ao Departamento de Coordenação e Controle das Empresas Estatais - Dest, à Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão - SLTI/MPOG, ao Conselho Nacional do Ministério Público - CNMP, à Secretaria Geral da Presidência do Tribunal de Contas da União - Segepres/TCU, à Diretoria Geral da Câmara dos Deputados e à Diretoria Geral do Senado Federal que, no âmbito de suas respectivas áreas de atuação:

9.1.1. orientem as unidades sob sua jurisdição, supervisão ou estrutura acerca da necessidade de estabelecer formalmente: (i) objetivos institucionais de TI alinhados às estratégias de negócio; (ii) indicadores para cada objetivo definido, preferencialmente em termos de benefícios para o negócio da instituição; (iii) metas para cada indicador definido; (iv) mecanismos para que a alta administração acompanhe o desempenho da TI da instituição;

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. ABNT NBR ISO/IEC 38500:2009 – Governança corporativa de tecnologia da informação.

p. 6 ***2.2 Modelo.*** *Convém que os dirigentes governem TI através de três tarefas principais: c) Monitorar o cumprimento das políticas e o desempenho em relação aos planos.*

p. 13 ***3.5 Princípio 4: Desempenho. Monitorar*** *– Convém que os dirigentes monitorem até que ponto a TI dá suporte ao negócio. Convém que os dirigentes monitorem até que ponto as políticas, tais como aquelas relacionadas com a exatidão dos dados e a eficiência do uso da TI, são seguidas corretamente.*

p. 14 ***3.6 Princípio 5: Conformidade. Monitorar*** *– Convém que os dirigentes monitorem o cumprimento e conformidade da TI por meio de relatos apropriados e práticas de auditoria, assegurando que análises críticas ocorram dentro dos prazos e sejam realizadas de forma completa e apropriadas, para a avaliação do grau de satisfação do negócio. Convém que os dirigentes monitorem as atividades de TI, incluindo a liberação de ativos e dados, para assegurar o cumprimento das exigências ambientais, de privacidade, de gerenciamento do conhecimento estratégico e de preservação da memória organizacional e outras obrigações relevantes.*

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. COBIT - Control Objectives for Information and related Technology. COBIT 5 – Enabling Process.

p. 33 ***EDM01.03 Monitorar o sistema de governança*** *– Monitorar a efetividade e o desempenho da governança de TI. Avaliar se o sistema de governança e os mecanismos implementados (incluindo estruturas, princípios e processos) estão operando de forma efetiva e provendo supervisão adequada da TI* (tradução livre).

p. 99 ***APO10.05 Monitorar desempenho e conformidade de fornecedores*** *– Revisar periodicamente o desempenho do fornecedor, a conformidade com as cláusulas de contrato, a relação custo-benefício da contratação (comparada com fornecedores alternativos e condições atuais de mercado), e tratar questões identificadas* (tradução livre).

p. 115 ***APO013.03 Monitorar e revisar o sistema de gestão da segurança da informação (SGSI)*** *– Manter e comunicar regularmente a necessidade e os benefícios da melhoria continua da segurança da informação* (tradução livre). ***Atividade 1*** *– Realizar revisões periódicas da efetividade do SGSI, incluindo o cumprimento de políticas e objetivos do SGSI, e revisar as práticas de segurança* (tradução livre). ***Atividade 2*** *– Realizar auditorias internas do SGSI em intervalos planejados* (tradução livre).

p. 203 ***MEA01 Monitorar e avaliar desempenho e conformidade*** *– Coletar, validar e avaliar objetivos e métricas de negócio, TI e processos. Monitorar se os processos estão executados de acordo com metas e métricas de desempenho e conformidade acordadas e prover comunicação sistemática e tempestiva (tradução livre).*

1.8. Com relação à auditoria interna:

a. a auditoria interna possui pessoal capacitado para avaliar a governança e a gestão de TI.

Informe o quantitativo desse pessoal: _____

b. a auditoria interna monitora as ações de governança e de gestão de TI.

c. a organização aprova, de forma periódica, plano de auditoria que inclua avaliação da governança e da gestão de TI.

d. a auditoria interna avalia a gestão de riscos de TI.

e. a auditoria interna avalia os riscos considerados críticos para o negócio e a eficácia dos respectivos controles.

f. a auditoria interna avalia as respostas apresentadas aos questionários dos Levantamentos de Governança de TI realizados pelo TCU.

Referências

BRASIL. Tribunal de Contas da União. Referencial Básico de Governança

p.37 ***COMPONETE C2. Auditoria Interna. Prática C2.2. -*** *Prover condições para que a auditoria interna seja independente e para que os auditores internos sejam proficientes, atuem de forma objetiva e com zelo profissional ao executar seus trabalhos.*

Brasil. Tribunal de Contas da União. Acórdão 1.603/2008-TCU-Plenário.

9.1. recomendar ao Conselho Nacional de Justiça - CNJ e ao Conselho Nacional do Ministério Público - CNMP que, nos órgãos integrantes da estrutura do Poder Judiciário Federal e do Ministério Público da União, respectivamente:

9.1.8. introduzam práticas voltadas à realização de Auditorias de TI, que permitam a avaliação regular da conformidade, da qualidade, da eficácia e da efetividade dos serviços prestados;

9.3. recomendar à Controladoria-Geral da União - CGU que realize regularmente Auditorias de TI e/ou promova ações para estimular a realização dessas Auditorias nos órgãos/entidades da Administração Pública Federal;

Brasil. Tribunal de Contas da União. Acórdão 1.233/2012-TCU-Plenário.

9.10. Recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, à Controladoria-Geral da União (CGU/PR) que:

9.10.2. oriente as unidades de auditoria interna sob sua orientação normativa a considerar os temas governança de TI, riscos de TI e controles de TI na seleção dos objetos a auditar, consoante o previsto nas boas práticas internacionais para que a atividade de auditoria interna seja mais efetiva (e.g., IPPF 2110.A2, 2120.A1 e 2130.A1; subitem II.11).

9.13. Recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Conselho Nacional da Justiça (CNJ) que:

9.13.15. oriente as unidades de auditoria interna sob sua orientação normativa a considerar os temas governança de TI, riscos de TI e controles de TI na seleção dos objetos a auditar, consoante o previsto nas boas práticas internacionais para que a atividade de auditoria interna seja mais efetiva (e.g., IPPF 2110.A2, 2120.A1 e 2130.A1; subitem II.11);

9.15. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Conselho Nacional do Ministério Público (CNMP) que:

9.15.19. oriente as unidades de auditoria interna sob sua orientação normativa a considerar os temas governança de TI, riscos de TI e controles de TI na seleção dos objetos a auditar, consoante o previsto nas boas práticas internacionais para que a atividade de auditoria interna seja mais efetiva (e.g., IPPF 2110.A2, 2120.A1 e 2130.A1; subitem II.11);

2. Estratégias e Planos

2.1. Com relação ao planejamento estratégico institucional:

Processo

a. a organização executa periodicamente processo de planejamento estratégico institucional.
b. o processo de planejamento estratégico institucional prevê a participação das áreas mais relevantes da organização.
c. o processo de planejamento estratégico institucional prevê a participação da área de TI.
d. o processo de planejamento estratégico institucional está formalmente instituído, como norma de cumprimento obrigatório.

Plano Vigente

e. a organização possui plano estratégico institucional vigente, formalmente instituído pelo seu dirigente máximo.
f. o plano estratégico institucional vigente contém pelo menos um indicador de resultado para quantificar o cumprimento de cada objetivo estratégico estabelecido.
g. o plano estratégico institucional vigente contém metas de curto, médio e longo prazos, associadas aos indicadores de resultado.
h. o plano estratégico institucional vigente estabelece os projetos e ações considerados necessários e suficientes para o alcance das metas fixadas.
i. a execução do plano estratégico institucional vigente é acompanhada periodicamente quanto ao alcance das metas estabelecidas, para correção de desvios.
j. o plano estratégico institucional vigente está publicado na internet para acesso livre.

Referências

Brasil. Decreto-Lei 200, de 25 de fevereiro de 1967.

Art. 6º As atividades da Administração Federal obedecerão aos seguintes princípios fundamentais:

I - Planejamento.

Art. 7º A ação governamental obedecerá a planejamento que vise a promover o desenvolvimento econômico-social do País e a segurança nacional, norteando-se segundo planos e programas elaborados, na forma do Título III, e compreenderá a elaboração e atualização dos seguintes instrumentos básicos:

a) plano geral de governo;

b) programas gerais, setoriais e regionais, de duração plurianual;

Brasil. Tribunal de Contas da União. Acórdão 1.603/2008-TCU-Plenário.

9.1. recomendar ao Conselho Nacional de Justiça - CNJ e ao Conselho Nacional do Ministério Público - CNMP que, nos órgãos integrantes da estrutura do Poder Judiciário Federal e do Ministério Público da União, respectivamente:

9.1.1. promovam ações com o objetivo de disseminar a importância do planejamento estratégico, procedendo, inclusive mediante orientação normativa, ações voltadas à implantação e/ou aperfeiçoamento de planejamento estratégico institucional, planejamento estratégico de TI e comitê diretivo de TI, com vistas a propiciar a alocação dos recursos públicos conforme as necessidades e prioridades da organização;

Brasil. Tribunal de Contas da União. Acórdão 1.233/2012-TCU-Plenário.

9.1. recomendar, com fundamento no art. 43, inciso I, da Lei 8.443/1992, c/c o art. 250, inciso III do Regimento Interno do TCU, à Câmara de Políticas de Gestão, Desempenho e Competitividade (CGDC) do Conselho de Governo que:

9.1.1 em atenção Decreto-Lei 200/1967, art. 6º, inciso I, e art. 7º, normatize a obrigatoriedade de que todos os entes sob sua jurisdição estabeleçam processo de planejamento estratégico institucional, observando as boas práticas sobre o tema, a exemplo do critério de avaliação 2 do Gespública, contemplando, pelo menos (subitem II.1):

9.1.1.1. elaboração, com participação de representantes dos diversos setores da organização, de um documento que materialize o plano estratégico institucional de longo prazo, contemplando, pelo menos, objetivos, indicadores e metas para a organização;

9.1.1.2. aprovação, pela mais alta autoridade da organização, do plano estratégico institucional;

9.1.1.3. desdobramento do plano estratégico pelas unidades executoras;

9.1.1.4. divulgação do plano estratégico institucional para conhecimento dos cidadãos brasileiros, exceto nos aspectos formalmente declarados sigilosos ou restritos;

9.1.1.5. acompanhamento periódico do alcance das metas estabelecidas, para correção de desvios;

9.1.1.6. divulgação interna e externa do alcance das metas, ou dos motivos de não as ter alcançado;

9.15. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Conselho Nacional do Ministério Público (CNMP) que:

9.15.1. em atenção ao Decreto-Lei 200/1967, art. 6º, inciso I, e art. 7º, normatize a obrigatoriedade de que todos os entes sob sua jurisdição estabeleçam processo de planejamento estratégico institucional, observando as boas práticas sobre o tema, a exemplo do critério de avaliação 2 do Gespública, contemplando, pelo menos (subitem II.1):

9.15.1.1. elaboração, com participação de representantes dos diversos setores da organização, de um documento que materialize o plano estratégico institucional de longo prazo, contemplando, pelo menos, objetivos, indicadores e metas para a organização;

9.15.1.2. aprovação, pela mais alta autoridade da organização, do plano estratégico institucional;

9.15.1.3. desdobramento do plano estratégico pelas unidades executoras;

9.15.1.4.divulgação do plano estratégico institucional para conhecimento dos cidadãos brasileiros, exceto nos aspectos formalmente declarados sigilosos ou restritos;

9.15.1.5. acompanhamento periódico do alcance das metas estabelecidas, para correção de desvios;

9.15.1.6. divulgação interna e externa do alcance das metas, ou dos motivos de não as ter alcançado.

Brasil. Tribunal de Contas da União. Acórdão 1.233/2012-TCU-Plenário.

9.1. recomendar ao Conselho Nacional de Justiça, Conselho Nacional do Ministério Público, Secretaria de Logística e Tecnologia da Informação e Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União, com fundamento na Lei nº 8.443/92, art. 43, inciso I, c/c Regimento Interno do TCU, art. 250, inciso III, que:
9.1.1. orientem as instituições sob sua jurisdição para que:

9.1.1.1. em atenção ao art. 6º da Lei nº 12.527/2011 e aos princípios da transparência e da prestação de contas, implementem instrumentos de planejamento estratégico institucional e de tecnologia da informação, dando-lhes ampla divulgação, com exceção das informações classificadas como não públicas, nos termos da lei;
Brasil. Conselho Nacional de Justiça. Resolução 70, de 18 de março de 2009.
Art. 1° Fica instituído o Planejamento Estratégico do Poder Judiciário, consolidado no Plano Estratégico Nacional consoante do Anexo.

2.2. Com relação ao planejamento de tecnologia da informação:

Processo
a. a organização executa periodicamente **processo** de planejamento de TI.
b. o **processo** de planejamento de TI prevê a participação das áreas mais relevantes da organização.
c. o **processo** de planejamento de TI prevê o apoio do comitê de TI.
d. o **processo** de planejamento de TI está formalmente instituído, como norma de cumprimento obrigatório.
Plano Vigente
e. a organização possui **plano** de TI **vigente**, formalmente instituído pelo seu dirigente máximo.
f. o **plano** de TI **vigente** contempla objetivos, indicadores e metas para a TI, com os objetivos explicitamente alinhados aos objetivos de negócio constantes do plano estratégico institucional.
g. o **plano** de TI **vigente** contempla alocação de recursos (orçamentários, humanos e materiais) e estratégia de execução indireta (terceirização).
h. a execução do **plano** de TI **vigente** é acompanhada periodicamente quanto ao alcance das metas estabelecidas, para correção de desvios.
i. o **plano** de TI **vigente** vincula as ações (atividades e projetos) a indicadores e metas de negócio.
j. o **plano** de TI **vigente** fundamenta a proposta orçamentária de TI.

Referências

Brasil. Decreto-Lei 200, de 25 de fevereiro de 1967.

Art. 6º As atividades da Administração Federal obedecerão aos seguintes princípios fundamentais:

I - Planejamento.

Art. 7º A ação governamental obedecerá a planejamento que vise a promover o desenvolvimento econômico-social do País e a segurança nacional, norteando-se segundo planos e programas elaborados, na forma do Título III, e compreenderá a elaboração e atualização dos seguintes instrumentos básicos:

a) plano geral de governo;

b) programas gerais, setoriais e regionais, de duração plurianual;

Brasil. Tribunal de Contas da União. Acórdão 1.603/2008-TCU-Plenário.

9.1. recomendar ao Conselho Nacional de Justiça - CNJ e ao Conselho Nacional do Ministério Público - CNMP que, nos órgãos integrantes da estrutura do Poder Judiciário Federal e do Ministério Público da União, respectivamente:

9.1.1. promovam ações com o objetivo de disseminar a importância do planejamento estratégico, procedendo, inclusive mediante orientação normativa, ações voltadas à implantação e/ou aperfeiçoamento de planejamento estratégico institucional, planejamento estratégico de TI e comitê diretivo de TI, com vistas a propiciar a alocação dos recursos públicos conforme as necessidades e prioridades da organização.

Brasil. Tribunal de Contas da União. Acórdão 2.308/2010-TCU-Plenário.

9.1. recomendar ao Conselho Nacional de Justiça - CNJ, ao Departamento de Coordenação e Controle das Empresas Estatais - Dest, à Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão - SLTI/MPOG, ao Conselho Nacional do Ministério Público - CNMP, à Secretaria Geral da Presidência do Tribunal de Contas da União - Segepres/TCU, à Diretoria Geral da Câmara dos Deputados e à Diretoria Geral do Senado Federal que, no âmbito de suas respectivas áreas de atuação:

9.1.1. orientem as unidades sob sua jurisdição, supervisão ou estrutura acerca da necessidade de estabelecer formalmente: (i) objetivos institucionais de TI alinhados às estratégias de negócio; (ii) indicadores para cada objetivo definido, preferencialmente em termos de benefícios para o negócio da instituição; (iii) metas para cada indicador definido; (iv) mecanismos para que a alta administração acompanhe o desempenho da TI da instituição;

9.1.2. normatizem a obrigatoriedade de a alta administração de cada instituição sob sua jurisdição, supervisão ou estrutura estabelecer os itens acima;

Brasil. Tribunal de Contas da União. Acórdão 1.233/2012-TCU-Plenário.

9.1. recomendar, com fundamento no art. 43, inciso I, da Lei 8.443/1992, c/c o art. 250, inciso III do Regimento Interno do TCU, à Câmara de Políticas de Gestão, Desempenho e Competitividade (CGDC) do Conselho de Governo que:

9.1.2. em atenção Decreto-Lei 200/1967, art. 6º, inciso I, e art. 7º, normatize a obrigatoriedade de que todos os entes sob sua jurisdição estabeleçam processo de planejamento estratégico de TI, observando as boas práticas sobre o tema, a exemplo do processo "PO1 - Planejamento Estratégico de TI" do Cobit 4.1, contemplando, pelo menos (subitem II.2):

9.1.2.1. elaboração, com participação de representantes dos diversos setores da organização, de um documento que materialize o plano estratégico de TI, contemplando, pelo menos:

9.1.2.1.1. objetivos, indicadores e metas para a TI organizacional, sendo que os objetivos devem estar explicitamente alinhados aos objetivos de negócio constantes do plano estratégico institucional;

9.1.2.1.2. alocação de recursos (financeiros, humanos, materiais etc);

9.1.2.1.3. estratégia de terceirização;

9.1.2.2. aprovação, pela mais alta autoridade da organização, do plano estratégico de TI;

9.1.2.3. desdobramento do plano estratégico de TI pelas unidades executoras;

9.1.2.4. divulgação do plano estratégico de TI para conhecimento dos cidadãos brasileiros, exceto nos aspectos formalmente declarados sigilosos ou restritos;

9.1.2.5. acompanhamento periódico do alcance das metas estabelecidas, para correção de desvios;

9.1.2.6. divulgação interna e externa do alcance das metas, ou os motivos de não as ter alcançado;

9.15. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Conselho Nacional do Ministério Público (CNMP) que:

9.15.2. em atenção ao Decreto-Lei 200/1967, art. 6º, inciso I, e art. 7º, normatize a obrigatoriedade de que todos os entes sob sua jurisdição estabeleçam processo de planejamento estratégico de TI, observando as boas práticas sobre o tema, a exemplo do processo "PO1 - Planejamento Estratégico de TI" do Cobit 4.1, contemplando, pelo menos (subitem II.2):

9.15.2.1. elaboração, com participação de representantes dos diversos setores da organização, de um documento que materialize o plano estratégico de TI, contemplando, pelo menos:

9.15.2.1.1. objetivos, indicadores e metas para a TI organizacional, sendo que os objetivos devem estar explicitamente alinhados aos objetivos de negócio constantes do plano estratégico institucional;

9.15.2.1.2. alocação de recursos (financeiros, humanos, materiais etc);

9.15.2.1.3. estratégia de terceirização;

9.15.2.2. aprovação, pela mais alta autoridade da organização, do plano estratégico de TI;

9.15.2.3. desdobramento do plano estratégico de TI pelas unidades executoras;

9.15.2.4. divulgação do plano estratégico de TI para conhecimento dos cidadãos brasileiros, exceto nos aspectos formalmente declarados sigilosos ou restritos;

9.15.2.5. acompanhamento periódico do alcance das metas estabelecidas, para correção de desvios;

9.15.2.6. divulgação interna e externa do alcance das metas, ou os motivos de não as ter alcançado.

Brasil. Tribunal de Contas da União. Acórdão 1.233/2012-TCU-Plenário.

9.1. recomendar ao Conselho Nacional de Justiça, Conselho Nacional do Ministério Público, Secretaria de Logística e Tecnologia da Informação e Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União, com fundamento na Lei nº 8.443/92, art. 43, inciso I, c/c Regimento Interno do TCU, art. 250, inciso III, que:
9.1.1. orientem as instituições sob sua jurisdição para que:

9.1.1.1. em atenção ao art. 6º da Lei nº 12.527/2011 e aos princípios da transparência e da prestação de contas, implementem instrumentos de planejamento estratégico institucional e de tecnologia da informação, dando-lhes ampla divulgação, com exceção das informações classificadas como não públicas, nos termos da lei;
INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. COBIT - Control Objectives for Information and related Technology. COBIT 5 – Enabling Process.

p.57 ***APO02 Gerenciar a estratégia. Finalidade do Processo –*** *Alinhar os planos estratégicos de TI com os objetivos de negócio. Comunicar claramente os objetivos e responsabilidades associadas para que sejam compreendidos por todos, com as opções estratégicas de TI identificadas, estruturadas e integradas com os planos de negócio (tradução livre).*

3. Informações

3.1. Com relação à informatização dos processos organizacionais:

a. a organização identifica e mapeia os principais processos de negócio.

b. os principais processos de negócio da organização são suportados por sistemas informatizados.

c. há catálogo publicado com informações atualizadas de cada um dos sistemas informatizados.

d. a organização designa **formalmente** responsáveis da área de negócio para a gestão dos respectivos sistemas informatizados.

e. a organização avalia periodicamente a efetiva utilização dos sistemas informatizados que suportam o negócio.

Referências

Brasil. Tribunal de Contas da União. Acórdão 2.585/2012-TCU-Plenário.

9.1. recomendar ao Conselho Nacional de Justiça, Conselho Nacional do Ministério Público, Secretaria de Logística e Tecnologia da Informação e Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União, com fundamento na Lei nº 8.443/92, art. 43, inciso I, c/c Regimento Interno do TCU, art. 250, inciso III, que:
9.1.1. orientem as instituições sob sua jurisdição para que:

9.1.1.2. identifiquem os processos críticos de negócio e designem formalmente os gestores responsáveis pelos sistemas de informação que dão suporte a esses processos, à semelhança das orientações da ABNT NBR ISO/IEC 38500;

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. ABNT NBR ISO/IEC 38500:2009 – Governança corporativa de tecnologia da informação.

p. 11 ***3.3 Princípio 2: Estratégia. Avaliar*** *– Convém que os dirigentes avaliem os desenvolvimentos em TI e os processos dos negócios para garantir que a TI apoiará às necessidades futuras do negócio.*

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. COBIT - Control Objectives for Information and related Technology. COBIT 5 – Enabling Process.

p. 55 ***APO01.06 Definir proprietários de informações e sistemas*** *– Definir e manter responsabilidades para proprietários de informações (dados) e de sistemas de informação* (tradução livre).

p. 65-66 ***APO03.02 Definir arquitetura de referência*** *– A arquitetura de referência descreve a arquitetura atual e a desejada para os domínios negócio, informação, dados, aplicações e tecnologia.* ***Atividade 5*** *– Manter um modelo de arquitetura de processo como parte das descrições de domínios. Padronizar as descrições e documentações de processos* (tradução livre).

p. 90 ***APO08.01 Entender as expectativas de negócio*** *– Entender os objetivos e as questões de negócio atuais e as expectativas do negócio em relação à TI.* ***Atividade 3*** *– Manter um entendimento dos processos de negócio e das atividades associadas* (tradução livre).

p. 94 ***APO09.01 Identificar serviços de TI*** *– Analisar necessidades de negócio e o modo pelo qual os serviços de TI suportam os processos de negócio.* ***Atividade 1*** *– Avaliar os serviços de TI atuais para identificar lacunas entre os serviços existentes e as atividades de negócio suportadas.* ***Atividade 3*** *– Analisar atividades de processos de negócio para identificar a necessidade de serviços de TI novos ou redesenhados.* ***Atividade 6*** *– Revisar regularmente o portfólio de serviços de TI para identificar serviços obsoletos* (tradução livre). ***APO09.02 Catalogar serviços de TI*** *– Definir e manter um ou mais catálogos de serviços. Publicar e manter os serviços de TI disponíveis nos catálogos de serviços* (tradução livre).

3.2. Com relação à transparência das informações relacionadas à gestão e uso de TI:

a. os planos de TI vigentes são divulgados na internet, sendo facilmente acessados.

b. as informações sobre o alcance dos objetivos de TI planejados são divulgados na internet, sendo facilmente acessadas.

c. as informações sobre o acompanhamento das ações e dos projetos de TI são divulgadas na internet, sendo facilmente acessadas.

d. os editais, seus respectivos anexos e os resultados das licitações de TI (inteiro teor) são divulgados na internet, sendo facilmente acessados.

e. os estudos técnicos preliminares (inteiro teor) são divulgados na internet, juntamente com os editais de licitação de TI, sendo facilmente acessados.

f. os contratos de TI e os respectivos aditivos (inteiro teor) são divulgados na internet, sendo facilmente acessados.

g. a execução orçamentária de TI, ao longo do exercício, é divulgada na internet, sendo facilmente acessada.

h. as respostas aos questionários dos levantamentos de governança de TI realizados pelo TCU, bem como os respectivos relatórios de *feedback*, são divulgados na internet, sendo facilmente acessados.

i. as informações sobre gestão e uso de TI divulgadas pela organização atendem aos princípios dos “Dados Abertos Governamentais” (http://dados.gov.br/dados-abertos).

Referências

Brasil. Lei 12.527/2011 (Lei de Acesso a Informações - LAI) – Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº8.159, de 8 de janeiro de 1991; e dá outras providências.

Art. 3º Os procedimentos previstos nesta Lei destinam-se a assegurar o direito fundamental de acesso à informação e devem ser executados em conformidade com os princípios básicos da administração pública e com as seguintes diretrizes:

I - observância da publicidade como preceito geral e do sigilo como exceção;

II - divulgação de informações de interesse público, independentemente de solicitações;

III - utilização de meios de comunicação viabilizados pela tecnologia da informação;

Art. 7º O acesso à informação de que trata esta Lei compreende, entre outros, os direitos de obter:

I - orientação sobre os procedimentos para a consecução de acesso, bem como sobre o local onde poderá ser encontrada ou obtida a informação almejada;

II - informação contida em registros ou documentos, produzidos ou acumulados por seus órgãos ou entidades, recolhidos ou não a arquivos públicos;

III - informação produzida ou custodiada por pessoa física ou entidade privada decorrente de qualquer vínculo com seus órgãos ou entidades, mesmo que esse vínculo já tenha cessado;

IV - informação primária, íntegra, autêntica e atualizada;

V - informação sobre atividades exercidas pelos órgãos e entidades, inclusive as relativas à sua política, organização e serviços;

VI - informação pertinente à administração do patrimônio público, utilização de recursos públicos, licitação, contratos administrativos; e

VII - informação relativa:

a) à implementação, acompanhamento e resultados dos programas, projetos e ações dos órgãos e entidades públicas, bem como metas e indicadores propostos;

b) ao resultado de inspeções, auditorias, prestações e tomadas de contas realizadas pelos órgãos de controle interno e externo, incluindo prestações de contas relativas a exercícios anteriores.

Art. 8º É dever dos órgãos e entidades públicas promover, independentemente de requerimentos, a divulgação em local de fácil acesso, no âmbito de suas competências, de informações de interesse coletivo ou geral por eles produzidas ou custodiadas.

*§ 1º Na divulgação das informações a que se refere o **caput**, deverão constar, no mínimo:*

II - registros de quaisquer repasses ou transferências de recursos financeiros;

III - registros das despesas;

IV - informações concernentes a procedimentos licitatórios, inclusive os respectivos editais e resultados, bem como a todos os contratos celebrados;

V - dados gerais para o acompanhamento de programas, ações, projetos e obras de órgãos e entidades; e

VI - respostas a perguntas mais frequentes da sociedade.

*§ 2º Para cumprimento do disposto no **caput**, os órgãos e entidades públicas deverão utilizar todos os meios e instrumentos legítimos de que dispuserem, sendo obrigatória a divulgação em sítios oficiais da rede mundial de computadores (internet).*

§ 3º Os sítios de que trata o § 2º deverão, na forma de regulamento, atender, entre outros, aos seguintes requisitos:

I - conter ferramenta de pesquisa de conteúdo que permita o acesso à informação de forma objetiva, transparente, clara e em linguagem de fácil compreensão;

II - possibilitar a gravação de relatórios em diversos formatos eletrônicos, inclusive abertos e não proprietários, tais como planilhas e texto, de modo a facilitar a análise das informações;

III - possibilitar o acesso automatizado por sistemas externos em formatos abertos, estruturados e legíveis por máquina;

IV - divulgar em detalhes os formatos utilizados para estruturação da informação;

V - garantir a autenticidade e a integridade das informações disponíveis para acesso;

VI - manter atualizadas as informações disponíveis para acesso;

VII - indicar local e instruções que permitam ao interessado comunicar-se, por via eletrônica ou telefônica, com o órgão ou entidade detentora do sítio;

Brasil. Tribunal de Contas da União. Acórdão 2.585/2012-TCU-Plenário.

9.1. recomendar ao Conselho Nacional de Justiça, Conselho Nacional do Ministério Público, Secretaria de Logística e Tecnologia da Informação e Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União, com fundamento na Lei nº 8.443/92, art. 43, inciso I, c/c Regimento Interno do TCU, art. 250, inciso III, que:
9.1.1. orientem as instituições sob sua jurisdição para que:

9.1.1.1. em atenção ao art. 6º da Lei nº 12.527/2011 e aos princípios da transparência e da prestação de contas, implementem instrumentos de planejamento estratégico institucional e de tecnologia da informação, dando-lhes ampla divulgação, com exceção das informações classificadas como não públicas, nos termos da lei;

9.1.1.4. em atenção ao art. 6º da Lei nº 12.527/2011, propiciem amplo acesso e divulguem as respostas ao questionário deste levantamento e as informações do relatório a ser encaminhado oportunamente pelo TCU, com exceção daquelas classificadas como não públicas nos termos da lei;
Brasil. Tribunal de Contas da União. Acórdão 1.233/2012-TCU-Plenário.

9.1. recomendar, com fundamento no art. 43, inciso I, da Lei 8.443/1992, c/c o art. 250, inciso III do Regimento Interno do TCU, à Câmara de Políticas de Gestão, Desempenho e Competitividade (CGDC) do Conselho de Governo que:

9.1.1 em atenção Decreto-Lei 200/1967, art. 6º, inciso I, e art. 7º, normatize a obrigatoriedade de que todos os entes sob sua jurisdição estabeleçam processo de planejamento estratégico institucional, observando as boas práticas sobre o tema, a exemplo do critério de avaliação 2 do Gespública, contemplando, pelo menos (subitem II.1):

9.1.1.4. divulgação do plano estratégico institucional para conhecimento dos cidadãos brasileiros, exceto nos aspectos formalmente declarados sigilosos ou restritos;

9.1.1.5. acompanhamento periódico do alcance das metas estabelecidas, para correção de desvios;

9.1.1.6. divulgação interna e externa do alcance das metas, ou dos motivos de não as ter alcançado;

9.1.2. em atenção Decreto-Lei 200/1967, art. 6º, inciso I, e art. 7º, normatize a obrigatoriedade de que todos os entes sob sua jurisdição estabeleçam processo de planejamento estratégico de TI, observando as boas práticas sobre o tema, a exemplo do processo "PO1 – Planejamento Estratégico de TI" do Cobit 4.1, contemplando, pelo menos (subitem II.2):

9.1.2.4. divulgação do plano estratégico de TI para conhecimento dos cidadãos brasileiros, exceto nos aspectos formalmente declarados sigilosos ou restritos;

9.1.2.5. acompanhamento periódico do alcance das metas estabelecidas, para correção de desvios;

9.1.2.6. divulgação interna e externa do alcance das metas, ou os motivos de não as ter alcançado;

9.15. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Conselho Nacional do Ministério Público (CNMP) que:

9.15.1. em atenção ao Decreto-Lei 200/1967, art. 6º, inciso I, e art. 7º, normatize a obrigatoriedade de que todos os entes sob sua jurisdição estabeleçam processo de planejamento estratégico institucional, observando as boas práticas sobre o tema, a exemplo do critério de avaliação 2 do Gespública, contemplando, pelo menos (subitem II.1):

9.15.1.4.divulgação do plano estratégico institucional para conhecimento dos cidadãos brasileiros, exceto nos aspectos formalmente declarados sigilosos ou restritos;

9.15.1.5. acompanhamento periódico do alcance das metas estabelecidas, para correção de desvios;

9.15.1.6. divulgação interna e externa do alcance das metas, ou dos motivos de não as ter alcançado;

9.15.2. em atenção ao Decreto-Lei 200/1967, art. 6º, inciso I, e art. 7º, normatize a obrigatoriedade de que todos os entes sob sua jurisdição estabeleçam processo de planejamento estratégico de TI, observando as boas práticas sobre o tema, a exemplo do processo "PO1 – Planejamento Estratégico de TI" do Cobit 4.1, contemplando, pelo menos (subitem II.2):

9.15.2.4. divulgação do plano estratégico de TI para conhecimento dos cidadãos brasileiros, exceto nos aspectos formalmente declarados sigilosos ou restritos;

9.15.2.5. acompanhamento periódico do alcance das metas estabelecidas, para correção de desvios;

9.15.2.6. divulgação interna e externa do alcance das metas, ou os motivos de não as ter alcançado;

Brasil. Departamento de Governo Eletrônico. Secretaria de Logística e Tecnologia da informação. Ministério do Planejamento, Orçamento e Gestão – Dados Abertos Governamentais.

Os Dados Abertos Governamentais são uma metodologia para a publicação de dados do governo em formatos reutilizáveis, visando o aumento da transparência e maior participação política por parte do cidadão, além de gerar diversas aplicações desenvolvidas colaborativamente pela sociedade.

Brasil. Secretaria de Logística e Tecnologia da informação. Ministério do Planejamento, Orçamento e Gestão – O que são dados abertos?

Segundo a definição da Open Knowledge Foundation, em suma, dados são abertos quando qualquer pessoa pode livremente usá-los, reutilizá-los e redistribuí-los, estando sujeito a, no máximo, a exigência de creditar a sua autoria e compartilhar pela mesma licença.

Isso geralmente é satisfeito pela publicação dos dados em formato aberto e sob uma licença aberta.

Os dados abertos também são pautados pelas três leis e oito princípios.

Brasil. Secretaria de Logística e Tecnologia da informação. Ministério do Planejamento, Orçamento e Gestão. Instrução Normativa 4/2012 – Institui a Infraestrutura Nacional de Dados Abertos – INDA.

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. COBIT - Control Objectives for Information and related Technology. COBIT 5 – Enabling Process.

p. 47 ***EDM05 Assegurar transparência para as partes interessadas*** *– Assegurar que a mensuração e a comunicação do desempenho e da conformidade da TI da organização são transparentes, com aprovação pelas partes interessadas dos objetivos, das métrica e das ações corretivas necessárias. Objetivo: Certificar que a comunicação com as partes interessadas é efetiva e tempestiva e a base para a comunicação está estabelecida para aumentar o desempenho, identificar áreas de melhoria e confirmar que os objetivos e as estratégias de TI estão alinhadas com a estratégia da organização (tradução livre).*

4. Pessoas

4.1. Com relação ao desenvolvimento de competências de TI:

a. a organização define as competências necessárias para o pessoal de TI executar suas atividades.
b. a organização define critérios para avaliação e atendimento dos pedidos de capacitação.
c. a organização elabora, periodicamente, plano de capacitação para suprir as necessidades de desenvolvimento de competências de TI.

d. a organização acompanha a execução do plano de capacitação, com identificação e correção de desvios.
e. a organização avalia a execução do plano de capacitação, verificando se os objetivos e resultados esperados foram alcançados.
f. o plano de capacitação inclui o desenvolvimento de competências em gestão de TI.
g. o plano de capacitação inclui o desenvolvimento de competências em contratação de bens e serviços de TI e na gestão dos contratos decorrentes.
h. a organização possui algum programa de benefício, financeiro ou não, para incentivar o desenvolvimento de competências do pessoal de TI.

Referências

Brasil. Decreto 5.707, de 23 de fevereiro de 2006.

Art. 2º Para os fins deste Decreto, entende-se por:

I - capacitação: processo permanente e deliberado de aprendizagem, com o propósito de contribuir para o desenvolvimento de competências institucionais por meio do desenvolvimento de competências individuais;

Art. 5º São instrumentos da Política Nacional de Desenvolvimento de Pessoal:

I - plano anual de capacitação;

II - relatório de execução do plano anual de capacitação; e

III - sistema de gestão por competência.

§ 1º Caberá à Secretaria de Gestão do Ministério do Planejamento, Orçamento e Gestão desenvolver e implementar o sistema de gestão por competência.

§ 2º Compete ao Ministro de Estado do Planejamento, Orçamento e Gestão disciplinar os instrumentos da Política Nacional de Desenvolvimento de Pessoal.

Art. 6º Os órgãos e entidades da administração pública federal direta, autárquica e fundacional deverão incluir em seus planos de capacitação ações voltadas à habilitação de seus servidores para o exercício de cargos de direção e assessoramento superiores, as quais terão, na forma do art. 9o da Lei no 7.834, de 6 de outubro de 1989, prioridade nos programas de desenvolvimento de recursos humanos.

Brasil. Tribunal de Contas da União. Acórdão 1.603/2008-TCU-Plenário.

9.1. recomendar ao Conselho Nacional de Justiça - CNJ e ao Conselho Nacional do Ministério Público - CNMP que, nos órgãos integrantes da estrutura do Poder Judiciário Federal e do Ministério Público da União, respectivamente:

9.1.2. atentem para a necessidade de dotar a estrutura de pessoal de TI do quantitativo de servidores efetivos necessário ao pleno desempenho das atribuições do setor, garantindo, outrossim, sua capacitação, como forma de evitar o risco de perda de conhecimento organizacional, pela atuação excessiva de colaboradores externos não comprometidos com a instituição;

9*.4. recomendar ao Ministério do Planejamento, Orçamento e Gestão - MPOG que, nos órgãos/entidades da Administração Pública Federal:*

9.4.2. atente para a necessidade de dotar a estrutura de pessoal de TI do quantitativo de servidores efetivos necessário ao pleno desempenho das atribuições do setor, garantindo, outrossim, sua capacitação, como forma de evitar o risco de perda de conhecimento organizacional, pela atuação excessiva de colaboradores externos não comprometidos com a instituição;

Brasil. Tribunal de Contas da União. Acórdão 1.233/2012-TCU-Plenário.

9.9. Recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Comitê Gestor da Política Nacional de Desenvolvimento de Pessoal que, em atenção ao Decreto 5.707/2006, art. 7º, II e IV:

9.9.1. oriente os órgãos e entidades sob sua jurisdição sobre a obrigatoriedade de aprovar o plano anual de capacitação, nos termos do Decreto 5.707/2006, arts. 5º e 2º, c/c Portaria MP 208/2006, art. 2º, I, e art. 4º (subitem II.9);

9.9.2. estabeleça, após consulta à Secretaria de Logística e Tecnologia da Informação, um programa de capacitação em governança e em gestão de tecnologia da informação (subitem II.9).

9.13. Recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Conselho Nacional da Justiça (CNJ) que:

9.13.10. oriente os órgãos e entidades sob sua jurisdição sobre a obrigatoriedade de aprovar o plano anual de capacitação, nos termos da Resolução - CNJ 90/2009, art. 3º (subitem II.9);

9.13.11. estabeleça um programa de capacitação em governança e em gestão de tecnologia da informação (subitem II.9);

9.15. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Conselho Nacional do Ministério Público (CNMP) que:

9.15.14. estabeleça a obrigatoriedade de que os órgãos e entidades sob sua jurisdição aprovem um plano anual de capacitação (subitem II.9);
9.15.15. estabeleça um programa de capacitação em governança e em gestão de tecnologia da informação (subitem II.9);

Brasil. Tribunal de Contas da União. Acórdão 1.233/2012-TCU-Plenário.

9.1. recomendar ao Conselho Nacional de Justiça, Conselho Nacional do Ministério Público, Secretaria de Logística e Tecnologia da Informação e Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União, com fundamento na Lei nº 8.443/92, art. 43, inciso I, c/c Regimento Interno do TCU, art. 250, inciso III, que:

9.1.1. orientem as instituições sob sua jurisdição para que:

9.1.2. se articulem com a Escola Nacional de Administração Pública e outras escolas de governo para ampliar a oferta de ações de capacitação em planejamento e gestão de contratos de tecnologia da informação para as instituições sob sua jurisdição;

4.2. Com relação ao desempenho do pessoal de TI:

a. a organização estabelece metas de desempenho para o pessoal de TI.

a. a organização avalia periodicamente o desempenho do pessoal de TI.

b. a organização estabelece benefício, financeiro ou não, em função do desempenho alcançado pelo pessoal de TI.

Referências

Brasil. Constituição da República Federativa do Brasil de 1998.
Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte:[...]

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. COBIT - Control Objectives for Information and related Technology. COBIT 5 – Enabling Process.

p. 86 ***APO07.04*** *Avaliar o desempenho do empregado – realizar avaliações de desempenho regulares em relação ao objetivos individuais decorrentes dos objetivos estratégicos, normas estabelecidas, responsabilidades específicas, e do quadro de competências e habilidades. Empregados devem receber treinamento em desempenho e conduta sempre que apropriado.*

4.3. Com relação à força de trabalho em TI, informe:

a. quantitativo previsto e aprovado como força de trabalho em TI.

b. quantitativo necessário (ideal) como força de trabalho em TI.

c. quantitativo total da força de trabalho existente (real) em TI.

d. quantitativo de servidores/empregados públicos efetivos da carreira de TI da própria instituição.

e. quantitativo de servidores/empregados públicos cedidos de outras instituições públicas.

f. quantitativo de servidores/empregados públicos não efetivos em cargos de livre nomeação.

g. quantitativo de estagiários.

h. quantitativo de terceirizados que trabalham regularmente no ambiente da instituição (contratos de serviços continuados com cessão de mão de obra).

i. quantitativo de terceirizados que trabalham no ambiente da instituição para execução de projetos de tempo determinado.

j. quantitativo de servidores/empregados públicos do quadro de TI que NÃO atuam na área de TI da instituição.

k. quantitativo de servidores/empregados públicos do quadro de TI que NÃO atuam na instituição.

l. outro(s). Qual(is)?

m. o quantitativo considerado ideal (item b) foi estimado com base em estudo técnico de avaliação quantitativa e qualitativa do quadro de pessoal da área de TI.

Referências

Brasil. Tribunal de Contas da União. Acórdão 1.603/2008-TCU-Plenário.

9.1.2. atentem para a necessidade de dotar a estrutura de pessoal de TI do quantitativo de servidores efetivos necessário ao pleno desempenho das atribuições do setor, garantindo, outrossim, sua capacitação, como forma de evitar o risco de perda de conhecimento organizacional, pela atuação excessiva de colaboradores externos não comprometidos com a instituição;

Brasil. Tribunal de Contas da União. Acórdão 1.233/2012-TCU-Plenário.

9.2. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, à Secretaria de Logística e Tecnologia da Informação (SLTI/MP) que:
9.2.2. oriente os órgãos e entidades sob sua jurisdição a realizar avaliação quantitativa e qualitativa do pessoal do setor de TI, de forma a delimitar as necessidades de recursos humanos necessárias para que estes setores realizem a gestão das atividades de TI da organização (subitem II.3);
9.11. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, à Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União (CGPAR) que:
9.11.2. oriente os órgãos e entidades sob sua jurisdição a realizar avaliação quantitativa e qualitativa do pessoal do setor de TI, de forma a delimitar as necessidades de recursos humanos necessárias para que estes setores realizem a gestão das atividades de TI da organização (subitem II.3);
9.13. Recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Conselho Nacional da Justiça (CNJ) que:
9.13.1. oriente os órgãos e entidades sob sua jurisdição a realizar avaliação quantitativa e qualitativa do pessoal do setor de TI, de forma a delimitar as necessidades de recursos humanos necessárias para que estes setores realizem a gestão das atividades de TI da organização (subitem II.3);
9.15. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Conselho Nacional do Ministério Público (CNMP) que:
9.15.4. oriente os órgãos e entidades sob sua jurisdição a realizarem avaliação quantitativa e qualitativa do pessoal do setor de TI, de forma a delimitar as necessidades de recursos humanos necessárias para que estes setores realizem a gestão das atividades de TI da organização (subitem II.3);

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. COBIT - Control Objectives for Information and related Technology. COBIT 5 – Enabling Process.

p. 84 ***APO07.01 Manter pessoal adequado e apropriado*** *– avaliar as necessidades de pessoal de forma regular ou quando ocorrerem mudanças no ambiente organizacional, operacional ou de TI, para assegurar que a organização tenha recursos humanos suficientes para suportar os objetivos e metas corporativos. Pessoal inclui recursos internos e externos.*

5. Processos

5.1. Com relação aos processos de gerenciamento de serviços de TI:

Desenho de serviço

a. a organização executa processo de gerenciamento do catálogo de serviços.
b. o processo de gerenciamento de gerenciamento do catálogo de serviços está formalmente instituído, como norma de cumprimento obrigatório.
c. a organização executa processo de gerenciamento da continuidade dos serviços de TI.
d. o processo de gerenciamento de continuidade dos serviços de TI está formalmente instituído, como norma de cumprimento obrigatório.

Transição de serviço

e. a organização executa processo de gerenciamento de mudanças.
f. o processo de gerenciamento de gerenciamento de mudanças está formalmente instituído, como norma de cumprimento obrigatório.
g. a organização executa processo de gerenciamento de configuração e ativos.
h. o processo de gerenciamento de gerenciamento de configuração e ativos está formalmente instituído, como norma de cumprimento obrigatório.
i. a organização executa processo de gerenciamento de liberação e implantação.
j. o processo de gerenciamento de liberação e implantação está formalmente instituído, como norma de cumprimento obrigatório.

Operação de serviço

k. a organização executa processo de gerenciamento de incidentes.
l. o processo de gerenciamento de gerenciamento de incidentes está formalmente instituído, como norma de cumprimento obrigatório.
m. a organização executa processo de gerenciamento de problemas.

n. o processo de gerenciamento de gerenciamento de problemas está formalmente instituído, como norma de cumprimento obrigatório.

Referências

Brasil. Tribunal de Contas da União. Acórdão 1.233/2012-TCU-Plenário.

9.2. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, à Secretaria de Logística e Tecnologia da Informação (SLTI/MP) que:

9.2.7. elabore um modelo de processo de gestão de serviços para os entes sob sua jurisdição que inclua, pelo menos, gestão de configuração, gestão de incidentes e gestão de mudança, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 20.000, Itil; subitem II.7);

9.2.8. estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem processos de gestão de serviços para si, incluindo, pelo menos, gestão de configuração, gestão de incidentes e gestão de mudança, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 20.000, Itil; subitem II.7);

9.11. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, à Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União (CGPAR) que:

9.11.8. estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem processos de gestão de serviços para si, incluindo, pelo menos, gestão de configuração, gestão de incidentes e gestão de mudança, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 20.000, Itil; subitem II.7);

9.13. Recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Conselho Nacional da Justiça (CNJ) que:

9.13.7. elabore um modelo de processo de gestão de serviços para os entes sob sua jurisdição que inclua, pelo menos, gestão de configuração, gestão de incidentes e gestão de mudança, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 20.000, Itil; subitem II.7);

9.13.8. estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem processos de gestão de serviços para si, incluindo, pelo menos, gestão de configuração, gestão de incidentes e gestão de mudança, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 20.000, Itil; subitem II.7);

9.15. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Conselho Nacional do Ministério Público (CNMP) que:

9.15.10. elabore um modelo de processo de gestão de serviços para os entes sob sua jurisdição que inclua, pelo menos, gestão de configuração, gestão de incidentes e gestão de mudança, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 20.000, Itil; subitem II.7);

9.15.11. estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem processos de gestão de serviços para si, incluindo, pelo menos, gestão de configuração, gestão de incidentes e gestão de mudança, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 20.000, Itil; subitem II.7);

itSMF. The IT Service Managent Forum. ITIL Version 3 Service Strategy.

p.186 5.3 Gerenciamento de Portfólio de Serviço (tradução livre)

p.201 5.5 Gerenciamento de Demanda (tradução livre)

itSMF. The IT Service Managent Forum. ITIL Version 3 Service Design.

p.101 4.1 Gerenciamento de Catálogo de Serviço (tradução livre)

p.216 4.5 Gerenciamento de Continuidade de Serviço de TI (tradução livre)

itSMF. The IT Service Managent Forum. ITIL Version 3 Service Transition.

p.77 4.2 Gerenciamento de Mudança (tradução livre)

p.118 4.3 Gerenciamento de Configuração e Ativo (tradução livre)

p.152 4.4 Gerenciamento de Liberação e Implantação (tradução livre)

itSMF. The IT Service Managent Forum. ITIL Version 3 Service Operation.

p.86 4.2 Gerenciamento de Incidente (tradução livre)

p.111 4.4 Gerenciamento de Problema (tradução livre)

5.2. Com relação ao gerenciamento de nível de serviço de TI:

a. a organização mantém um catálogo publicado e atualizado dos serviços de TI oferecidos às áreas clientes, incluindo os níveis de serviço definidos.
b. os níveis de serviço são formalmente definidos entre a área de TI e as áreas clientes (Acordo de Nível de Serviço - ANS).
c. os ANS incluem, como indicador de nível de serviço, o grau de satisfação dos usuários, apurado mediante a avaliação dos serviços de TI pelas áreas clientes.
d. a área de TI monitora o alcance dos níveis de serviço definidos.
e. a área de TI implementa ações corretivas em caso de não alcance dos níveis de serviço definidos.
f. a área de TI comunica periodicamente o resultado desse monitoramento às áreas clientes.

Referências

Brasil. Tribunal de Contas da União. Acórdão 1.603/2008-TCU-Plenário.

9.1. recomendar ao Conselho Nacional de Justiça - CNJ e ao Conselho Nacional do Ministério Público - CNMP que, nos órgãos integrantes da estrutura do Poder Judiciário Federal e do Ministério Público da União, respectivamente:

9.1.5. promovam ações voltadas à implantação e/ou aperfeiçoamento de gestão de níveis de serviço de TI, de forma a garantir a qualidade dos serviços prestados internamente, bem como a adequação dos serviços contratados externamente às necessidades da organização;

9.4. recomendar ao Ministério do Planejamento, Orçamento e Gestão - MPOG que, nos órgãos/entidades da Administração Pública Federal:

9.4.4. promova ações voltadas à implantação e/ou aperfeiçoamento de gestão de níveis de serviço de TI, de forma a garantir a qualidade dos serviços prestados internamente, bem como a adequação dos serviços contratados externamente às necessidades da organização;

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. ABNT NBR ISO 20000-2:2008 – Tecnologia da Informação – Gerenciamento de serviços – Parte 2: Código de Prática

p.8 ***6. Processo de entrega de serviços. 6.1 Gerenciamento do nível de serviço. 6.1.1 Catálogo de serviços*** *– Convém que um catálogo de serviços defina todos os serviços. Ele pode ser referenciado a partir do ANS e convém que seja usado para manter materiais considerados voláteis para o próprio ANS.Convém que o catálogo de serviços seja mantido e atualizado permanentemente. O catálogo de serviços é um documento-chave para estabelecer expectativas de clientes e convém que ele seja de fácil acesso e amplamente disponível para o cliente e para as equipes de suporte.* ***6.1.2 Acordos de Nível de Serviço (ANS)*** *– Convém que um serviço seja formalmente documentado em um acordo de nível de serviço (ANS). Convém que o ANS seja formalmente autorizado por representantes executivos do cliente e do provedor de serviços. Convém que o ANS esteja sujeito ao gerenciamento de mudanças, assim como o serviço que ele descreve. Convém que as necessidades e o orçamento da organização sejam a base para a definição para o conteúdo, estrutura e metas do ANS. Convém que as metas, em relação às quais convém que o serviço entregue seja medido, sejam definidas segundo a perspectiva do cliente.* ***6.1.3 O processo de gerenciamento do nível de serviços (GNS)*** *– A satisfação do cliente é uma parte importante do gerenciamento do nível de serviço, mas convém que ela seja reconhecida como uma medição subjetiva, enquanto que as metas dos serviços dentro de um ANS sejam medições objetivas. Convém que o processo de gerenciamento do nível de serviço trabalhe em conjunto com os processos de gerenciamento do relacionamento com a organização e de gerenciamento de fornecedores. Convém que o processo de gerenciamento do nível de serviço gerencie e coordene os contribuintes dos níveis de serviços, incluindo: a) concordância com os requisitos do serviço e características da carga de trabalho do serviço;b) acordo sobre as metas do serviço; c) medição e relato dos níveis de serviço alcançados, das cargas de trabalho e uma explicação se as metas acordadas não forem alcançadas (ver 6.2); d) iniciação de ação corretiva; e) entrada para um plano de melhoria do serviço.*

itSMF. The IT Service Managent Forum. ITIL Version 3 Service Design.

p.100 ***4.2 Gerenciamento de Nível de Serviço. 4.2.5 Atividades, Métodos e Técnicas do Processo*** *– As atividades-chave do processo de gerenciamento de nível de serviço (SLM) devem incluir: 1) determinar, negociar, documentar e acordar requisitos para mudanças ou novos serviços em Requisitos de Nível de Serviço (SLR), gerenciar e revisá-los através do ciclo de vida do serviço em Acordos de Nível de Serviço (SLA) para serviços operacionais; 2) Monitorar e mensurar o resultado do desempenho de todos os serviços operacionais em relação às metas definidas nos SLA; 3) Coletar, mensurar e melhorar a satisfação do cliente; 4) Produzir relatório de serviço; 5) Revisar SLA, escopo de serviço nos Acordos de Nível Operacional (OLA), contratos e qualquer outro acordo subjacente.*

5.3. Com relação à gestão de riscos de TI:

a. a organização identifica os riscos de TI dos processos críticos de negócio.

b. a organização avalia os riscos de TI dos processos críticos de negócio.

c. a organização trata os riscos de TI dos processos críticos de negócio com base em um plano de tratamento de risco.

d. a organização executa um processo de gestão de riscos de TI.

e. o processo de gestão de riscos de TI está formalmente instituído, como norma de cumprimento obrigatório.

Referências

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. ABNT NBR ISO/IEC 38500:2009 – Governança corporativa de tecnologia da informação.

p. 11 ***3.3 Princípio 2: Estratégia. Avaliar*** *– Convém que os dirigentes assegurem que a utilização de TI seja submetida à análise e avaliações de risco, de acordo com as devidas normas nacionais e internacionais.*

p. 13 ***3.5 Princípio 4: Desempenho. Avaliar*** *– Convém que os dirigentes avaliem proposições para assegurar que a TI apoiará os processos do negócio com a capacidade e competência necessárias. Convém que estas propostas enderecem a continuidade normal da operação dos negócios e o tratamento dos riscos associados com o uso da TI. Convém que os dirigentes avaliem os riscos à continuidade da operação resultantes das atividades de TI. Convém que os dirigentes avaliem os riscos à integridade da informação e à proteção dos ativos de TI, incluindo a propriedade intelectual e a base de conhecimentos da organização.*

p. 15 ***3.7 Princípio 6: Comportamento humano. Dirigir*** *– Convém que os dirigentes exijam que as atividades de TI sejam compatíveis com as diferenças do comportamento humano. Convém que os dirigentes exijam que riscos, oportunidades, constatações e preocupações possam ser identificados e relatados por qualquer pessoa a qualquer momento. Esses riscos devem ser gerenciados de acordo com as políticas e procedimentos publicados e levados ao conhecimento dos respectivos responsáveis pelas tomadas de decisão.*

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. COBIT - Control Objectives for Information and related Technology. COBIT 5 – Enabling Process.

p. 107 ***APO12 Gestão de riscos*** *– Continuamente identificar, avaliar e reduzir os riscos de TI para de níveis de tolerância estabelecidos pela organização* (tradução livre). *Objetivo: Integrar a gestão de risco organizacional associado ao uso de TI com a gestão de risco organizacional em geral, e equilibrar os custos e os benefícios da gestão de riscos de TI* (tradução livre).

p. 108 ***APO12.01 Coletar dados*** *– Identificar e coletar dados relevantes para viabilizar identificação, análise e comunicação de riscos de TI efetivas* (tradução livre).

p. 109 ***APO12.02 Analisar riscos*** *– Desenvolver informação útil para suportar decisões que levam em conta a relevância para o negócio dos fatores de riscos* (tradução livre).

p. 110 ***APO12.03 Manter um perfil de risco*** *– Manter um inventário de riscos conhecidos e de atributos de risco (incluindo frequência esperada, impacto potencial e respostas) e de recursos, capacidades e atividades de controle* (tradução livre). ***APO12.04 Comunicar risco*** *– Para possibilitar respostas apropriadas, fornecer informação tempestiva à partes interessadas a respeito do estado atual de exposições e oportunidades relacionadas ao uso da TI* (tradução livre). ***APO12.05 Definir um portfólio de ações para gerenciamento de risco*** *– Gerenciar oportunidades para reduzir riscos a níveis aceitáveis* (tradução livre).

p. 111 ***APO12.06 Responder aos riscos*** *– Responder de maneira tempestiva com medidas efetivas para limitar a magnitude de perda com eventos relacionados à TI* (tradução livre).

5.4. Com relação à gestão corporativa da segurança da informação:

Políticas e Responsabilidades

a. a organização dispõe de uma política de segurança da informação formalmente instituída, como norma de cumprimento obrigatório.

b. a organização dispõe de comitê de segurança da informação, formalmente instituído, responsável por formular e conduzir diretrizes para a segurança da informação corporativa, composto por representantes de áreas relevantes da organização.

c. a organização possui gestor de segurança da informação, formalmente designado, responsável pelas ações corporativas de segurança da informação.

d. a organização dispõe de política de controle de acesso à informação e aos recursos e serviços de TI formalmente instituída, como norma de cumprimento obrigatório.

e. a organização dispõe de política de cópias de segurança (*backup*) formalmente instituída, como norma de cumprimento obrigatório.

Controles e Atividades

f. a organização executa processo de gestão de ativos, assegurando a definição de responsabilidades e a manutenção de inventário dos ativos.

g. o processo de gestão de ativos está formalmente instituído, como norma de cumprimento obrigatório.

h. a organização executa processo para classificação e tratamento de informações.

i. o processo para classificação e tratamento de informações está formalmente instituído, como norma de cumprimento obrigatório.

j. a organização implementa controles para garantir a proteção adequada ao grau de confidencialidade de cada classe de informação.

k. a organização executa processo de gestão de riscos de segurança da informação.

l. o processo de gestão de riscos de segurança da informação está formalmente instituído, como norma de cumprimento obrigatório.

m. a organização executa processo de gestão de vulnerabilidades técnicas de TI, com objetivo de reduzir o risco de exploração de vulnerabilidades conhecidas.

n. o processo de gestão de vulnerabilidades técnicas de TI está formalmente instituído, como norma de cumprimento obrigatório.

o. a organização executa processo de monitoramento do uso dos recursos de TI, com objetivo de detectar atividades não autorizadas.

p. o processo de monitoramento do uso dos recursos de TI está formalmente instituído, como norma de cumprimento obrigatório.

q. a organização executa processo de gestão de incidentes de segurança da informação.

r. o processo de gestão de incidentes de segurança da informação está formalmente instituído, como norma de cumprimento obrigatório.

s. a organização possui equipe de tratamento e resposta a incidentes de segurança em redes computacionais, formalmente instituída.

t. a organização realiza, de forma periódica, ações de conscientização, educação e treinamento em segurança da informação para seus colaboradores.

u. a organização utiliza sistema criptográfico, aderente ao processo de certificação digital da ICP-Brasil, para garantir a autenticidade (autoria e integridade) das informações.

Referências

Brasil. Lei 12.527/2011 (Lei de Acesso a Informações - LAI) – Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº8.159, de 8 de janeiro de 1991; e dá outras providências.

Brasil. Decreto 7.845/2012 – Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.

Brasil. Presidência da República. Medida Provisória 2.200-2/2001 – Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.

Art. 1º Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

Art. 10º Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.

§ 1º As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei nº 3.071, de 1º de janeiro de 1916 - Código Civil.

Brasil. Tribunal de Contas da União. Acórdão 1.603/2008-TCU-Plenário.

9.1. recomendar ao Conselho Nacional de Justiça - CNJ e ao Conselho Nacional do Ministério Público - CNMP que, nos órgãos integrantes da estrutura do Poder Judiciário Federal e do Ministério Público da União, respectivamente:

9.1.3. orientem sobre a importância do gerenciamento da segurança da informação, promovendo, inclusive mediante normatização, ações que visem estabelecer e/ou aperfeiçoar a gestão da continuidade do negócio, a gestão de mudanças, a gestão de capacidade, a classificação da informação, a gerência de incidentes, a análise de riscos de TI, a área específica para gerenciamento da segurança da informação, a política de segurança da informação e os procedimentos de controle de acesso;

9.2. recomendar ao Gabinete de Segurança Institucional da Presidência da República - GSI/PR que oriente os órgãos/entidades da Administração Pública Federal sobre a importância do gerenciamento da segurança da informação, promovendo, inclusive mediante orientação normativa, ações que visem estabelecer e/ou aperfeiçoar a gestão da continuidade do negócio, a gestão de mudanças, a gestão de capacidade, a classificação da informação, a gerência de incidentes, a análise de riscos de TI, a área específica para gerenciamento da segurança da informação, a política de segurança da informação e os procedimentos de controle de acesso;

Brasil. Tribunal de Contas da União. Acórdão 1.233/2012-TCU-Plenário.

9.2. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, à Secretaria de Logística e Tecnologia da Informação (SLTI/MP) que:

9.2.9. em atenção ao Decreto-Lei 200/1967, art. 6º, V, estabeleça, normativamente para todos os entes sob sua jurisdição, a obrigatoriedade de a alta administração implantar uma estrutura de controles internos mediante a definição de atividades de controle em todos os níveis da organização para mitigar os riscos de suas atividades, pelo menos nos seguintes processos (subitem II.11):

9.2.9.7. segurança da informação;

9.8. Recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Gabinete de Segurança Institucional da Presidência da república (GSI/PR) que:

9.8.1. em atenção à Lei 10.168/2003, art. 6º, IV, articule-se com as escolas de governo, notadamente à Enap, a fim de ampliar a oferta de ações de capacitação em segurança da informação para os entes sob sua jurisdição (subitem II.8);

9.8.2. em atenção a Lei 10.168/2003, art. 6º, IV, oriente os órgãos e entidades sob sua jurisdição que a implantação dos controles gerais de segurança da informação positivados nas normas do GSI/PR não é faculdade, mas obrigação da alta administração, e sua não implantação sem justificativa é passível da sanção prevista na Lei 8.443/1992, art. 58, II (subitem II.8);

9.11. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, à Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União (CGPAR) que:

9.11.12. em atenção ao Decreto-Lei 200/1967, art. 6º, V, estabeleça, normativamente para todos os entes sob sua jurisdição, a obrigatoriedade de a alta administração implantar uma estrutura de controles internos mediante a definição de atividades de controle em todos os níveis da organização para mitigar os riscos de suas atividades, pelo menos nos seguintes processos (subitem II.11):

9.11.12. 8. segurança da informação;

9.13. Recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Conselho Nacional da Justiça (CNJ) que:

9.13.9. crie procedimentos para orientar os entes sob sua jurisdição na implementação dos seguintes controles (subitem II.8):

9.13.9.1. nomeação de responsável pela segurança da informação na organização, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 6.1.3 – Atribuição de responsabilidade para segurança da informação;

9.13.9.2. criação de comitê para coordenar os assuntos de segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 6.1.2 – Coordenação de segurança da informação;

9.13.9.3. processo de gestão de riscos de segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27005 – Gestão de riscos de segurança da informação;

9.13.9.4. estabelecimento de política de segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 5.1 – Política de segurança da informação;

9.13.9.5. processo de elaboração de inventário de ativos, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 7.1 – Inventário de ativos;

9.13.9.6. processo de classificação da informação, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 7.2 – Classificação da informação, processo necessário segundo o Decreto 4.553/2002, art. 6º, § 2º, inciso II, e art. 67;

9.13.14. em atenção ao Decreto-Lei 200/1967, art. 6º, V, estabeleça, normativamente para todos os entes sob sua jurisdição, a obrigatoriedade de a alta administração implantar uma estrutura de controles internos mediante a definição de atividades de controle em todos os níveis da organização para mitigar os riscos de suas atividades, pelo menos nos seguintes processos (subitem II.11):

9.13.14.8. segurança da informação;

9.15. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Conselho Nacional do Ministério Público (CNMP) que:

9.15.12. estabeleça a obrigatoriedade de que os entes sob sua jurisdição implementem os seguintes controles gerais de TI relativos à segurança da informação (subitem II.8):

9.15.12.1. nomeação de responsável pela segurança da informação na organização, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 6.1.3 – Atribuição de responsabilidade para segurança da informação;

9.15.12.2. criação de comitê para coordenar os assuntos de segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 6.1.2 – Coordenação de segurança da informação;

9.15.12.3. processo de gestão de riscos de segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27005 – Gestão de riscos de segurança da informação;

9.15.12.4. estabelecimento de política de segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 5.1 – Política de segurança da informação;

9.15.12.5. processo de elaboração de inventário de ativos, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 7.1 – Inventário de ativos;

9.15.12.6. processo de classificação da informação, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 7.2 – Classificação da informação, processo necessário segundo o Decreto 4.553/2002, art. 6º, § 2º, inciso II e art. 67;

9.15.13. crie procedimentos para orientar os entes sob sua jurisdição na implementação dos controles listados no item acima (subitem II.8);

9.15.18. em atenção ao Decreto-Lei 200/1967, art. 6º, V, estabeleça, normativamente para todos os entes sob sua jurisdição, a obrigatoriedade de a alta administração implantar uma estrutura de controles internos mediante a definição de atividades de controle em todos os níveis da organização para mitigar os riscos de suas atividades, pelo menos, nos seguintes processos (subitem II.11):

9.15.18.8. segurança da informação;

Brasil. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Norma Complementar 03/IN01/DSIC/GSIPR – Diretrizes para elaboração de política de segurança da informação e comunicações nos órgãos e entidades da Administração Pública Federal.

Brasil. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Norma Complementar 04/IN01/DSIC/GSIPR – Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC.

Brasil. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Norma Complementar 05/IN01/DSIC/GSIPR – Criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR.

Brasil. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Norma Complementar 07/IN01/DSIC/GSIPR – Diretrizes para Implementação de controles de Acesso Relativos à Segurança da Informação e Comunicações.

Brasil. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Norma Complementar 08/IN01/DSIC/GSIPR – Gestão de ETIR: Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos Órgãos e Entidades da Administração Pública Federal.

Brasil. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Norma Complementar 10/IN01/DSIC/GSIPR – Inventário e Mapeamento de Ativos de Informação nos Aspectos Relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal.

Brasil. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Norma Complementar 17/IN01/DSIC/GSIPR – Atuação e Adequações para

Profissionais da Área de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal.

Brasil. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Norma Complementar 18/IN01/DSIC/GSIPR – Diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal.

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. 6 ***4 Análise/avaliação e tratamento de riscos. 4.1. Analisando/avaliando os riscos de segurança da informação*** *– 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. Convém que a análise/avaliação de riscos inclua um enfoque sistemático de estimar a magnitude do risco (análise de riscos) e o processo de comparar os riscos estimados contra os critérios de risco para determinar a significância do risco (avaliação do risco).* ***4.2. Tratando os riscos de segurança da informação*** *– Convém que, antes de considerar o tratamento de um risco, a organização defina os critérios para determinar se os riscos podem ser ou não aceitos. Para cada um dos riscos identificados, seguindo a análise/avaliação de riscos, uma decisão sobre o tratamento do risco precisa ser tomada.*

p. 8 ***5 Política de segurança da informação. 5.1 Política de segurança da informação*** *– Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes. Convém que a direção estabeleça uma política clara, alinhada com os objetivos do negócio e demonstre apoio e comprometimento com a segurança da informação por meio da publicação e manutenção de uma política de segurança da informação para toda a organização.* ***5.1.1 Documento da política de 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 ***6 Organizando a segurança da informação. 6.1 Organização interna*** – Objetivo: Gerenciar a segurança da informação dentro da organização. *Convém que uma estrutura de gerenciamento seja estabelecida para iniciar e controlar a implementação da segurança da informação dentro da organização.*

p. 11 ***6.1.2 Coordenação da segurança da informação*** *– Convém que as atividades de segurança da informação sejam coordenadas por representantes de diferentes partes da organização, com funções e papéis relevantes.* ***6.1.3 Atribuição de responsabilidades para a segurança da informação*** *– Convém que todas as responsabilidades pela segurança da informação, estejam claramente definidas.*

p. 11 ***6.1.3 Atribuição de responsabilidades para a segurança da informação*** *– Convém que todas as responsabilidades pela segurança da informação, estejam claramente definidas. Em muitas organizações um gestor de segurança da informação pode ser indicado para assumir a responsabilidade global pelo desenvolvimento e implementação da segurança da informação e para apoiar a identificação de controles.*

p. 21 ***7 Gestão de ativos. 7.1 Responsabilidade pelos ativos*** *– Objetivo: Alcançar e manter a proteção adequada dos ativos da organização. Convém que todos os ativos sejam inventariados e tenham um proprietário responsável.* ***7.1.1 Inventário dos ativos*** *– Convém que todos os ativos sejam claramente identificados e um inventário de todos os ativos importantes seja estruturado e mantido.*

p. 22 ***7.1.2 Proprietário dos ativos*** *– Convém que todas as informações e ativos associados com os recursos de processamento da informação tenham um proprietário designado por uma parte definida da organização.* ***7.1.3 Uso aceitável dos ativos*** *– Convém que sejam identificadas, documentadas e implementadas regras para que sejam permitidos o uso de informações e de ativos associados aos recursos de processamento da informação.*

p. 23 ***7.2 Classificação da informação*** *– Objetivo: Assegurar que a informação receba um nível adequado de proteção. Convém que a informação seja classificada para indicar a necessidade, prioridades e o nível esperado de proteção quando do tratamento da informação.* ***7.2.1 Recomendações para classificação*** *– Convém que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para a organização.*

p. 24 ***7.2.2 Rótulos e tratamento da informação*** *– Convém que um conjunto apropriado de procedimentos para rotulação e tratamento da informação seja definido e implementado de acordo com o esquema de classificação adotado pela organização.*

p. 26 ***8 Segurança em recursos humanos. 8.2 Durante a contratação*** *– Objetivo: Assegurar que os funcionários, fornecedores e terceiros estão conscientes das ameaças e preocupações relativas à segurança da informação, suas responsabilidades e obrigações, e estão preparados para apoiar a política de segurança da informação da organização durante os seus trabalhos normais, e para reduzir o risco de erro humano. Convém que um nível adequado de conscientização, educação e treinamento nos procedimentos de segurança da informação e no uso correto dos recursos de processamento da informação seja fornecido para todos os funcionários, fornecedores e terceiros, para minimizar possíveis*

riscos de segurança da informação. ***8.2.2 Conscientização, educação e treinamento em segurança da informação*** *– Convém que todos os funcionários da organização e, onde pertinente, fornecedores e terceiros recebam treinamento apropriados em conscientização, e atualizações regulares nas políticas e procedimentos organizacionais, relevantes para as suas funções.*

p. 48 ***10.5 Cópias de segurança*** *– Objetivo: Manter a integridade e disponibilidade da informação e dos recursos de processamento de informação. Convém que procedimentos de rotina sejam estabelecidos para implementar as políticas de estratégias para a geração de cópias de segurança (ver 14.1) e possibilitar a geração das cópias de segurança dos dados e sua recuperação em um tempo aceitável.* ***10.5.1 Cópias de segurança das informações*** *– Convém que as cópias de segurança das informações e dos softwares sejam efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida.*

p. 60 ***10.10 Monitoramento*** *– Objetivo: Detectar atividades não autorizadas de processamento da informação. Convém que os sistemas sejam monitorados e eventos de segurança da informação sejam registrados.*

p. 61 ***10.10.1 Registros de auditoria*** *– Convém que registros (log) de auditoria contendo atividades dos usuários, exceções e outros eventos de segurança da informação sejam produzidos e mantidos por um período de tempo acordado para auxiliar em futuras investigações e monitoramento de controle de acesso.* ***10.10.2 Monitoramento do uso do sistema*** *– Convém que sejam estabelecidos procedimentos para o monitoramento do uso dos recursos de processamento da informação e os resultados das atividades de monitoramento sejam analisados criticamente, de forma regular.*

p. 65 ***11 Controle de acessos. 11.1 Requisitos de negócio para controle de acesso*** *– Objetivo: Controlar acesso à informação. Convém que o acesso à informação, recursos de processamento das informações e processos de negócios sejam controlados com base nos requisitos de negócio e segurança da informação.* ***11.1.1 Política de controle de acesso*** *– Convém que a política de controle de acesso seja estabelecida documentada e analisada criticamente, tomando-se como base os requisitos de acesso dos negócios e segurança da informação.*

p. 87 ***12.3 Controles criptográficos*** *– Objetivo: Proteger a confidencialidade, a autenticidade ou a integridade das informações por meios criptográficos. Convém que uma política seja desenvolvida para o uso de controles criptográficos. Convém que o gerenciamento de chaves seja implementado para apoiar o uso de técnicas criptográficas.*

p. 96 ***12.6 Gestão de vulnerabilidades técnicas*** *– Objetivo: Reduzir riscos resultantes da exploração de vulnerabilidades técnicas conhecidas. Convém que a implementação da gestão de vulnerabilidades técnicas seja implementada de forma efetiva, sistemática e de forma repetível com medições de confirmação da efetividade. Convém que estas considerações incluam sistemas operacionais e quaisquer outras aplicações em uso.*

p. 98 ***13 Gestão de incidentes de segurança da informação. 13.1 Notificação de fragilidades e eventos de segurança da informação*** – Objetivo: *Assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil. Convém que sejam estabelecidos procedimentos formais de registro e escalonamento.*

p. 100 ***13.2 Gestão de incidentes de segurança da informação e melhorias*** *– Objetivo: Assegurar que um enfoque consistente e efetivo seja aplicado à gestão de incidentes de segurança da informação. Convém que responsabilidades e procedimentos estejam definidos para o manuseio efetivo de eventos de segurança da informação e fragilidades, uma vez que estes tenham sido notificados. Convém que um processo de melhoria contínua seja aplicado às respostas, monitoramento, avaliação e gestão total de incidentes de segurança da informação.*

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. ABNT NBR ISO/IEC 27005:2008 – Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.

p. 4 **6** ***Visão geral do processo de gestão de riscos de segurança da informação*** *– O processo de gestão de riscos de segurança da informação consiste na definição do contexto (Seção 7), análise/avaliação de riscos (Seção 8), tratamento do risco (Seção 9), aceitação do risco (Seção 10), comunicação do risco (Seção 11) e monitoramento e análise crítica de riscos (Seção 12).*

p. 9 **7.4** ***Organização para gestão de riscos de segurança da informação*** *– Convém que a organização e as responsabilidades para o processo de gestão de riscos de segurança da informação sejam estabelecidas e mantidas.*

5.5. Com relação ao processo de software:

a. a organização executa um processo de software, para assegurar que o software a ser desenvolvido, direta ou indiretamente, atenda às suas necessidades.

b. o processo de software é acompanhado por meio de mensurações, com indicadores quantitativos e metas de processo a cumprir.

c. o processo de software é periodicamente revisado e melhorado com base nas mensurações obtidas.

d. a organização possui pessoal próprio capacitado para gerenciar o processo de software.

e. o processo de software está formalmente instituído, como norma de cumprimento obrigatório.

Referências

Brasil. Tribunal de Contas da União. Acórdão 1.233/2012-TCU-Plenário.

9.2. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, à Secretaria de Logística e Tecnologia da Informação (SLTI/MP) que:

9.2.3. elabore um modelo de processo de software para a os entes sob sua jurisdição, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 12.207 e 15.504, MPS.BR, CMMI; subitem II.5);

9.2.4. estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem um processo de software para si, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 12.207 e 15.504, MPS.BR, CMMI; subitem II.5);

9.3. determinar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso II, à Secretaria de Logística e Tecnologia da Informação (SLTI/MP) que:

9.3.1. em atenção ao previsto no Decreto 7.579/2011, art. 4º, V, oriente os entes sob sua jurisdição sobre a necessidade de vincular seus contratos de serviços de desenvolvimento ou manutenção de software a um processo de software, pois, sem esta vinculação, o objeto do contrato não estará precisamente definido, em desconformidade com o disposto na Lei 8.666/1993, art. 6º, inciso IX (subitem II.5);

9.11. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, à Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União (CGPAR) que:

9.11.4. elabore um modelo de processo de software para os entes sob sua jurisdição, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 12.207 e 15.504, MPS.BR, CMMI; subitem II.5);

9.11.5. estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem um processo de software para si, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 12.207 e 15.504, MPS.BR, CMMI; subitem II.5);

9.12. Determinar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso II, à Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União (CGPAR) que, em atenção ao previsto no Decreto 6.021/2007, art. 3º, I, b, oriente os entes sob sua jurisdição sobre necessidade de vincular seus contratos de serviços de desenvolvimento ou manutenção de software a um processo de software, pois, sem essa vinculação, o objeto do contrato não estará precisamente definido, em desconformidade com o disposto na Lei 8.666/1993, art. 6º, inciso IX (subitem II.5).

9.13. Recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Conselho Nacional da Justiça (CNJ) que:

9.13.3. elabore um modelo de processo de software para os entes sob sua jurisdição, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 12.207 e 15.504, MPS.BR, CMMI; subitem II.5);

9.13.4. estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem um processo de software para si, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 12.207 e 15.504, MPS.BR, CMMI; subitem II.5);

9.14. determinar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso II, ao Conselho Nacional de Justiça (CNJ) que:

9.14.1. em atenção ao previsto na Constituição Federal, art. 103-B, § 4º, II, oriente os entes sob sua jurisdição sobre necessidade de vincular seus contratos de serviços de desenvolvimento ou manutenção de software a um processo de software, pois, sem esta vinculação, o objeto do contrato não estará precisamente definido, em desconformidade com o disposto na Lei 8.666/1993, art. 6º, inciso IX (subitem II.5);

9.15. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Conselho Nacional do Ministério Público (CNMP) que:

9.15.6. elabore um modelo de processo de software para os entes sob sua jurisdição, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 12.207 e 15.504, MPS.BR, CMMI; subitem II.5);

9.15.7. estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem um processo de software para si, observando as boas práticas sobre o tema (e.g., NBR ISO/IEC 12.207 e 15.504, MPS.BR, CMMI; subitem II.5;

9.16. determinar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso II, ao Conselho Nacional do Ministério Público (CNMP) que:

9.16.1. em atenção ao previsto na Constituição Federal, art. 130-A, § 2º, II, oriente os entes sob sua jurisdição sobre necessidade de vincular seus contratos de serviços de desenvolvimento ou manutenção de software a um processo de software, pois, sem esta vinculação, o objeto do contrato não estará precisamente definido, em desconformidade com o disposto na Lei 8.666/1993, art. 6º, inciso IX (subitem II.5).

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. ABNT NBR ISO/IEC 12207:2009 – Engenharia de sistemas e software – Processos de ciclo de vida de software.

p.18 ***6. Processos de Ciclo de Vida de Sistema***

5.6. Com relação ao gerenciamento de projetos de TI:

a. a organização possui portfólio de projetos de TI.

b. a organização executa processo de gerenciamento de projetos de TI.

c. o processo de gerenciamento de projetos de TI é acompanhado por meio de mensurações, com indicadores quantitativos e metas de processo a cumprir.

d. o processo de gerenciamento de projetos de TI é periodicamente revisado e melhorado com base nas mensurações obtidas.

e. o processo de gerenciamento de projetos de TI está formalmente instituído, como norma de cumprimento obrigatório.

f. a organização possui um escritório de projetos, ao menos para projetos de TI.

Referências

Brasil. Tribunal de Contas da União. Acórdão 1.233/2012-TCU-Plenário.

9.2. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, à Secretaria de Logística e Tecnologia da Informação (SLTI/MP) que:

9.2.5. elabore um modelo de estrutura de gerenciamento de projetos para os entes sob sua jurisdição, observando as boas práticas sobre o tema (e.g., PMBoK; subitem II.6);

9.2.6. estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem um processo de gerenciamento de projetos para si, observando as boas práticas sobre o tema (e.g., PMBoK; subitem II.6);

9.11. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, à Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União (CGPAR) que:

9.11.6. elabore um modelo de estrutura de gerenciamento de projetos para os entes sob sua jurisdição, observando as boas práticas sobre o tema (e.g., PMBoK; subitem II.6);

9.11.7. estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem um processo de gerenciamento de projetos para si, observando as boas práticas sobre o tema (e.g., PMBoK; subitem II.6);

9.13. Recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Conselho Nacional da Justiça (CNJ) que:

9.13.5. elabore um modelo de estrutura de gerenciamento de projetos para os entes sob sua jurisdição, observando as boas práticas sobre o tema (e.g., PMBoK; subitem II.6);

9.13.6. estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem um processo de gerenciamento de projetos para si, observando as boas práticas sobre o tema (e.g., PMBoK; subitem II.6);

9.15. recomendar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso III, ao Conselho Nacional do Ministério Público (CNMP) que:

9.15.8. elabore um modelo de estrutura de gerenciamento de projetos para os entes sob sua jurisdição, observando as boas práticas sobre o tema (e.g., PMBoK; subitem II.6);

9.15.9. estabeleça a obrigatoriedade de que os entes sob sua jurisdição formalizem um processo de gerenciamento de projetos para si, observando as boas práticas sobre o tema (e.g., PMBoK; subitem II.6);

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

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. COBIT - Control Objectives for Information and related Technology. COBIT 5 – Enabling Process.

p.119 ***BAI01 Gerenciar Programas e Projetos. Finalidade do Processo –*** *Realizar benefício de negócio e reduzir o risco de atrasos inesperados, custos e valores extrapolados, por meio de melhoria da comunicação e do envolvimento do negócio com os usuários finais, assegurando o valor e a qualidade dos projetos entregues e maximizando sua contribuição para o portfólio de serviços e investimentos. (tradução livre).*

5.7. Com relação às contratações de serviços de TI:

a. a organização realiza estudos técnicos preliminares para avaliar a viabilidade da contratação.

b. a organização explicita, nos autos, as necessidades de negócio que se pretende atender com a contratação.

c. a organização explicita, nos autos, os indicadores dos benefícios de negócio que serão alcançados.

d. a organização explicita, nos autos, o alinhamento entre a contratação e os **planos** estratégico institucional e de TI **vigentes**.

e. a organização realiza análise dos riscos que possam comprometer o sucesso do processo de contratação e dos resultados que atendam as necessidades de negócio.

f. a organização adota métricas objetivas para mensuração de resultados do contrato.

g. a organização realiza os pagamentos dos contratos em função da mensuração objetiva dos resultados entregues e aceitos.

h. a organização realiza a análise dos benefícios reais já obtidos, utilizando-a como critério para prorrogar o contrato.

i. a organização diferencia e define formalmente os papéis de gestor e fiscal do contrato.

Referências

BRASIL. Tribunal de Contas da União. Guia de boas práticas em contratação de soluções de tecnologia da informação.

p.57 ***6.1 Estudos Técnicos Preliminares*** *– (...)a elaboração dos estudos técnicos preliminares constitui a primeira etapa do planejamento de uma contratação (planejamento preliminar) e serve essencialmente para:*

a) assegurar a viabilidade técnica da contratação, bem como o tratamento de seu impacto ambiental;

b) embasar o termo de referência ou o projeto básico, que somente é elaborado se a contratação for considerada viável, bem como o plano de trabalho, no caso de serviços, de acordo com exigência que consta no Decreto 2.271/1997, art. 2º.

p.62 ***6.1.1 Necessidade da contratação*** *- É a justificativa da contratação da solução de TI, decorrente da necessidade de atender a uma demanda do negócio.*

(...)
Adicionalmente, a gestão contratual deve ser executada usando como referência a necessidade da contratação (e.g. a decisão a respeito da conveniência ou não da prorrogação de um contrato deve ser feita com base na necessidade da contratação).
(...)
4.1) Sugestões de controles internos: (1) a alta administração deve publicar normativo definindo qual é a unidade gestora de cada solução de TI do órgão, que normalmente é a área requisitante da solução, e quais são as obrigações dessa unidade com relação à solução de TI. Entre essas obrigações deve estar incluída a verificação da pertinência da solução de TI em termos de negócio a cada prorrogação do contrato ou repactuação, observando aspectos como economicidade, eficácia e eficiência.

P.68 ***6.1.2 Alinhamento entre a contratação e os planos do órgão governante superior, do órgão e de TI do órgão*** *– é a indicação exata do alinhamento da contratação com elementos dos planos estratégicos e de TI do órgão governante superior ao qual o órgão está vinculado (e.g.CNJ ou SLTI), dos planos do órgão (e.g. planos estratégicos e diretores) e de TI do órgão (e.g. PDTI), bem como com as metas do Plano Plurianual (PPA). Isto é, a área requisitante, com o apoio da área de TI, deve explicitar como a contratação da solução de TI colabora para o alcance de objetivos estabelecidos nos planos citados.*

p.106 ***6.1.10 Resultados pretendidos*** *- os resultados pretendidos são os benefícios diretos que o órgão almeja com a contratação da solução, em termos de economicidade, eficácia, eficiência, de melhor aproveitamento dos recursos humanos, materiais e financeiros disponíveis, inclusive com respeito a impactos ambientais positivos (e.g. diminuição do consumo de papel ou de energia elétrica), bem como, se for caso, de melhoria da qualidade de produtos ou serviços, de forma a atender à necessidade da contratação.*

(...)

É de se esperar que pelo menos alguns dos resultados pretendidos sejam mensuráveis. Por exemplo, se o resultado esperado com uma determinada contratação é aumentar a produtividade de um processo de trabalho, esse resultado deve ser retratado em números. Assim, deve-se estabelecer um critério de medição, medir como o órgão tem executado o processo antes da contratação da solução e após a sua implantação, comparando as medidas pré e pós-implantação.

p.199 ***6.1.12 Análise de risco*** *- Análise dos riscos relativos à contratação e à gestão do contrato, que inclui as ações para mitigar os riscos identificados.*

p.152 ***6.3.6 Modelo de gestão do contrato*** *- O modelo de gestão do contrato deve contemplar as seguintes definições básicas:*

1) Definição de quais atores do órgão participarão das atividades de acompanhamento e fiscalização do contrato, bem como as atividades a cargo de cada um deles. É necessário definir os papéis dos vários atores envolvidos, sob pena do fiscal do contrato ficar sobrecarregado. Diversos atores participam da gestão contratual, entre os quais:

a) responsável pelo acompanhamento e fiscalização do contrato (fiscal do contrato), que efetua o recebimento provisório, no caso de serviços, de acordo com o art. 73, inciso I, alínea "a", da Lei 8.666/1993. No caso de compras ou locação de equipamentos, o recebimento provisório deve ocorrer de acordo com o art. 73, inciso II, alínea "a", da lei citada;

(...)

c) gestor do contrato: servidor com atribuições gerenciais, técnicas e operacionais relacionadas ao processo de gestão do contrato, indicado por autoridade competente, de acordo com a IN – SLTI 4/2010, art. 2º, inciso IV.

3) Definição da forma de pagamento do serviço, devidamente justificada: Trata do detalhamento dos valores ou percentuais que serão pagos ao longo da execução do contrato, com as devidas justificativas, lembrando que se deve estabelecer forma de pagamento que condicione a remuneração da contratada à entrega dos produtos ou serviços contratados. Por exemplo, pagamentos mensais de serviços contínuos, feitos após avaliação dos níveis de serviço entregues, ou pagamentos por produtos entregues em cada etapa de um serviço, de acordo com cronograma físico-financeiro.

5.8. Com relação ao processo de planejamento das contratações de TI:

a. a organização possui procedimentos internos que auxiliam na padronização das atividades de planejamento das contratações de TI.

b. a organização executa processo de planejamento das contratações de TI.

c. o processo de planejamento da contratação de TI é acompanhado por meio de mensurações, com indicadores quantitativos e metas de processo a cumprir.

d. o processo de planejamento da contratação de TI é periodicamente revisado e melhorado com base nas mensurações obtidas.

e. o processo de planejamento das contratações está formalmente instituído, como norma de cumprimento obrigatório.

Referências

BRASIL. Tribunal de Contas da União. Guia de boas práticas em contratação de soluções de tecnologia da informação.

p.51 ***5. Processo de planejamento da contratação de soluções de TI -*** *O planejamento da contratação de uma solução de TI, em termos conceituais, é um projeto, pois tem início, meio e fim. Entretanto, cada vez que uma contratação é realizada, o planejamento deve seguir essencialmente os mesmos passos, de maneira que haja previsibilidade com relação à execução e se garanta a aderência à legislação e à jurisprudência. Ou seja, cada contratação de solução de TI deve seguir um mesmo processo de trabalho.*

Para garantir que o processo de trabalho de planejamento da contratação de soluções de TI seja seguido de forma padronizada, torna-se necessária a sua formalização, divulgação e capacitação dos servidores envolvidos. Esse processo de trabalho deve ser publicado após sua aprovação pela alta administração do órgão.

p.231 ***8.4 Publicar políticas e normas*** *- Com a publicação de políticas e normas, diversas práticas necessárias à contratação e gestão de contratos de soluções de TI podem ser formalizadas e aprimoradas ao longo do tempo, tornando-as menos dependentes das pessoas que as executam e tornando mais simples a inserção de novos servidores nos processos de trabalho de contratação*

e gestão de soluções de TI.

5.9. Com relação ao processo de gestão dos contratos de TI:

a. a organização possui procedimentos internos que auxiliam na padronização das atividades de gestão de contratos de TI.

b. a organização executa processo de gestão de contratos de TI.

c. o processo de gestão de contratos de TI é acompanhado por meio de mensurações, com indicadores quantitativos e metas de processo a cumprir.

d. o processo formal de gestão de contratos de TI é periodicamente revisado e melhorado com base nas mensurações obtidas.

e. o processo de gestão de contratos está formalmente instituído, como norma de cumprimento obrigatório.

Referências

BRASIL. Tribunal de Contas da União. Guia de boas práticas em contratação de soluções de tecnologia da informação.

p.152 ***6.3.6 Modelo de gestão do contrato*** *- após o encerramento do processo licitatório e contratado o vencedor do certame para o fornecimento do objeto, inicia-se a fase de execução contratual. Nessa fase, compete à Administração garantir que a contratada cumpra os termos contratuais, de forma que o objeto do contrato seja fornecido nas condições estabelecidas.*

É na execução do contrato que o órgão alcança ou não os resultados pretendidos que atendam à necessidade que deu origem à contratação. A qualidade dessa etapa depende, em grande medida, dos trabalhos desenvolvidos na fase de planejamento da contratação, pois é no planejamento que as regras da gestão contratual são estabelecidas.

p.231 ***8.4 Publicar políticas e normas*** *- com a publicação de políticas e normas, diversas práticas necessárias à contratação e gestão de contratos de soluções de TI podem ser formalizadas e aprimoradas ao longo do tempo, tornando-as menos dependentes das pessoas que as executam e tornando mais simples a inserção de novos servidores nos processos de trabalho de contratação e gestão de soluções de TI.*

5.10. Com relação às contratações de TI (bens ou serviços) realizadas em 2013, informe:

a. contratações realizadas.

b. contratações que adotaram o sistema de registro de preço (RP), em que a própria organização foi gerenciadora da ata, com participação de outras instituições no planejamento (RP conjunto).

c. contratações que adotaram o sistema de registro de preço, em que a própria organização foi gerenciadora da ata, sem participação de outras instituições no planejamento (RP solitário).

d. contratações que adotaram o sistema de registro de preço, com a participação no planejamento inicial de outra organização, que foi a gestora da ata (participação em RP conjunto).

e. contratações por adesão tardia a ata de registro de preço ("carona"), sem participação no planejamento da contratação.

f. contratações por dispensa de licitação por contrato emergencial.

g. contratações por dispensa de licitação para contratar órgão/entidade da Administração Pública (Lei 8.666/1993, art. 24, VII ou XVI).

h. contratações por inexigibilidade de licitação.

Referências

Brasil. Lei 8.666, de 21 de junho de 1993.

Art. 15. As compras, sempre que possível, deverão:

II - ser processadas através de sistema de registro de preços;

§ 1o O registro de preços será precedido de ampla pesquisa de mercado.

§ 2o Os preços registrados serão publicados trimestralmente para orientação da Administração, na imprensa oficial.

§ 3o O sistema de registro de preços será regulamentado por decreto, atendidas as peculiaridades regionais, observadas as seguintes condições:

I - seleção feita mediante concorrência;

II - estipulação prévia do sistema de controle e atualização dos preços registrados;

III - validade do registro não superior a um ano.

Art. 24. É dispensável a licitação:

IV - nos casos de emergência ou de calamidade pública, quando caracterizada urgência de atendimento de situação que possa ocasionar prejuízo ou comprometer a segurança de pessoas, obras, serviços, equipamentos e outros bens, públicos ou particulares, e somente para os bens necessários ao atendimento da situação emergencial ou calamitosa e para as parcelas de obras e serviços que possam ser concluídas no prazo máximo de 180 (cento e oitenta) dias consecutivos e ininterruptos, contados da ocorrência da emergência ou calamidade, vedada a prorrogação dos respectivos contratos;

Art. 26. As dispensas previstas nos §§ 2o e 4o do art. 17 e no inciso III e seguintes do art. 24, as situações de inexigibilidade referidas no art. 25, necessariamente justificadas, e o retardamento previsto no final do parágrafo único do art. 8o desta Lei deverão ser comunicados, dentro de 3 (três) dias, à autoridade superior, para ratificação e publicação na imprensa oficial, no prazo de 5 (cinco) dias, como condição para a eficácia dos atos. (Redação dada pela Lei nº 11.107, de 2005)

Parágrafo único. O processo de dispensa, de inexigibilidade ou de retardamento, previsto neste artigo, será instruído, no que couber, com os seguintes elementos:

I - caracterização da situação emergencial ou calamitosa que justifique a dispensa, quando for o caso;

II - razão da escolha do fornecedor ou executante;

III - justificativa do preço.

IV - documento de aprovação dos projetos de pesquisa aos quais os bens serão alocados.

Art. 25. É inexigível a licitação quando houver inviabilidade de competição, em especial:

I - para aquisição de materiais, equipamentos, ou gêneros que só possam ser fornecidos por produtor, empresa ou representante comercial exclusivo, vedada a preferência de marca, devendo a comprovação de exclusividade ser feita através de atestado fornecido pelo órgão de registro do comércio do local em que se realizaria a licitação ou a obra ou o serviço, pelo Sindicato, Federação ou Confederação Patronal, ou, ainda, pelas entidades equivalentes;

II - para a contratação de serviços técnicos enumerados no art. 13 desta Lei, de natureza singular, com profissionais ou empresas de notória especialização, vedada a inexigibilidade para serviços de publicidade e divulgação;

III - para contratação de profissional de qualquer setor artístico, diretamente ou através de empresário exclusivo, desde que consagrado pela crítica especializada ou pela opinião pública.

Brasil. Tribunal de Contas da União. Acórdão 1.233/2012-TCU-Plenário.

9.3. determinar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso II, à Secretaria de Logística e Tecnologia da Informação (SLTI/MP) que:

9.3.2. em atenção ao disposto no Decreto 1.094/1994, art. 2º, inciso I, oriente os órgãos e entidades sob sua jurisdição para que (subitem III.1):

9.3.2.1. ao realizarem licitação com finalidade de criar ata de registro de preços atentem que:

9.3.2.1.1. devem fundamentar formalmente a criação de ata de registro de preços, e.g., por um dos incisos do art. 2º do Decreto 3.931/2001 (Acórdão 2.401/2006-TCU-Plenário);

9.3.2.1.2. devem praticar todos os atos descritos no Decreto 3.931/2001, art. 3º, § 2º, em especial o previsto no seu inciso I, que consiste em "convidar mediante correspondência eletrônica ou outro meio eficaz, os órgãos e entidades para participarem do registro de preços";

9.3.2.1.3. o planejamento da contratação é obrigatório, sendo que se o objeto for solução de TI, caso seja integrante do Sisp, deve executar o processo de planejamento previsto na IN - SLTI/MP 4/2010 (IN - SLTI/MP 4/2010, art. 18, inciso III) ou, caso não o seja, deve realizar os devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

9.3.2.1.4. a fixação, no termo de convocação, de quantitativos (máximos) a serem contratados por meio dos contratos derivados da ata de registro de preços, previstos no Decreto 3.931/2001, art. 9º, inciso II, é obrigação e não faculdade do gestor (Acórdão 991/2009-TCU-Plenário, Acórdão 1.100/2007-TCU-Plenário e Acórdão 4.411/2010-TCU-2ª Câmara);

9.3.2.1.5. em atenção ao princípio da vinculação ao instrumento convocatório (Lei 8.666/1993, art. 3º, caput), devem gerenciar a ata de forma que a soma dos quantitativos contratados em todos os contratos derivados da ata não supere o quantitativo máximo previsto no edital;

9.3.3. quando realizarem adesão à ata de registro de preços atentem que:

9.3.3.1. o planejamento da contratação é obrigatório, sendo que se o objeto for solução de TI, caso seja integrante do Sisp, deve executar o processo de planejamento previsto na IN - SLTI/MP 4/2010 (IN - SLTI/MP 4/2010, art. 18, inciso III) ou, caso não o seja, realizar os devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

9.3.3.2. devem demonstrar formalmente a vantajosidade da adesão, nos termos do Decreto 3.931/2001, art. 8º;

9.3.3.3. as regras e condições estabelecidas no certame que originou a ata de registro de preços devem ser conformes as necessidades e condições determinadas na etapa de planejamento da contratação (Lei 8.666/1993, art. 6º, inciso IX, alínea d, c/c o art. 3º, § 1º, inciso I, e Lei 10.520/2002, art. 3º, inciso II);

9.7. determinar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso II, à Departamento de Coordenação e Governança das Estatais (Dest/MP) que:

9.7.3. em atenção ao disposto no Decreto 7.063/2010, art. 6º, inciso XII, oriente as entidades sob sua jurisdição para que (subitem III.1):

9.7.3.1. ao realizarem licitação com finalidade de criar ata de registro de preços atentem que:

9.7.3.1.1. devem fundamentar formalmente a criação de ata de registro de preços, e.g., por um dos incisos do art. 2º do Decreto 3.931/2001 (Acórdão 2.401/2006-TCU-Plenário);

9.7.3.1.2. devem praticar todos os atos descritos no Decreto 3.931/2001, art. 3º, § 2º, em especial o previsto no seu inciso I, que consiste em "convidar mediante correspondência eletrônica ou outro meio eficaz, os órgãos e entidades para participarem do registro de preços";

9.7.3.1.3. o planejamento da contratação é obrigatório, sendo obrigatória a realização dos devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

9.7.3.1.4. a fixação, no termo de convocação, de quantitativos (máximos) a serem contratados por meio dos contratos derivados da ata de registro de preços, previstos no Decreto 3.931/2001, art. 9º, inciso II, é obrigação e não faculdade do gestor (Acórdão 991/2009-TCU-Plenário, Acórdão 1.100/2007-TCU-Plenário e Acórdão 4.411/2010-TCU-2ª Câmara);

9.7.3.1.5. em atenção ao princípio da vinculação ao instrumento convocatório (Lei 8.666/1993, art. 3º, caput), devem gerenciar a ata de forma que a soma dos quantitativos contratados em todos os contratos derivados da ata não supere o quantitativo máximo previsto no edital;

9.7.3.2. quando realizarem adesão à ata de registro de preços atentem que:

9.7.3.2.1. o planejamento da contratação é obrigatório, sendo obrigatória a realização dos devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

9.7.3.2.2. devem demonstrar formalmente a vantajosidade da adesão, nos termos do Decreto 3.931/2001, art. 8º;

9.7.3.2.3. as regras e condições estabelecidas no certame que originou a ata de registro de preços devem ser conformes as necessidades e condições determinadas na etapa de planejamento da contratação (Lei 8.666/1993, art. 6º, inciso IX, alínea d, c/c o art. 3º, § 1º, inciso I, e Lei 10.520/2002, art. 3º, inciso II);

9.14. determinar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso II, ao Conselho Nacional de Justiça (CNJ) que:

9.14.2. em atenção ao previsto na Constituição Federal, art. 103-B, § 4º, II, oriente os órgãos e entidades sob sua jurisdição para que (subitem III.1):

9.14.2.1. ao realizarem licitação com finalidade de criar ata de registro de preços atentem que:

9.14.2.1.1. devem fundamentar formalmente a criação de ata de registro de preços, e.g., por um dos incisos do art. 2º do Decreto 3.931/2001 (Acórdão 2.401/2006-TCU-Plenário);

9.14.2.1.2. devem praticar todos os atos descritos no Decreto 3.931/2001, art. 3º, § 2º, em especial o previsto no seu inciso I, que consiste em "convidar mediante correspondência eletrônica ou outro meio eficaz, os órgãos e entidades para participarem do registro de preços";

9.14.2.1.3. o planejamento da contratação é obrigatório, sendo obrigatória a realização dos devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

9.14.2.1.4. a fixação, no termo de convocação, de quantitativos (máximos) a serem contratados por meio dos contratos derivados da ata de registro de preços, previstos no Decreto 3.931/2001, art. 9º, inciso II, é obrigação e não faculdade do gestor (Acórdão 991/2009-TCU-Plenário, Acórdão 1.100/2007-TCU-Plenário e Acórdão 4.411/2010-TCU-2ª Câmara)

9.14.2.1.5. em atenção ao princípio da vinculação ao instrumento convocatório (Lei 8.666/1993, art. 3º, caput), devem gerenciar a ata de forma que a soma dos quantitativos contratados em todos os contratos derivados da ata não supere o quantitativo máximo previsto no edital;

9.14.3. quando realizarem adesão à ata de registro de preços atentem que:

9.14.3.1. o planejamento da contratação é obrigatório, sendo obrigatória a realização dos devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

9.14.3.2. devem demonstrar formalmente a vantajosidade da adesão, nos termos do Decreto 3.931/2001, art. 8º;

9.14.3.3. as regras e condições estabelecidas no certame que originou a ata de registro de preços devem ser conformes as necessidades e condições determinadas na etapa de planejamento da contratação (Lei 8.666/1993, art. 6º, inciso IX, alínea d, c/c o art. 3º, § 1º, inciso I, e Lei 10.520/2002, art. 3º, inciso II);

9.16. determinar, com fundamento na Lei 8.443/1992, art. 43, inciso I, c/c RITCU, art. 250, inciso II, ao Conselho Nacional do Ministério Público (CNMP) que:

9.16.2. em atenção ao previsto na Constituição Federal, art. 130-A, § 2º, II, oriente os órgãos e entidades sob sua jurisdição para que (subitem III.1):

9.16.2.1. ao realizarem licitação com finalidade de criar ata de registro de preços atentem que:

9.16.2.1.1devem fundamentar formalmente a criação de ata de registro de preços, e.g., por um dos incisos do art. 2º do Decreto 3.931/2001 (Acórdão 2.401/2006-TCU-Plenário);

9.16.2.1.2. devem praticar todos os atos descritos no Decreto 3.931/2001, art. 3º, § 2º, em especial o previsto no seu inciso I, que consiste em "convidar mediante correspondência eletrônica ou outro meio eficaz, os órgãos e entidades para participarem do registro de preços";

9.16.2.1.3. o planejamento da contratação é obrigatório, sendo obrigatória a realização dos devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

9.16.2.1.4. a fixação, no termo de convocação, de quantitativos (máximos) a serem contratados por meio dos contratos derivados da ata de registro de preços, previstos no Decreto 3.931/2001, art. 9º, inciso II, é obrigação e não faculdade do gestor (Acórdão 991/2009-TCU-Plenário, Acórdão 1.100/2007-TCU-Plenário e Acórdão 4.411/2010-TCU-2ª Câmara);

9.16.2.1.5. em atenção ao princípio da vinculação ao instrumento convocatório (Lei 8.666/1993, art. 3º, caput), devem gerenciar a ata de forma que a soma dos quantitativos contratados em todos os contratos derivados da ata não supere o quantitativo máximo previsto no edital;

19.16. 2.2. quando realizarem adesão à ata de registro de preços atentem que:

19.16. 2.2.1.o planejamento da contratação é obrigatório, sendo obrigatória a realização dos devidos estudos técnicos preliminares (Lei 8.666/1993, art. 6º, inciso IX);

19.16. 2.2.2. devem demonstrar formalmente a vantajosidade da adesão, nos termos do Decreto 3.931/2001, art. 8º;

19.16. 2.2.3. as regras e condições estabelecidas no certame que originou a ata de registro de preços devem ser conformes as necessidades e condições determinadas na etapa de planejamento da contratação (Lei 8.666/1993, art. 6º, inciso IX, alínea d, c/c o art. 3º, § 1º, inciso I, e Lei 10.520/2002, art. 3º, inciso II);

Brasil. Decreto 7.892, de 23 de janeiro de 2013 - Regulamenta o Sistema de Registro de Preços previsto no art. 15 da Lei 8.666, de 21 de junho de 2002.

6. Resultados de TI

6.1. Com relação aos objetivos de TI planejados pela organização, informe as metas mais relevantes para cumprimento em 2013 (até cinco):

Referências

Brasil. Tribunal de Contas da União. Acórdão 2.308/2010-TCU-Plenário.

9.1. recomendar ao Conselho Nacional de Justiça - CNJ, ao Departamento de Coordenação e Controle das Empresas Estatais - Dest, à Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão - SLTI/MPOG, ao Conselho Nacional do Ministério Público - CNMP, à Secretaria Geral da Presidência do Tribunal de Contas da União - Segepres/TCU, à Diretoria Geral da Câmara dos Deputados e à Diretoria Geral do Senado Federal que, no âmbito de suas respectivas áreas de atuação:

9.1.1. orientem as unidades sob sua jurisdição, supervisão ou estrutura acerca da necessidade de estabelecer formalmente: (i) objetivos institucionais de TI alinhados às estratégias de negócio; (ii) indicadores para cada objetivo definido, preferencialmente em termos de benefícios para o negócio da instituição; (iii) metas para cada indicador definido; (iv) mecanismos para que a alta administração acompanhe o desempenho da TI da instituição;

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. ABNT NBR ISO/IEC 38500:2009 – Governança corporativa de tecnologia da informação.

p. 6 ***2.2 Modelo.*** *Convém que os dirigentes governem TI através de três tarefas principais:* c) Monitorar o cumprimento das políticas e o desempenho em relação aos planos.

p. 11 ***3.3 Princípio 2: Estratégia. Monitorar*** *– Convém que os dirigentes monitorem o progresso das propostas de TI aprovadas para garantir que atinjam seus objetivos dentro dos prazos exigidos utilizando os recursos disponibilizados.*

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. COBIT - Control Objectives for Information and related Technology. COBIT 5 – Enabling Process.

p. 37 **EDM02.03 Monitorar otimização de valor** *– Monitorar os objetivos e as métricas principais para determinar em que medida o negócio está gerando o valor e os benefícios esperados para a organização por meio de investimentos e serviços de TI. Identificar problemas significativos e considerar ações corretivas* (tradução livre).

p. 44 **EDM04.03 Monitorar a gestão de recursos** – *Monitorar os objetivos e as métricas principais dos processos de gestão de recursos e estabelecer como desvios ou problemas serão identificados, acompanhados e reportados para remediação* (tradução livre).

p. 203 ***MEA01 Monitorar e avaliar desempenho e conformidade*** – *Coletar, validar e avaliar objetivos e métricas de negócio, TI e processos. Monitorar se os processos estão executados de acordo com metas e métricas de desempenho e conformidade acordadas e prover comunicação sistemática e tempestiva* (tradução livre).

6.2. Com relação aos projetos de TI:

Referências

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE - ITGI. COBIT - Control Objectives for Information and related Technology. COBIT 5 – Enabling Process.

p.35 ***EDM02 Assegurar a entrega de benefícios. Descrição do Processo*** – *Otimizar a contribuição de valor para o negócio a partir dos processos de negócio, serviços de TI e ativos de TI, resultantes dos investimentos em TI a custos aceitáveis.*

p.119 ***BAI01 Gerenciar Programas e Projetos. Finalidade do Processo –*** *Realizar benefício de negócio e reduzir o risco de atrasos inesperados, custos e valores extrapolados, por meio de melhoria da comunicação e do envolvimento do negócio com os usuários finais, assegurando o valor e a qualidade dos projetos entregues e maximizando sua contribuição para o portfólio de serviços e investimentos. (tradução livre).*

6.3. Com relação aos principais serviços de TI que sustentam as atividades da organização, informe:

Referências

Brasil. Tribunal de Contas da União. Acórdão 1.603/2008-TCU-Plenário.

9.1. recomendar ao Conselho Nacional de Justiça - CNJ e ao Conselho Nacional do Ministério Público - CNMP que, nos órgãos integrantes da estrutura do Poder Judiciário Federal e do Ministério Público da União, respectivamente:

9.1.5. promovam ações voltadas à implantação e/ou aperfeiçoamento de gestão de níveis de serviço de TI, de forma a garantir a qualidade dos serviços prestados internamente, bem como a adequação dos serviços contratados externamente às necessidades da organização;

9.4. recomendar ao Ministério do Planejamento, Orçamento e Gestão - MPOG que, nos órgãos/entidades da Administração Pública Federal:

9.4.4. promova ações voltadas à implantação e/ou aperfeiçoamento de gestão de níveis de serviço de TI, de forma a garantir a qualidade dos serviços prestados internamente, bem como a adequação dos serviços contratados externamente às necessidades da organização;

BRASIL. Associação Brasileira de Normas Técnicas - ABNT. ABNT NBR ISO 20000-2:2008 – Tecnologia da Informação – Gerenciamento de serviços – Parte 2: Código de Prática

p.8 ***6. Processo de entrega de serviços. 6.1 Gerenciamento do nível de serviço. 6.1.1 Catálogo de serviços*** – *Convém que um catálogo de serviços defina todos os serviços. Ele pode ser referenciado a partir do ANS e convém que seja usado para manter materiais considerados voláteis para o próprio ANS.Convém que o catálogo de serviços seja mantido e atualizado permanentemente. O catálogo de serviços é um documento-chave para estabelecer expectativas de clientes e convém que ele seja de fácil acesso e amplamente disponível para o cliente e para as equipes de suporte.* ***6.1.2 Acordos de Nível de Serviço (ANS)*** *– Convém que um serviço seja formalmente documentado em um acordo de nível de serviço (ANS). Convém que o ANS seja formalmente autorizado por representantes executivos do cliente e do provedor de serviços. Convém que o ANS esteja sujeito ao gerenciamento de mudanças, assim como o serviço que ele descreve. Convém que as necessidades e o orçamento da organização sejam a base para a definição para o conteúdo, estrutura e metas do ANS. Convém que as metas, em relação às quais convém que o serviço entregue seja medido, sejam definidas segundo a perspectiva do cliente.* ***6.1.3 O processo de gerenciamento do nível de serviços (GNS)*** *– A satisfação do cliente é uma parte importante do gerenciamento do nível de serviço, mas convém que ela seja reconhecida como uma medição subjetiva, enquanto que as metas dos serviços dentro de um ANS sejam medições objetivas. Convém que o processo de gerenciamento do nível de serviço trabalhe em conjunto com os processos de gerenciamento do relacionamento com a organização e de gerenciamento de fornecedores. Convém que o processo de gerenciamento do nível de serviço gerencie e coordene os contribuintes dos níveis de serviços, incluindo: a) concordância com os requisitos do serviço e características da carga de trabalho do serviço;b) acordo sobre as metas do serviço; c) medição e relato dos níveis*

de serviço alcançados, das cargas de trabalho e uma explicação se as metas acordadas não forem alcançadas (ver 6.2); d) iniciação de ação corretiva; e) entrada para um plano de melhoria do serviço.

itSMF. The IT Service Managent Forum. ITIL Version 3 Service Design.

p.100 ***4.2 Gerenciamento de Nível de Serviço. 4.2.5 Atividades, Métodos e Técnicas do Processo*** *– As atividades-chave do processo de gerenciamento de nível de serviço (SLM) devem incluir: 1) determinar, negociar, documentar e acordar requisitos para mudanças ou novos serviços em Requisitos de Nível de Serviço (SLR), gerenciar e revisá-los através do ciclo de vida do serviço em Acordos de Nível de Serviço (SLA) para serviços operacionais; 2) Monitorar e mensurar o resultado do desempenho de todos os serviços operacionais em relação às metas definidas nos SLA; 3) Coletar, mensurar e melhorar a satisfação do cliente; 4) Produzir relatório de serviço; 5) Revisar SLA, escopo de serviço nos Acordos de Nível Operacional (OLA), contratos e qualquer outro acordo subjacente.*

6.4. Com relação aos serviços disponíveis ao cidadão/cliente:

a. os serviços são acessíveis via internet.

b. os serviços acessíveis via internet implementam as recomendações do Modelo de Acessibilidade de Governo Eletrônico – eMAG, previsto no Programa de Governo Eletrônico Brasileiro.

c. os serviços acessíveis via internet implementam as diretrizes e as especificações dos Padrões de Interoperabilidade de Governo Eletrônico – ePING, previsto no Programa de Governo Eletrônico Brasileiro.

d. os serviços acessíveis via internet observam as recomendações dos Padrões Web em Governo Eletrônico – ePWG, previsto no Programa de Governo Eletrônico Brasileiro.

e. há catálogo publicado com informações claras e precisas em relação a cada um dos serviços acessíveis via internet.

f. os serviços acessíveis via internet são avaliados pelo cidadão/cliente por meio de pesquisas periódicas de satisfação.

g. os resultados das avaliações dos serviços acessíveis via internet são divulgados ao cidadão/cliente.

h. a organização possui perfil oficial em rede social com a finalidade de descobrir e atender às necessidades do cidadão/cliente.

Referências

Brasil. Lei 12.527/2011 (Lei de Acesso a Informações - LAI) – Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº8.159, de 8 de janeiro de 1991; e dá outras providências.

Art. 3º Os procedimentos previstos nesta Lei destinam-se a assegurar o direito fundamental de acesso à informação e devem ser executados em conformidade com os princípios básicos da administração pública e com as seguintes diretrizes:

I - observância da publicidade como preceito geral e do sigilo como exceção;

II - divulgação de informações de interesse público, independentemente de solicitações;

III - utilização de meios de comunicação viabilizados pela tecnologia da informação;

Art. 7º O acesso à informação de que trata esta Lei compreende, entre outros, os direitos de obter:

V - informação sobre atividades exercidas pelos órgãos e entidades, inclusive as relativas à sua política, organização e serviços;

Art. 8º É dever dos órgãos e entidades públicas promover, independentemente de requerimentos, a divulgação em local de fácil acesso, no âmbito de suas competências, de informações de interesse coletivo ou geral por eles produzidas ou custodiadas.

*§ 2º Para cumprimento do disposto no **caput**, os órgãos e entidades públicas deverão utilizar todos os meios e instrumentos legítimos de que dispuserem, sendo obrigatória a divulgação em sítios oficiais da rede mundial de computadores (internet).*

Brasil. Tribunal de Contas da União. Acórdão 1.386/2006-TCU-Plenário.

9.2. recomendar à Secretaria de Logística e Tecnologia da Informação, do Ministério do Planejamento, Orçamento e Gestão, como Secretaria-Executiva do CEGE e como órgão gestor do programa Governo Eletrônico (8002), que:

9.2.16. oriente os órgãos da APF para que realizem pesquisas junto aos usuários, após implementação de serviços eletrônicos, e disponibilizem os resultados à coordenação do Programa;

9.2.17 oriente os órgãos da APF para que identifiquem os serviços prioritários sob o ponto de vista do cidadão e avaliem sua adaptação ou implementação na Internet, com fixação de prazos e metas;

Brasil. Tribunal de Contas da União. Acórdão 2.585/2012-TCU-Plenário.

9.4. recomendar à Controladoria-Geral da União, com fundamento na Lei nº 8.443/92, art. 43, inciso I, c/c Regimento Interno do TCU, art. 250, inciso III, e em atenção ao art. 11 do Decreto nº 6.932/2009, que avalie, nas contas anuais dos órgãos/entidades sob sua jurisdição, o cumprimento da obrigação de divulgar os serviços prestados diretamente aos cidadãos, as formas de acesso a esses serviços e os respectivos compromissos e padrões de qualidade de atendimento ao público;

Brasil. Departamento de Governo Eletrônico. Secretaria de Logística e Tecnologia da informação. Ministério do Planejamento, Orçamento e Gestão – Programa de Governo Eletrônico Brasileiro.

O desenvolvimento de programas de Governo Eletrônico tem como princípio a utilização das modernas tecnologias de informação e comunicação (TICs) para democratizar o acesso à informação, ampliar discussões e dinamizar a prestação de serviços públicos com foco na eficiência e efetividade das funções governamentais.

Brasil. Departamento de Governo Eletrônico. Secretaria de Logística e Tecnologia da informação. Ministério do Planejamento, Orçamento e Gestão – Dados Abertos Governamentais.

Os Dados Abertos Governamentais são uma metodologia para a publicação de dados do governo em formatos reutilizáveis, visando o aumento da transparência e maior participação política por parte do cidadão, além de gerar diversas aplicações desenvolvidas colaborativamente pela sociedade.

Brasil. Departamento de Governo Eletrônico. Secretaria de Logística e Tecnologia da informação. Ministério do Planejamento, Orçamento e Gestão – Inclusão Digital.

O governo eletrônico também atua por meio da inclusão digital para que o cidadão exerça a sua participação política na sociedade do conhecimento. As iniciativas nessa área visam garantir a disseminação e o uso das tecnologias da informação e comunicação orientadas ao desenvolvimento social, econômico, político, cultural, ambiental e tecnológico, centrados nas pessoas, em especial nas comunidades e segmentos excluídos.

Brasil. Departamento de Governo Eletrônico. Secretaria de Logística e Tecnologia da informação. Ministério do Planejamento, Orçamento e Gestão – ePING – Padrões de Interoperabilidade de Governo Eletrônico.

A arquitetura ePING – Padrões de Interoperabilidade de Governo Eletrônico – define um conjunto mínimo de premissas, políticas e especificações técnicas que regulamentam a utilização da Tecnologia de Informação e Comunicação (TIC) no governo federal, estabelecendo as condições de interação com os demais Poderes e esferas de governo e com a sociedade em geral.

Brasil. Departamento de Governo Eletrônico. Secretaria de Logística e Tecnologia da informação. Ministério do Planejamento, Orçamento e Gestão – ePWG – Padrões Web em Governo Eletrônico.

Os Padrões Web em Governo Eletrônico (ePWG) são recomendações de boas práticas agrupadas em formato de cartilhas com o objetivo de aprimorar a comunicação e o fornecimento de informações e serviços prestados por meios eletrônicos pelos órgãos do Governo Federal.

Brasil. Departamento de Governo Eletrônico. Secretaria de Logística e Tecnologia da informação. Ministério do Planejamento, Orçamento e Gestão – eMAG - Modelo de Acessibilidade de Governo Eletrônico.

O Modelo de Acessibilidade de Governo Eletrônico (eMAG) consiste em um conjunto de recomendações a ser considerado para que o processo de acessibilidade dos sítios e portais do governo brasileiro seja conduzido de forma padronizada e de fácil implementação.

Brasil. Departamento de Governo Eletrônico. Secretaria de Logística e Tecnologia da informação. Ministério do Planejamento, Orçamento e Gestão – Sítios e e-Serviços.

Carta de Serviços - é um documento elaborado por uma organização pública que visa informar aos cidadãos quais os serviços prestados por ela, como acessar e obter esses serviços e quais são os compromissos de atendimento estabelecidos.

Indicadores e Métricas para Avaliação de e-Serviços - Projeto desenvolvido para avaliar a qualidade dos serviços públicos prestados por meios eletrônicos de acordo com a conveniência do cidadão. São 8 indicadores e 19 critérios que verificam a maturidade, comunicabilidade, confiabilidade, multiplicidade de acesso, disponibilidade, acessibilidade, facilidade de uso e nível de transparência do serviço prestado.

Brasil. Departamento de Governo Eletrônico. Secretaria de Logística e Tecnologia da informação. Ministério do Planejamento, Orçamento e Gestão – Redes Sociais.

No Brasil, uma das frentes fundamentais da política de Governo Eletrônico é a atuação junto ao cidadão, que deve ser incluído como produtor de conhecimento coletivo.

Dessa forma, a conduta recomendada pelo governo federal é a de que os perfis governamentais promovam a interação, reconhecendo que esses instrumentos de propagação são formas que o Estado tem para quebrar barreiras e buscar o diálogo e a aproximação do cidadão. Os administradores dos perfis nas redes sociais devem buscar sugestões para as políticas do governo, utilizar estratégias para estimular a interação com os usuários, disseminar boas práticas e promover respostas ágeis aos questionamentos feitos pelos usuários.