Programa de Auditoria (PA)
Governança de Tecnologia da Informação

Ação Coordenada de Auditoria 2018

1. **Área a ser auditada:**

Sistema de Governança da Tecnologia da Informação – Unidade Técnica responsável pela Tecnologia da Informação e Comunicação.

2. **Objetivo:**

Avaliar os conteúdos estabelecidos para a governança e gestão de TI, considerando projetos, processos, riscos e resultados de TI em comparação com padrões internacionalmente aceitos, como COBIT, PMBOK, ITIL, CMMI, ISO 17799, ISO 27001, as Resoluções CNJ nº 91/2009, nº 182/2013, nº 198/2014 e nº 211/2015 e o perfil de governança de TI traçado pelo TCU.

3. **Escopo:**

Serão examinados os conteúdos dos planos de tecnologia da informação, dos controles de governança, de gestão, de riscos e de resultados de TI.

4. **Período da auditoria:** 02 de maio a 30 de junho de 2018.

5. **Equipe de auditoria:**
   - Indicação a cargo da Unidade de Auditoria Interna (UAI) do tribunal, conselho ou seção judiciária.

6. **Custo do trabalho:**

Não está prevista a utilização de diárias, passagens ou ajuda de custo pela equipe. Os custos previstos são aqueles inerentes ao valor-hora dos servidores envolvidos.

7. **Questões de Auditoria:**

1ª) Existem políticas e diretrizes definidas para governança e gestão de tecnologia da informação?
2ª) Os planos estratégicos institucional e de TI fornecem suporte apropriado à governança e à gestão de TI?
3ª) As necessidades relacionadas ao desenvolvimento de pessoas e à força de trabalho da área de TI são gerenciadas?
4ª) Os processos de gestão de TI são gerenciados?
5ª) O processo de planejamento de contratação de TI está sendo executado de acordo com o disposto na Resolução CNJ nº 182/2013?
6ª) Os resultados apresentados pela TI são dimensionados?
7ª) A Unidade de Auditoria Interna (UAI) realiza exames de auditoria na área de TIC para aferir o estágio da governança e gestão de TI?

7.1. 1ª Questão de auditoria:

- Existem políticas e diretrizes definidas para a governança e gestão de tecnologia da informação?

7.1.1. Informações requeridas:

a) Definição dos papéis e responsabilidades na governança corporativa e de TI;
b) Instituição e atuação de comitê de TI;
c) Política de gestão de riscos;
d) Política de gestão de continuidade do negócio;
e) Diretrizes para o planejamento de TI;
f) Diretrizes para contratação de bens e serviços de TI;
g) Diretrizes para avaliação do desempenho dos serviços de TI;
h) Diretrizes para gestão dos riscos de TI;
i) Diretrizes para desenvolvimento de competências e retenção de gestores e técnicos de TI;
j) Diretrizes para avaliação e incentivo ao desempenho de gestores e técnicos de TI;
k) Diretrizes para escolha dos líderes da área de TI;
l) Diretrizes para comunicação com o público interno e externo sobre os resultados da gestão e do uso de TI; e
m) Diretrizes para avaliação da governança e da gestão de TI.

7.1.2. Fontes de Informação:

a) Referencial Básico de Governança do TCU;
b) ABNT NBR ISO 31000:2009 – Gestão de riscos – princípios e diretrizes;
c) ABNT NBR ISO 22313:2015 – Sistemas de gestão de continuidade de negócios;
d) ABNT NBR ISO 38500:2009 – Governança corporativa de tecnologia da informação;
e) COBIT 5 – *Control Objectives for Information and related Technology*;
f) Acórdão TCU nº 1.603/2008 – Plenário;
g) Acórdão TCU nº 2.308/2010 – Plenário;
h) Acórdão TCU nº 1.233/2012 – Plenário;
i) Acórdão TCU nº 2.585/2012 – Plenário; e
j) Resolução CNJ nº 211/2015.

7.1.3. Procedimentos:

Descrição dos Procedimentos	Referência PT	Membro da equipe responsável	Observações
Verificar se há definição dos papéis e responsabilidades para a governança e gestão de TI. Caso positivo, verificar se os responsáveis são formalmente comunicados. Verificar se existe Comitê de Governança de TI formalmente instituído. Caso positivo, verificar se: • é composto por representantes de	(Nº do Papel de Trabalho e referência) .		COBIT 5. Resolução CNJ nº 211/2015.

áreas relevantes da organização, incluindo magistrado(s); • realiza as atividades previstas em seu ato constitutivo; e • efetivamente auxilia o órgão a priorizar as ações de TI.			
Verificar se existe Comitê de Gestão de TI. **Caso positivo**, verificar se: • elabora planos táticos e operacionais; • realiza análise das demandas de TI; • acompanha a execução de planos de TI; e • estabelece indicadores operacionais.			Resolução CNJ nº 211/2015.
Verificar se existem diretrizes formais para: • planejamento de TI; • gestão do portfólio de projetos e de serviços de TI; • contratação de bens e serviços de TI; e • avaliação do desempenho dos serviços de TI.			ISO 38500; Acórdão TCU nº 1.603/2008 - Plenário.
Verificar se existe política formal para a gestão de riscos de TI. **Caso positivo,** verificar se: • os papéis e responsabilidades de riscos de TI são definidos e comunicados formalmente; • os níveis de risco de TI aceitáveis são definidos; e • são tomadas decisões estratégicas considerando os níveis de risco de TI definidos.			ISO 31000; COBIT 5.
Verificar se existem políticas formais para: • gestão de pessoas, de forma a promover o desenvolvimento de competências e a retenção de gestores e técnicos de TI; • avaliação e incentivo ao desempenho de gestores e técnicos de TI; e • escolha dos líderes da área de TI, ocupantes de cargos de chefia e de assessoramento.			Resolução CNJ nº 211/2015; Acórdão TCU nº 1.233/2012 - Plenário; ISO 38500; COBIT 5.

Verificar se existem diretrizes para comunicação com as partes interessadas, considerando os públicos interno e externo, sobre os resultados da gestão e do uso de TI. **Caso positivo,** verificar se contempla: • a divulgação; • o conteúdo; • a frequência; e • o formato das comunicações. Verificar se existem diretrizes para avaliação da governança e da gestão de TI. **Caso positivo**, verificar se são realizadas avaliações periódicas de: • governança e de gestão de TI; • sistemas de informação; • segurança da informação; e • contratos de TI. Verificar se foram instituídas políticas de: • controle de acesso à informação, aos recursos e serviços de TI; e • cópia de segurança (*backup*).			ISO 38500; COBIT 5; Acórdão TCU nº 2.585/2012 – Plenário; ISO 38500; COBIT 5. ISO 27002:05

7.1.4. Possíveis achados:

- Ausência de definição de papéis e responsabilidades de TI;
- Ausência de designação formal dos papéis e responsabilidades de TI;
- Ausência de Comitê de Governança de TI e/ou de Comitê de Gestão de TI;
- Ausência de participação do Comitê de Governança de TI e/ou de Comitê de Gestão de TI nas decisões que requerem a sua manifestação;
- Ausência de política de gestão de riscos ou sua não aplicação;
- Ausência de incentivos para desenvolvimento e retenção de pessoal de TI;
- Ausência de comunicação com partes interessadas sobre os resultados de TI; e
- Ausência de avaliação da governança e/ou gestão de TI.

7.2. 2ª Questão de auditoria:

- Os planos estratégicos institucional e de TI fornecem suporte apropriado à governança e à gestão de TI?

7.2.1. Informações requeridas:

a) Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-Jud);
b) Plano Estratégico Institucional (PEI);
c) Plano Estratégico de Tecnologia da Informação e Comunicação (PETIC); e
d) Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC).

7.2.2. Fontes de Informação:

a) Decreto-Lei nº 200, de 25 de fevereiro de 1967;
b) Resolução CNJ nº 182/2013;
c) Resolução CNJ nº 198/2014;
d) Resolução CNJ nº 211/2015;
e) Acórdão TCU nº 1.603/2008 – Plenário;
f) Acórdão TCU nº 2.308/2010 – Plenário;
g) Acórdão TCU nº 1.233/2012 – Plenário;
h) Acórdão TCU nº 2.585/2012 – Plenário; e
i) Lei nº 12.527/2011 – Lei de Acesso a Informações (LAI).

7.2.3. Procedimentos:

Descrição dos Procedimentos	Referência PT	Membro da Equipe responsável	Observações
Verificar se a área de TI participou do processo de formulação do Plano Estratégico Institucional. Verificar se existe Plano Estratégico de Tecnologia da Informação e Comunicação (PETIC) formalmente instituído e vigente. Caso positivo, verificar se: • o processo de formulação contou com a participação de áreas relevantes da organização; • o plano está alinhado às diretrizes estratégicas institucionais e nacionais, conforme disposto na Resolução CNJ nº 198/2014; • o plano contempla objetivos, indicadores e metas de TI, com objetivos explicitamente alinhados aos objetivos de negócio; • o plano fundamenta a proposta	(Nº do Papel de Trabalho e referência).		Acórdão TCU nº 1.603/2008 – Plenário; Acórdão TCU nº 1.233/2012 - Plenário. Resolução CNJ nº 211/2015; Acórdão TCU nº 1.603/2008 – Plenário; Acórdão TCU nº 2.308/2010 - Plenário; Acórdão nº 1.233/2012 - Plenário; Acórdão TCU nº 2.585/2012 - Plenário; COBIT 5.

orçamentária de TI; • a execução é acompanhada periodicamente; e • o plano é revisado periodicamente. Verificar se existe Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) formalmente instituído e vigente. **Caso positivo,** verificar se: • o processo de formulação do PDTI é apoiado pelo Comitê de TI; • contempla as ações a serem desenvolvidas com vinculação às estratégias institucional e nacional do Poder Judiciário; • o plano vincula as ações e projetos a indicadores e metas de negócio; • a execução é acompanhada periodicamente; e • o plano é revisado periodicamente. Verificar se os planos de TI são divulgados por meio de fácil acesso. Verificar se existem planos, além do PETIC ou PDTIC, voltados a atender aos objetivos estratégicos institucionais vinculados à área de TI do órgão.			Resolução CNJ nº 211/2015; Acórdão TCU nº 1.603/2008 - Plenário; Acórdão TCU nº 2.308/2010 - Plenário; Acórdão TCU nº 1.233/2012 - Plenário; Acórdão TCU nº 2.585/2012 – Plenário; COBIT 5. Acórdão TCU nº 2.585/2012 - Plenário; Acórdão TCU nº 1.233/2012 - Plenário; COBIT 5.
7.2.4. Possíveis achados:			
• Ausência de participação da área de TI na construção do Plano Estratégico Institucional (PEI); • Ausência de Plano Estratégico de Tecnologia da Informação e Comunicação (PETIC); • Ausência de Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC); e • Ausência de divulgação dos planos de TI.			

7.3. 3ª Questão de auditoria:

- As necessidades relacionadas ao desenvolvimento de pessoas e à força de trabalho da área de TI são gerenciadas?

7.3.1. Informações requeridas:

a) Definição das competências necessárias para o pessoal de TI;
b) Plano de capacitação para o pessoal de TI;
c) Metas de desempenho para o pessoal de TI; e
d) Quantitativos da força de trabalho de TI.

7.3.2. Fontes de Informação:

a) Decreto nº 5.707/2006;
b) COBIT 5 – *Control Objectives for Information and related Technology*;
c) Acórdão TCU nº 1.603/2008 – Plenário;
d) Acórdão TCU nº 1.233/2012 – Plenário; e
e) Resolução CNJ nº 211/2015.

7.3.3. Procedimentos:

Descrição dos Procedimentos	Referência PT	Membro da Equipe responsável	Observações
Verificar se foram definidas as competências necessárias para o pessoal de TI executar suas atividades. Verificar se existe Plano Anual de Capacitação para o pessoal de TI. **Caso positivo**, verificar se: • o plano é revisado periodicamente; • há diretrizes para avaliação e atendimento aos pedidos de capacitação em TI; • inclui o desenvolvimento de competências em governança e gestão de TI; • inclui o desenvolvimento de competências em contratação de bens e serviços de TI e em gestão de contratos; e • há acompanhamento da execução do plano, inclusive dos objetivos e resultados esperados. Verificar se existem metas de desempenho para o pessoal de TI. **Caso positivo**, verificar se o desempenho é acompanhado periodicamente.	(Nº do Papel de Trabalho e referência).		Resolução CNJ nº 211/2015 Acórdão TCU nº 1.603/2008 Resolução CNJ nº 211/2015 Acórdão TCU nº 1.233/2012

Verificar se foram previstos e aprovados os quantitativos ideais de força de trabalho de TI. **Caso positivo**, verificar se os quantitativos previstos foram estimados com base no: a) estudo técnico que indica o número de usuários internos e externos de recursos de TI; e b) anexo da Resolução CNJ nº 211/2015.			Resolução CNJ nº 211/2015 COBIT 5 (APO 07.04) Resolução CNJ nº 211/2015 Acórdão TCU nº 1.603/2008 Acórdão TCU nº 1.233/2012 COBIT 5 (APO 07.01)
7.3.4. Possíveis achados:			
• Ausência de definição das competências necessárias para o pessoal de TI; • Ausência de Plano Anual de Capacitação para o pessoal de TI; • Ausência de acompanhamento dos resultados do Plano Anual de Capacitação da TI; • Ausência de acompanhamento do desempenho do pessoal de TI; e • Ausência de previsão dos quantitativos ideais da força de trabalho de TI ou previsão sem embasamento técnico.			

7.4. 4ª Questão de auditoria:

- Os processos de gestão de TI são gerenciados?

7.4.1. Informações requeridas:

a) Catálogo de serviços de TI;
b) Níveis de serviço definidos;
c) Riscos de TI identificados;
d) Política de segurança da informação;
e) Política de controle de acesso à informação e aos recursos de TI;
f) Política de cópias de segurança (*backup*);
g) Processo de *software* definido;
h) Portfólio de projetos de TI; e
i) Processo de gerenciamento de projetos definido.

7.4.2. Fontes de Informação:

a) Lei nº 12.527/2011 – Lei de Acesso a Informações (LAI);
b) Medida Provisória nº 2.200-2, de 24 de agosto de 2001 (ICP-Brasil);
c) Norma Complementar nº 03/IN01/DSIC/GSIPR – Diretrizes para elaboração de política de segurança da informação e comunicações nos órgãos e entidades da Administração Pública Federal;
d) Norma Complementar nº 04/IN01/DSIC/GSIPR – Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC;
e) Norma Complementar nº 05/IN01/DSIC/GSIPR – Criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR;
f) Norma Complementar nº 07/IN01/DSIC/GSIPR – Diretrizes para Implementação de controles de Acesso Relativos à Segurança da Informação e Comunicações;
g) Norma Complementar nº 08/IN01/DSIC/GSIPR – Gestão de ETIR: Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos Órgãos e Entidades da Administração Pública Federal;
h) 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;
i) 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;
j) 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;
k) *ITIL Version 3 – Service Strategy*;
l) *ITIL Version 3 – Service Design;*
m) *ITIL Version 3 – Service Transition*;
n) *ITIL Version 3 – Service Operation*;
o) COBIT 5 – *Control Objectives for Information and related*;

p) *PMBoK Guide – A Guide to the Project Management Body of Knowledge*;
q) ABNT NBR ISO 12207:2009 – Engenharia de sistemas e *software* – Processos de ciclo de vida de *software*;
r) ABNT NBR ISO 20000-2:2013 – Tecnologia da Informação – Gerenciamento de serviços – Parte 2: Guia de aplicação do sistema de gestão de serviços;
s) ABNT NBR ISO 27001:2013 – Tecnologia da Informação – Sistemas de gestão da segurança da informação – Requisitos;
t) ABNT NBR ISO 27002:2013 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para controles de segurança da informação;
u) ABNT NBR ISO 27005:2011 – Tecnologia da Informação – Técnicas de Segurança – Gestão de riscos de segurança da informação;
v) ABNT NBR ISO 38500:2009 – Governança corporativa de tecnologia da informação;
w) Acórdão TCU nº 1.603/2008 – Plenário; e
x) Acórdão TCU nº 1.233/2012 – Plenário.

7.4.3. Procedimentos:

Descrição dos Procedimentos	Referência PT	Membro da Equipe responsável	Observações
Verificar se foram formalmente instituídos processos de gerenciamento: • do portfólio de serviços; • do catálogo de serviços; • da continuidade dos serviços de TI; • de mudanças; • de configuração e de ativos; • de liberação e implantação; • de incidentes; • de eventos; • de problemas; e • de acesso.	(Nº do Papel de Trabalho e referência.).		Resolução CNJ 211/2015 Acórdão TCU 1.233/2012 ITIL 3 (*Service Strategy*) ITIL 3 (*Service Design*) ITIL 3 (*Service Transition*) ITIL 3 (*Service Operation*)
Verificar se existe Plano de Continuidade de Serviços Essenciais de TI. **Caso positivo**, verificar se é aplicado.			Resolução CNJ nº 211/15; Acórdão TCU nº 1.233/2012 – Plenário; ITIL 3
Verificar se existe catálogo de serviços de TI com os níveis de serviços entre a área de TI e as áreas clientes formalmente definidos (Acordo de Nível de Serviço – ANS). **Caso positivo**, verificar se: • os ANS incluem indicador de grau de satisfação dos usuários; • os níveis de serviço definidos são monitorados; • em caso de não alcance dos níveis definidos, são implementadas ações			Resolução CNJ nº 211/15 Acórdão TCU nº 1.603/2008 – Plenário ISO 20000:08 ITIL 3 (*Service Design*)

corretivas; e • os resultados do monitoramento são periodicamente comunicados às áreas clientes.			
Verificar se existe processo de gestão de riscos de TI formalmente instituído. **Caso positivo**, verificar se os riscos de TI dos processos críticos de negócio são: • identificados; • avaliados; e • tratados com base em plano de tratamento de riscos.			Resolução CNJ nº 211/15 ISO 38500:09 ISO 31000:09 COBIT 5 (APO 12)
Verificar se existe Comitê Gestor de Segurança da Informação. **Caso positivo**, verificar se elabora e aplica política de segurança da informação em todos os níveis da instituição.			Resolução CNJ nº 211/15 Acórdão nº 1.233/2012 - Plenário ISO 27002:05 ISO 27005:08 NC 03/IN01/DSIC/GSIPR
Verificar se existem processos formalmente instituídos de gestão da segurança da informação que englobem: • classificação e tratamento de informações, com controles que garantam a proteção adequado ao grau de confidencialidade de cada classe de informação; • riscos; • vulnerabilidades técnicas de TI; • monitoramento do uso dos recursos de TI; e • incidentes de segurança da informação.			
Verificar se existe equipe de tratamento e resposta a incidentes de segurança em redes computacionais formalmente instituída.			NC 05/IN01/DSIC/GSIPR
Verificar se são realizadas periodicamente ações de conscientização, educação e treinamento em segurança da informação para os colaboradores.			NC 18/IN01/DSIC/GSIPR
Verificar se existe processo de *software* formalmente instituído. **Caso positivo**, verificar se o processo de software é: • acompanhado por meio de mensurações, com indicadores quantitativos e metas; • periodicamente revisado; e			Resolução CNJ nº 211/15 Acórdão TCU nº 1.233/2012 - Plenário ISO 12.207/09

• gerenciado por pessoal próprio e capacitado. Verificar se existe escritório de projetos de TI ou unidade equivalente formalmente instituído. **Caso positivo**, verificar se realiza as atividades previstas em seu ato constitutivo. Verificar se o portfólio de projetos de TI é adequadamente gerenciado. Verificar se existe processo de gerenciamento de projetos de TI formalmente instituído. **Caso positivo**, verificar se o processo de gerenciamento de projetos é: • acompanhado por meio de mensurações; e • periodicamente revisado.			Resolução CNJ nº 211/2015 PMBOK 5ª Edição Resolução CNJ nº 211/2015 PMBOK 5ª Edição Resolução CNJ nº 211/2015 Acórdão TCU nº 1.233/2012 - Plenário PMBOK 5ª Edição COBIT 5

7.4.4. Possíveis achados:

- Ausência de processos de gestão de serviços formalmente instituídos;
- Ausência de Plano de Continuidade de Serviços Essenciais de TI;
- Ausência de Acordos de Níveis de Serviço (ANS) ou de gerenciamento dos níveis de serviço;
- Ausência de processos de gestão de riscos de TI ou riscos de TI não gerenciados;
- Ausência de Comitê Gestor de Segurança da Informação;
- Ausência de política de segurança da informação;
- Ausência de política de controle de acesso aos recursos de TI ou deficiências na sua aplicação;
- Ausência de política de cópia de segurança (*backup*) ou deficiências na sua aplicação;
- Ausência de processos de gestão da segurança da informação formalmente instituídos;
- Ausência de equipe de resposta a incidentes de segurança em redes computacionais;
- Ausência de ações de conscientização dos colaboradores quanto a segurança da informação;
- Ausência de processo de *software* instituído ou de gerenciamento do processo de *software*;
- Ausência de gerenciamento do portfólio de projetos de TI; e
- Ausência de processo de gerenciamento de projetos de TI.

7.5. 5ª Questão de auditoria:

- O processo de planejamento de contratação de TI está sendo executado de acordo com o disposto na Resolução CNJ nº 182/2013?

7.5.1. Informações requeridas:

a) Amostra de processos de contratação de TI (avaliar os três últimos processos de maior valor em 2017 na contratação de solução de TI).

7.5.2. Fontes de Informação:

a) Guia de boas práticas em contratação de soluções de tecnologia da informação do TCU;
b) Resolução CNJ nº 182/2013; e
c) Resolução CNJ nº 211/2015.

7.5.3. Procedimentos:

Descrição dos Procedimentos	Referência PT	Membro da Equipe responsável	Observações
Verificar se existe Plano de Contratações de Soluções de Tecnologia da Informação e Comunicação. **Caso positivo**, verificar se: • inclui as contratações necessárias ao alcance dos objetivos estabelecidos nos planejamentos estratégicos institucional e de TI; • é revisado periodicamente para incluir novas contratações pretendidas; e • contém prazos de entrega dos Estudos Preliminares e dos Projetos Básicos ou Termos de Referência.	(Nº do Papel de Trabalho e referência).		Resolução CNJ nº 182/2013 Guia boas práticas TCU
Verificar se os processos de contratações de TI contêm Documento de Oficialização da Demanda (DOD) com: • descrição da necessidade ou da solução pretendida e o alinhamento aos planos estratégicos; e • explicitação da motivação e demonstrativo de resultados a serem alcançados com a solução.			Resolução CNJ nº 182/2013 Guia boas práticas TCU
Verificar se os processos de contratações de TI contêm Análise de Viabilidade da Contratação com as informações mínimas requeridas pela Resolução CNJ nº 182/2013, inclusive: • a definição dos requisitos;			Resolução CNJ nº 182/2013 Guia boas práticas TCU

• a identificação de diferentes soluções para a demanda solicitada; • a análise e comparação de custos entre as diferentes soluções; • o orçamento estimado que expresse a composição de todos os custos unitários resultantes dos itens a serem contratados; e • a justificativa para a escolha da solução, com identificação dos benefícios a serem alcançados em termos de eficácia, eficiência, economicidade e padronização. Verificar se os processos de contratações de TI contêm Plano de Sustentação do Contrato, quando aplicável, com as informações mínimas requeridas pela Resolução CNJ nº 182/2013, inclusive: • o plano de continuidade do fornecimento da Solução de TI, no caso de eventual interrupção contratual; e • as atividades de transição contratual e de encerramento de contrato. Verificar se os processos de contratações de TI especificam a estratégia a ser adotada para a contratação, conforme as informações mínimas requeridas pela Resolução CNJ nº 182/2013. Verificar se os processos de contratações de TI contêm Análise de Riscos com as informações mínimas requeridas pela Resolução CNJ nº 182/2013, inclusive: • identificação dos principais riscos que possam comprometer o sucesso da contratação ou que emergirão caso a contratação não seja realizada; • mensuração das probabilidades de ocorrência e os impactos; • definição de ações que reduzam ou eliminem os riscos, se for o caso; • definição das ações de contingência a serem tomadas caso os riscos se concretizem; e • definição dos responsáveis pelas ações de prevenção e contingência.			Resolução CNJ nº 182/2013 Guia boas práticas TCU Resolução CNJ nº 182/2013 Guia boas práticas TCU Resolução CNJ nº 182/2013 Guia boas práticas TCU

Verificar se a Análise de Riscos trata dos riscos e ameaças que possam vir a comprometer o sucesso de todo o ciclo de vida da contratação, inclusive aqueles que possam influenciar a própria contratação. Verificar se as ações de prevenção e contingência previstas na Análise de Riscos são efetivamente colocadas em prática. Verificar se os processos de contratação de TI possuem Projeto Básico ou Termo de Referência com as informações mínimas requeridas pela Resolução CNJ nº 182/2013.			Resolução CNJ nº 182/2013 Resolução CNJ nº 182/2013 Guia boas práticas TCU

7.5.4. Possíveis achados:

- Ausência de Plano de Contratações de TI ou plano incompleto;
- Documento de Oficialização da Demanda (DOD) incompleto;
- Documento de Análise de Viabilidade de Contratação incompleto;
- Ausência de Plano de Sustentação de Contrato, quando aplicável, ou plano incompleto;
- Documento de Estratégia de Contratação incompleto;
- Análise incompleta dos riscos em contratações de TI; e
- Riscos de contratações não gerenciados.

7.6. 6ª Questão de auditoria:

- Os resultados apresentados pela TI são dimensionados?

7.6.1. Informações requeridas:

a) Principais processos de negócio mapeados;
b) Portfólio de sistemas informatizados; e
c) Designação formal de gestores dos respectivos sistemas informatizados.

7.6.2. Fontes de Informação:

a) Referencial Básico de Governança do TCU;
b) ABNT NBR ISO 38500:2009 – Governança corporativa de tecnologia da informação;
c) COBIT 5 – *Control Objectives for Information and related Technology*;
d) Acórdão TCU nº 2.585/2012 – Plenário;
e) Acórdão TCU nº 1.233/2012 – Plenário;
f) Referencial Básico de Governança do TCU; e
g) Lei nº 12.527/2011 – Lei de Acesso a Informações (LAI).

7.6.3. Procedimentos:

Descrição dos Procedimentos	Referência PT	Membro da Equipe responsável	Observações
Verificar se os resultados dos objetivos de TI que constam no PETIC e no PDTIC são medidos. Caso positivo, verificar se os objetivos estão sendo atingidos.	(Nº do Papel de Trabalho e referência).		Acórdão TCU nº 2.308/2010 ISO 38500:09 COBIT 5 (EDM2 e 4, MEA1)
Verificar se são divulgadas informações sobre os resultados dos objetivos de TI e o acompanhamento das ações e projetos de TI que constam no PETIC e no PDTIC.			Acórdão TCU nº 2.585/2012; Acórdão TCU nº 1.233/2012; COBIT 5.
Verificar se o grau de alcance dos objetivos e benefícios esperados que justificaram a abertura de projetos de TI é medido. Caso positivo, verificar se os resultados são satisfatórios.			COBIT 5 (EDM02, BAI01) PMBOK 5ª edição
Verificar se os sistemas de TI finalizados e entregues para operação têm orçamento estimado no início do projeto. Caso positivo, verificar: • se há diferenças significativas entre a estimativa inicial e o valor real obtido ao final; e • quais são os motivos para eventuais diferenças significativas.			PMBOK 5ª edição

Verificar se os serviços de TI que sustentam a organização possuem indicadores de nível de serviço. Caso positivo, verificar se os resultados apresentados estão dentro dos limites definidos.			Acórdão TCU nº 1.603/2008 – Plenário ISO 20000:08
Verificar se os processos críticos de negócio são suportados por sistemas informatizados.			Acórdão TCU nº 2.585/2012 – Plenário COBIT 5
Verificar se são designados formalmente os responsáveis da área de negócio para a gestão dos respectivos sistemas informatizados.			Acórdão TCU nº 2.585/2012 – Plenário COBIT 5 (APO 01.06)
Verificar se existe avaliação periódica da efetiva utilização dos sistemas informatizados que suportam o negócio.			COBIT 5 (APO 09.01) ISO 38500:09
Verificar se as iniciativas programadas pela área de Tecnologia da Informação e Comunicação constantes do Plano de Trabalho previsto no art. 29 da Resolução CNJ nº 211/2015 foram implementadas em relação aos Grupos 1 e 2, conforme especificado no § 1º do art. 29 da citada resolução.			Acórdão TCU nº 2.585/2012 – Plenário Resolução CNJ nº 211/2015

7.6.4. Possíveis achados:

- Ausência de medição dos resultados dos objetivos estratégicos;
- Ausência de medição do grau de alcance dos objetivos e benefícios esperados nos projetos de TI;
- Ausência de estimativa orçamentária completa nos projetos de TI;
- Estimativa orçamentária dos projetos de TI inadequada;
- Ausência de indicadores de níveis de serviço para os principais serviços de TI;
- Existência de processos críticos de negócio sem suporte por sistemas informatizados;
- Ausência de designação formal dos responsáveis da área de negócio para os sistemas informatizados;
- Ausência de avaliação periódica da efetiva utilização dos sistemas informatizados que suportam o negócio;
- Ausência de elaboração do Plano de Trabalho previsto no art. 29 da Resolução CNJ nº 211/2015; e
- Implantação incompleta das ações previstas para os Grupos 1 e 2 do Plano de Trabalho a que se refere o art. 29 da Resolução CNJ nº 211/2015.

7.7. 7ª Questão de auditoria:

- A Unidade de Auditoria Interna (UAI) realiza exames de auditoria na área de TI para aferir o estágio da governança e da gestão de TI?

7.7.1. Informações requeridas:

a) Amostra de relatórios de auditoria (avaliar os relatórios de auditoria de 2017).

7.7.2. Fontes de Informação:

b) Acórdãos TCU nº 1.233/2012, nº 2.622/2015 e nº 1.273/2015, todos do Plenário;
c) Referencial Básico de Governança do TCU;
d) Resolução CNJ nº 171/2013; e
e) Parecer nº 2/2013 – SCI/Presi/CNJ, aprovado na Sessão Plenária do CNJ de 18/12/2013.

7.7.3. Procedimentos:

Descrição dos Procedimentos	Referência PT	Membro da Equipe responsável	Observações
Verificar se a Unidade de Auditoria Interna (UAI) realizou, em 2015, 2016 e 2017, exames de auditoria para aferir o estágio da governança e da gestão de TI. **Caso positivo:** • Indicar em qual relatório constou avaliação detalhada sobre a implementação das Diretrizes formuladas pelo CNJ em relação a: a.1) Resolução CNJ nº 211/2015; e a.2) Resolução CNJ nº 182/2013. • Indicar em qual relatório constou avaliação detalhada sobre a eficácia dos controles da Governança e da Gestão de TIC, inclusive nos aspectos relativos a riscos afetos à segurança da informação, dos serviços judiciais e aos demais ativos de TIC críticos do órgão; • Indicar em qual relatório constou avaliação detalhada sobre a eficácia	(Nº do Papel de Trabalho e referência.).		Acórdãos TCU nº 1.233/2012, nº 2.622/2015 e nº 1.273/2015, todos do Plenário Resolução CNJ nº 211/2015

dos controles das contratações de soluções de TIC, inclusive nos aspectos relativos aos riscos críticos para o órgão; e • Indicar em qual relatório constou avaliação detalhada sobre a eficácia dos controles das contratações nos aspectos relativos à gestão de contratos.			

7.7.4. Possíveis achados:

- Ausência de realização de exames de auditoria na área de governança e gestão de TIC nos exercícios de 2015, 2016 e 2017;
- Ausência de avaliação da implementação das diretrizes estabelecidas na Resolução CNJ nº 182/2013;
- Ausência de avaliação da implementação das diretrizes estabelecidas na Resolução CNJ nº 211/2015;
- Ausência de avaliação e acompanhamento do Plano de Trabalho previsto no art. 29 da Resolução CNJ nº 211/2015;
- Ausência de avaliação detalhada sobre a eficácia dos controles da Governança e da Gestão de TIC;
- Ausência de avaliação dos aspectos relativos a riscos afetos à segurança da informação, dos serviços judiciais e aos demais ativos de TIC críticos do órgão;
- Ausência de avaliação detalhada sobre a eficácia dos controles das contratações de soluções de TIC;
- Ausência de avaliação dos riscos críticos para o órgão em relação às contratações; e
- Ausência de avaliação detalhada sobre a eficácia dos controles das contratações nos aspectos relativos à gestão de contratos.

Local e DATA

Líder da Equipe de Auditoria:

Supervisor: