



TRIBUNAL REGIONAL FEDERAL DA 1ª REGIÃO

RELATÓRIO FINAL DE AUDITORIA

SECRETARIA DE AUDITORIA INTERNA - SECAU

DIVISÃO DE AUDITORIA DE GESTÃO ADMINISTRATIVA - DIAUD

AÇÃO COORDENADA DE AUDITORIA EM GOVERNANÇA DE TI

1. INTRODUÇÃO

O presente relatório trata de Auditoria em Governança de Tecnologia da Informação - TI coordenada pela Secretaria de Auditoria Interna do Conselho Nacional de Justiça - CNJ, cujo escopo corresponde ao exame dos conteúdos dos planos de tecnologia da informação, dos controles de governança, de gestão, de resultados e de riscos de TI, em cumprimento ao Plano Anual de Atividades de Auditoria Interna – PAINT (5147712) para o exercício de 2018, aprovado pelo Presidente deste Tribunal, consoante PAe 0022434-78.2017.4.01.8000.

1.1 OBJETIVO

Avaliar os conteúdos estabelecidos pelo TRF 1ª Região 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 91/2009, 182/2013, 198/2014 e 211/2015 e o perfil de governança de TI traçado pelo TCU.

1.2 PERÍODO DE EXECUÇÃO

A presente auditoria foi realizada no período de **02/05/2018 a 30/06/2018**.

1.3 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?

1.4 COMPOSIÇÃO DA AMOSTRA AVALIADA

Os seguintes processos foram selecionados para compor a amostra, com observância dos critérios de relevância, materialidade e risco inerente.

Quadro 1 - Processos Analisados

Processo	Descrição
0008232-33.2016.4.01.8000	Definição da Política de Gestão de Pessoas
0014248-66.2017.4.01.8000	Elaboração do Itinerário Formativo - TI
0003791-77.2014.4.01.8000	Projeto Transparência de TI – TTI

Processo	Descrição
0026415-52.2016.4.01.8000	Projeto de Nivelamento da Infraestrutura de TI da Justiça Federal da 1ª Região
0013789-30.2018.4.01.8000	Evidências da Ação Coordenada de Auditoria de Governança e Gestão de TI CNJ 2018
0004687-23.2014.4.01.8000	Acompanhamento do Comitê Gestor de TI da JF1 – CGTI-TRF1
0000682-55.2014.4.01.8000	Projeto de Gestão de Demandas de Tecnologia da Informação
0015481-69.2015.4.01.8000	Adequação do quadro de TI à Resolução CNJ 211/2015
0008193-65.2018.4.01.8000	Regulamentação de normas
0005410-03.2018.4.01.8000	Transformação de cargos
0009686-77.2018.4.01.8000	Acompanhamento das reuniões do COGETI-TRF1
0016810-19.2015.4.01.8000	Licitação - Contratação de Serviços para Manutenção e Desenvolvimento de Sistemas
0021089-48.2015.4.01.8000	Licitação - Contratação de Serviço de Atendimento ao Usuário TI - TRF1
0026820-25.2015.4.01.8000	Licitação - Contratação de Serviço de apoio à Sustentação da Infraestrutura de TI
0026955-37.2015.4.01.8000	Cronograma da Política de Nivelamento de Infraestrutura de Tecnologia da Informação da Justiça Federal
0002542-91.2014.4.01.8000	Projeto - Implantação do PJe
0013459-67.2017.4.01.8000	Plano Anual de Contratações

6195926. Para esclarecimentos ou justificativas pertinentes às análises realizadas, foi expedida a Solicitação de Auditoria

1.5 EQUIPE DE AUDITORIA

Tiago Diniz Brasileiro Lira - auditor

Marcos de Oliveira Dias - coordenador

1.6 TÉCNICAS DE AUDITORIA

A metodologia utilizada neste trabalho está de acordo com as diretrizes de auditoria aplicáveis à Administração Pública previstas na [Resolução 171/2013](#), do Conselho Nacional de Justiça e [Resolução Presi TRF1 57/2017](#), deste Tribunal, e contemplou as seguintes técnicas:

- Análise documental;
- Pesquisa em sistemas informatizados;
- Exame dos registros;
- Confronto de informações e documentos;
- Comparação com a legislação, a jurisprudência do TCU e a doutrina;
- Amostragem.

1.7 PROCEDIMENTOS REALIZADOS

Os procedimentos realizados durante a auditoria são listados a seguir:

- Análise do Programa 5548784, elaborado pelo Conselho Nacional de Justiça – CNJ;
- Planejamento das ações para responder o questionário 5548852, elaborado pelo CNJ;
- Resposta às questões do questionário;
- Execução dos procedimentos presentes no programa 5548784;
- Análise de Processos Administrativos e sistemas informatizados;
- Envio de Solicitação de Auditoria 6195926 para a área de TI e Despacho 6259317 para a Secretaria de Gestão de Pessoas – SecGp, visando a análise e retificação, mediante apresentação de evidências, do preenchimento do questionário por esta Diaud;
- Análise da manifestação emitida pela unidade auditada;
- Submissão das respostas do questionário 6400084 ao CNJ, juntamente com as evidências presentes no PAe SEI 0013789-30.2018.4.01.8000; e
- Elaboração deste relatório com as recomendações pertinentes, sem prejuízo daquelas que serão emitidas pelo CNJ.

1.8 LEGISLAÇÃO APLICADA

1. ABNT NBR ISO 12207:2009 – Engenharia de sistemas e software – Processos de ciclo de vida de software;
2. ABNT NBR ISO 20000-2:2013 – Tecnologia da Informação – Gerenciamento de serviços – Parte 2: Guia de aplicação do sistema de gestão de serviços;
3. ABNT NBR ISO 22313:2015 – Sistemas de gestão de continuidade de negócios;
4. ABNT NBR ISO 27001:2013 – Tecnologia da Informação – Sistemas de gestão da segurança da informação – Requisitos;
5. ABNT NBR ISO 27002:2013 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para controles de segurança da informação;
6. ABNT NBR ISO 27005:2011 – Tecnologia da Informação – Técnicas de Segurança – Gestão de riscos de segurança da informação;
7. ABNT NBR ISO 31000:2009 – Gestão de riscos – princípios e diretrizes;
8. ABNT NBR ISO 38500:2009 – Governança corporativa de tecnologia da informação;
9. ABNT NBR ISO 38500:2009 – Governança corporativa de tecnologia da informação;
10. Acórdão TCU nº 1.233/2012 – Plenário;
11. Acórdão TCU nº 1.603/2008 – Plenário;
12. Acórdão TCU nº 2.308/2010 – Plenário;
13. Acórdão TCU nº 2.585/2012 – Plenário;
14. COBIT 5 – Control Objectives for Information and related Technology;
15. Decreto nº 5.707/2006;
16. Decreto-Lei nº 200, de 25 de fevereiro de 1967;
17. Guia de boas práticas em contratação de soluções de tecnologia da informação do TCU;
18. ITIL Version 3 – Service Design;
19. ITIL Version 3 – Service Operation;
20. ITIL Version 3 – Service Strategy;
21. ITIL Version 3 – Service Transition;
22. Lei nº 12.527/2011 – Lei de Acesso a Informações (LAI);
23. Medida Provisória nº 2.200-2, de 24 de agosto de 2001 (ICP-Brasil);
24. 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;
25. Norma Complementar nº 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;
26. Norma Complementar nº 18/IN01/DSIC/GSIPR – Diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal;
27. 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;
28. Norma Complementar nº 04/IN01/DSIC/GSIPR – Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC;
29. Norma Complementar nº 05/IN01/DSIC/GSIPR – Criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR;
30. Norma Complementar nº 07/IN01/DSIC/GSIPR – Diretrizes para Implementação de controles de Acesso Relativos à Segurança da Informação e Comunicações;
31. 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;
32. PMBoK Guide – A Guide to the Project Management Body of Knowledge;
33. Referencial Básico de Governança do TCU;
34. Resolução CNJ nº 182/2013;
35. Resolução CNJ nº 198/2014;
36. Resolução CNJ nº 211/2015.

2. ACHADOS

Os achados foram identificados durante as atividades desenvolvidas para responder às indagações presentes no questionário 5548852, elaborado pelo CNJ. O questionário foi estruturado em perguntas cujas opções de resposta consistem numa escala de 0 a 3, onde 3 é o melhor resultado possível. Exemplo de questionamento:

26 – Há avaliação específica de desempenho para o pessoal de TI?

- () 0 – Não existe avaliação específica do desempenho do pessoal de TI;
 () 1 – Não existe avaliação específica, mas há estudos para sua formulação;
 () 2 – Existe avaliação específica de desempenho, porém não periódica;
 () 3 – Existe avaliação específica de desempenho do pessoal de TI.

Evidência (para os itens 1, 2 e 3). **Para comprovação da Evidência nº 3 é necessário demonstrar a(s) avaliação(avaliações) de desempenho realizada(s) nos últimos 36 meses.**

Figura 1: Exemplo de questão formulada pelo CNJ

A exceção à regra foi a vigésima oitava questão, na qual deveriam ser selecionados os itens atendidos pelo Tribunal, como se vê na figura abaixo:

28 – Quais processos de gerenciamento foram formalmente instituídos?

() 0 – do portfólio de serviços;
 () 1 – do catálogo de serviços;
 () 2 – da continuidade dos serviços de TI;
 () 3 – de mudanças;
 () 4 – de configuração e de ativos;
 () 5 – de liberação e implantação;
 () 6 – de incidentes;
 () 7 – de eventos;
 () 8 – de problemas;
 () 9 – de acesso.

Evidência (para os itens 0 a 9).

Figura 2: Questão 28

Sobre as respostas, é apresentado abaixo quadro com a consolidação do resultado do TRF1, conforme documento 6400084:

Quadro 2: Consolidação das respostas

Resposta	Nº de Questões	% do Total
0*	9	17,31%
1	9	17,31%
2	17	32,69%
3	17	32,69%

* A questão 28 foi respondida como 0 pois nenhum dos 9 itens foi formalmente instituído.

Durante as atividades desenvolvidas para responder o questionário, foram identificadas situações que ensejaram recomendações, as quais são apresentadas neste relatório. Contudo, **há casos em que já existem recomendações em monitoramento**, provenientes de outras auditorias, realizadas anteriormente, e que, por esse motivo, foi dispensada uma nova recomendação. Os itens do questionário que abordam o tema, o problema/achado e a recomendação **atualmente em monitoramento** são apresentados no quadro abaixo:

Quadro 3: Situações que são objeto de monitoramento

Questão	Achado	Recomendação
3 – O Comitê de Gestão de TI foi formalmente instituído e mantém reuniões periódicas?	“2.2 FRAGILIDADES NA GESTÃO DA SEGURANÇA DA INFORMAÇÃO” do Relatório 01/2018 (5830757)	2.2.9.1 Providenciar a devida formalização do Modelo de Governança de TI, constante do PAe SEI 0004687-23.2014.4.01.8000, para regulamentar alterações na composição e no cronograma de reuniões da Comissão Local de Segurança da Informação - CLSI;
5 – Existem diretrizes formais da alta administração que direcionem a gestão do portfólio de projetos de TI e do portfólio de serviços de TI?	“2.1 BAIXO DESEMPENHO NA EXECUÇÃO DA ESTRATÉGIA DE TI” do Relatório 01/2018 (5830757)	2.1.9.2 Contemplar, nas reuniões do Comitê Gestor de Tecnologia da Informação - CGTI, a avaliação da situação das metas e indicadores estratégicos de modo a propiciar a definição de ações para o seu alcance;

Questão	Achado	Recomendação
13 – Existem diretrizes formais para a avaliação da governança e da gestão de TI?	“2.1 BAIXO DESEMPENHO NA EXECUÇÃO DA ESTRATÉGIA DE TI” do Relatório 01/2018 (5830757)	2.1.9.2 Contemplar, nas reuniões do Comitê Gestor de Tecnologia da Informação (CGTI), a avaliação da situação das metas e indicadores estratégicos de modo a propiciar a definição de ações para o seu alcance.
14 – Existe política formal para o controle de acesso à informação e aos recursos e serviços de TI?	“2.2 FRAGILIDADES NA GESTÃO DA SEGURANÇA DA INFORMAÇÃO” do Relatório 01/2018 (5830757)	2.2.9.2 Elaborar documentos acessórios previstos na Resolução CJF nº 006/2008.
15 – Existe política formal para a realização de cópias de segurança (backup)?	“2.2 FRAGILIDADES NA GESTÃO DA SEGURANÇA DA INFORMAÇÃO” do Relatório 01/2018 (5830757)	2.2.9.2 Elaborar documentos acessórios previstos na Resolução CJF nº 006/2008.
20 – Existe PDTIC vigente, acompanhado e revisado periodicamente?	“2.1 BAIXO DESEMPENHO NA EXECUÇÃO DA ESTRATÉGIA DE TI” do Relatório 01/2018 (5830757)	2.1.9.2 Contemplar, nas reuniões do Comitê Gestor de Tecnologia da Informação (CGTI), a avaliação da situação das metas e indicadores estratégicos de modo a propiciar a definição de ações para o seu alcance.
29 – Existe Plano de Continuidade de Serviços Essenciais de TI vigente e com revisão periódica?	“2.2 FRAGILIDADES NA GESTÃO DA SEGURANÇA DA INFORMAÇÃO” do Relatório 01/2018 (5830757)	2.2.9.2 Elaborar documentos acessórios previstos na Resolução CJF nº 006/2008.
32 – O Comitê Gestor de Segurança da Informação foi formalmente instituído?	“2.2 FRAGILIDADES NA GESTÃO DA SEGURANÇA DA INFORMAÇÃO” do Relatório 01/2018 (5830757)	2.2.9.1 Providenciar a devida formalização do Modelo de Governança de TI, constante do PAe SEI 0004687-23.2014.4.01.8000, para regulamentar alterações na composição e no cronograma de reuniões da Comissão Local de Segurança da Informação - CLSI.
33 – Existem processos de gestão da segurança da informação formalmente instituídos?	“2.2 FRAGILIDADES NA GESTÃO DA SEGURANÇA DA INFORMAÇÃO” do Relatório 01/2018 (5830757)	2.2.9.3 Estabelecer e manter, por meio da Comissão Local de Resposta a Incidentes de Segurança da Informação, ações preventivas e educativas na área de Segurança da Informação.
34 – A Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais - ETIR foi formalmente instituída e definida a sua autonomia?	“2.2 FRAGILIDADES NA GESTÃO DA SEGURANÇA DA INFORMAÇÃO” do Relatório 01/2018 (5830757)	2.2.9.4 Implantar metodologia na gestão de incidentes de segurança da informação por parte da Comissão Local de Resposta a Incidentes de Segurança da Informação.
35 – Ações de sensibilização, conscientização e capacitação em segurança da informação para os agentes públicos da instituição são realizadas periodicamente?	“2.2 FRAGILIDADES NA GESTÃO DA SEGURANÇA DA INFORMAÇÃO” do Relatório 01/2018 (5830757)	2.2.9.3 Estabelecer e manter, por meio da Comissão Local de Resposta à Incidentes de Segurança da Informação, ações preventivas e educativas na área de Segurança da Informação.
36 – Existe processo de software formalmente instituído?	“2.4 DEMORA NA EXECUÇÃO DOS SERVIÇOS DE TI” do Relatório 01/2018 (5830757)	2.4.9.1 Apresentar e realizar cronograma de adoção da metodologia de desenvolvimento de sistemas para todos os sistemas do TRF1, justificando a não adoção para o caso de sistemas que serão descontinuados.
44 - Os objetivos estratégicos e táticos de TI são monitorados com medições periódicas e revisões sempre que necessárias?	“2.1 BAIXO DESEMPENHO NA EXECUÇÃO DA ESTRATÉGIA DE TI” do Relatório 01/2018 (5830757)	2.1.9.2 Contemplar, nas reuniões do Comitê Gestor de Tecnologia da Informação (CGTI), a avaliação da situação das metas e indicadores estratégicos de modo a propiciar a definição de ações para o seu alcance.

Excluindo-se o que já é objeto de recomendação e monitoramento, e sem prejuízo das situações **que serão apontadas pelo CNJ** após a análise das respostas ao questionário enviadas por essa Diaud/Secau no documento 6400084, são apresentados a seguir os achados considerados relevantes para relato.

2.1 FRAGILIDADES NA GESTÃO DOS SERVIÇOS DE TI

2.1.1 Situação encontrada

Foi constatado que os processos que dão suporte aos serviços de TI não estão alinhados às melhores práticas da área e que inexistente uma sistemática instituída para avaliação e melhoria na prestação dos serviços realizados pela área de TI da Justiça Federal da 1ª Região.

2.1.2 Critérios

- *Information Technology Infrastructure Library (ITIL)*
- Acórdão TCU n. 1603/2008 – 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;

(...)

9.1.5. 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;"

- Acórdão TCU n. 1233/2012 – Plenário

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:

(...)

9.13.8. 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);”

2.1.3 Evidências

A biblioteca *ITIL* é um conjunto de melhores práticas na gestão de serviços de tecnologia da informação. Ela considera que os serviços devem ter seus resultados quantificados de forma clara e mensurável para propiciar o monitoramento e o aperfeiçoamento, culminando na melhoria do relacionamento entre os clientes e a área de TI.

No contexto da quantificação de resultados, embora o sistema de solicitação de serviços de TI (e-Sosti) exija a avaliação após o encerramento da demanda, conforme instituído pela Portaria Presi/Secin n. 445/2011, tal avaliação é atualmente destinada à apuração de nível de serviço das empresas contratadas e não ao desempenho da TI como um todo. Dessa maneira, fica prejudicada a existência de um referencial de resultados para medição, avaliação e melhoria dos serviços prestados pela Secretaria de Tecnologia da Informação – Secin.

Também foi verificado que o projeto “Gestão de Demandas de TI” (PAe SEI 0000682-55.2014.4.01.8000) tem como objetivos, dentre outros, proporcionar a definição de níveis de serviço para a TI e aumentar a satisfação dos clientes da TI, conforme presente no Termo de Abertura de Projeto – TAP 0004152. O projeto iniciado em 16/07/2014, sofreu atrasos, conforme Relatório 6930435, e seu término, que estava previsto para dezembro de 2018, foi adiado.

2.1.4 Causas

- Ausência de diretrizes para orientar as avaliações de desempenho dos serviços de TI.
- Ausência de indicadores de nível de serviço para os serviços de TI.
- Ausência de metodologia formal de gestão de riscos na execução dos serviços de TI.
- Atraso na conclusão do projeto "Gestão de Demandas de TI".

2.1.5 Efeitos

- Falta de Transparência sobre os resultados da área de TI.
- Impossibilidade de aferir o desempenho dos serviços prestados pela área de Tecnologia da Informação.
- Comprometimento da eficiência na execução dos serviços.

2.1.6 Responsáveis

- Secretaria de Tecnologia da Informação – Secin;
- Comitê Gestor de Tecnologia da Informação – CGTI.

2.1.7 Manifestação da área auditada

A área auditada informou que a conclusão do projeto Gestão de Demandas de TI permitirá a medição do desempenho da TI e que o projeto será desenvolvido com gestão de riscos. Também retificou entendimento dessa equipe de auditoria sobre abrangência do projeto, que abará toda a Justiça Federal.

2.1.8 Análise da Equipe de Auditoria

A ausência de sistemática de medição, bem como da implantação de outros processos previstos na literatura de referência, como a *Itil*, comprometem a avaliação, a melhoria na prestação dos serviços de TI e a forma como ela é vista por seus clientes. Há um projeto em andamento cuja conclusão, à luz de seus objetivos propostos, proporcionará o saneamento das fragilidades identificadas. Somando-se a isso, a gestão de riscos apresenta-se como ferramenta útil à melhoria da eficiência na prestação dos serviços de TI. Nesse sentido, são feitas as recomendações presentes no item a seguir.

2.1.9 Recomendações

2.1.9.1 Formalizar metodologia para divulgação de resultados dos serviços de TI.

2.1.9.2 Estabelecer sistemática, contemplando indicadores de nível de serviço, que propicie a avaliação e a validação de desempenho, pelos usuários, dos serviços prestados pela Secretaria de Tecnologia da Informação.

2.1.9.3 Implantar o gerenciamento de riscos na gestão dos serviços de TI.

2.2 FRAGILIDADES NA GESTÃO DE PESSOAS DA ÁREA DE TECNOLOGIA DA INFORMAÇÃO

2.2.1 Situação encontrada

Ausência de política formal para a gestão de pessoas da área de TI.

2.2.2 Critérios

- Acórdão TCU n. 1603/2008 – 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. atentar 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;

”

- Acórdão TCU n. 1233/2012 – Plenário

“

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);

”

- Resolução CNJ n. 2011/2015

“Art. 13. Cada órgão deverá compor o seu quadro permanente com servidores que exercerão atividades voltadas exclusivamente para a área de Tecnologia da Informação e Comunicação.

§ 1º O quadro permanente de servidores de que trata o caput deverá ser compatível com a demanda, adotando-se como critérios para fixar o quantitativo necessário o número de usuários internos e externos de recursos de TIC, bem como o referencial mínimo estabelecido no Anexo desta Resolução.

§ 2º O referencial mínimo contido no Anexo poderá ser aumentado com base em estudos que cada órgão realize, considerando ainda aspectos como o portfólio de projetos e serviços, o orçamento destinado à área de TIC e as especificidades de cada segmento de Justiça.

Art. 14. Cada órgão deverá definir e aplicar política de gestão de pessoas que promova a fixação de recursos humanos na área da Tecnologia da Informação e Comunicação, recomendando-se a criação de cargos, especialidades e gratificação específicos para essa área.”

2.2.3 Evidências

Constata-se o esforço do Tribunal no sentido de aumentar o quadro de servidores de TI, como constatado nos PAes SEI 0015481-69.2015.4.01.8000 e 0005410-03.2018.4.01.8000. Apesar disso, e considerando-se, ainda, a recente nomeação de novos servidores para a área, o quadro de servidores de TI continua aquém do quantitativo de referência estabelecido pela Resolução CNJ n. 211/2015.

Em paralelo, o TRF 1ª Região trabalha na elaboração de uma resolução para instituir uma política de gestão de pessoas no âmbito da Justiça Federal da 1ª Região, consoante registrado no PAe SEI 0008232-33.2016.4.01.8000. Tal resolução amolda-se ao estabelecido na Resolução CNJ 211/2015, mas ainda não foi aprovada, conforme extrato de julgamento 7029864.

2.2.4 Causas

- Demora na formalização da política para a gestão de pessoal de TI;
- Limitações para contratação de pessoal da área de TI.

2.2.5 Efeitos

- Dificuldade para obtenção de servidores especializados em determinadas áreas da Tecnologia da Informação;
- Maior custo com capacitação; e
- Dificuldade na realização de tarefas da área devido à sobrecarga de atividades dos servidores.

2.2.6 Responsáveis

- Secretaria de Gestão de Pessoas – SecGP

2.2.7 Manifestação da área auditada

A área auditada apresentou as iniciativas para identificação de necessidades de treinamento, bem como as capacitações realizadas e previstas para o ano de 2018 (Informação 6854788). Informou, ainda, que a minuta do normativo que visa à instituição de uma política de gestão de pessoas no âmbito da Justiça Federal da 1ª Região, constante do PAe 0008232-33.2016.4.01.8000, estaria em fase de validação e ajustes.

2.2.8 Análise da equipe de auditoria

Em 19/12/2018, foi aprovada a [Resolução PRESI 6903944](#), que institui a política de gestão de pessoas no âmbito da Justiça Federal da 1ª Região e aborda questões relativas ao pessoal de TI, considerando, entre outros aspectos, o disposto na [Resolução CNJ 211/2015](#), quanto à política de gestão de pessoas na área de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD). O cumprimento da política instituída pela [Resolução PRESI 6903944](#) será fundamental para promover melhorias na gestão do pessoal de TI na Justiça Federal da 1ª Região.

Com base nisso, considera-se que a recomendação preliminar *"Informar a Diaud/Secau sobre a finalização da elaboração da resolução e implantar, efetivamente, a política de gestão de pessoas no âmbito da Justiça Federal da 1ª Região em consonância com o estabelecido na Resolução CNJ n. 211/2015"* foi implementada.

2.3 FRAGILIDADES NA GESTÃO DE PROJETOS DE TI NÃO ESTRATÉGICOS

2.3.1 Situação encontrada

Projetos de TI não estratégicos são conduzidos de maneira diferente dos projetos estratégicos e em desacordo com as melhores práticas de TI.

2.3.2 Critérios

- PMBoK Guide – A Guide to the Project Management Body of Knowledge; e
- Manual de Gestão de Projetos da Justiça Federal

2.3.3 Evidências

O Manual de Gestão de Projetos da Justiça Federal foi desenvolvido com o intuito de favorecer o desenvolvimento, a cultura e a maturidade das organizações e aumentar as chances de sucesso e alcance dos objetivos de quem o utiliza. Dentre os benefícios da gestão de projetos, cita-se:

- **Transparência:** possibilita a disponibilização de registro padronizado dos fatos. Reuniões, planejamento de custos, cronogramas, problemas pontuados e propostas de ações corretivas são exemplos de registros documentados. Para tanto, os Escritórios de Projetos da Justiça Federal disponibilizam ferramentas e modelos de documentos;
- **Aprendizado:** o registro e a documentação de todas as fases dos projetos permitem que, com o passar do tempo, seja formada uma base histórica de dados referentes aos projetos da Justiça Federal, que poderá ser consultada para auxiliar no desenvolvimento de projetos futuros. Além disso, a utilização de um Manual de Gestão de Projetos propicia um aumento gradual do nível de maturidade em projetos da organização;
- **Tempestividade:** a gestão de projetos busca garantir que as ações, bem como as medidas corretivas e preventivas, sejam executadas no tempo oportuno e por isso com uma maior chance de eficácia;
- **Controle:** o Manual oferece mecanismos de acompanhamento periódico dos projetos, uma vez que, para cada etapa do processo de gestão, é necessário reportar dados sobre os produtos e/ou serviços entregues, medir indicadores, analisar riscos, registrar dificuldades encontradas na execução, avaliar a comunicação e as lições aprendidas. O referido acompanhamento favorece a identificação de situações críticas que necessitam de ações corretivas;

- **Qualidade dos produtos/serviços:** com um planejamento bem elaborado e ações de acompanhamento sugerido pelo Manual, a qualidade do produto/serviço tende a ser incrementada. Os produtos/serviços resultantes de um projeto visam à satisfação do cliente, sendo esta comprovada pela medição de indicadores de resultados; e
- **Otimização de recursos:** geralmente os projetos envolvem diferentes unidades e órgãos da Justiça Federal, num trabalho multidisciplinar. A aplicação da gestão de projetos facilita a coordenação e otimização de pessoas, equipamentos e outros materiais.

Durante a realização dos trabalhos foi constatado que somente os projetos estratégicos de TI seguem O Manual de Gestão de Projetos da Justiça Federal e que os demais projetos são conduzidos em sistemática distinta.

2.3.4 Causas

- Escritório de Projetos de TI com atuação parcial, promovendo a adoção da metodologia formalizada no Manual de Gestão de Projetos da Justiça Federal somente nos projetos estratégicos.

2.3.5 Efeitos

- Falta de transparência na execução dos projetos; e
- Dificuldade na aferição dos resultados dos projetos.

2.3.6 Responsáveis

- Secretaria de Tecnologia da Informação – Secin

2.3.7 Manifestação da área auditada

A Secin informou que considera como projetos somente as ações de TI mais complexas e de maior duração, com necessidade de acompanhamento mais formal. Alegou, também, inexistir óbice ao surgimento de novos projetos na área de TI. Nesse sentido, a equipe responsável pelo acompanhamento do Plano Diretor de Tecnologia da Informação (PDTI) poderá estabelecer projetos a partir do acompanhamento das iniciativas presentes no plano.

2.3.8 Análise da equipe de auditoria

Para o *Project Management Institute* (PMI), um projeto é um empreendimento temporário desenvolvido para criar um produto, serviço ou resultado único e o gerenciamento de projetos envolve, dentre outros:

- Atendimento de várias necessidades, questões e expectativas dos *stakeholders* (partes interessadas) no planejamento e na execução do projeto;
- Estabelecimento, manutenção e execução de comunicação entre os *stakeholders* ativos no projeto.

Considerando o volume de atividades desempenhadas pela área de TI, bem como ser a maioria das atividades classificadas como processos e não projetos, esta equipe de auditoria entende ser necessária uma revisão das atividades para o estabelecimento de projetos – que não serão necessariamente estratégicos – cujo gerenciamento melhor estruturado trará melhorias, ganhos de transparência e eficiência em sua execução.

2.3.9 Recomendações

2.3.9.1 Revisar as ações de TI realizadas na Secin, de modo a identificar e gerir – por meio de um portfólio – aquelas que se caracterizam como projetos.

2.3.9.2 Estabelecer um repositório centralizado para acompanhamento de objetivos, cronograma, riscos, atividades e resultados dos projetos realizados pela área de TI.

3. CONCLUSÃO

Foram avaliados nesta auditoria, sob coordenação do Conselho Nacional de Justiça, os conteúdos dos planos de tecnologia da informação, dos controles de governança, de gestão, de riscos e de resultados de TI.

As recomendações inseridas no corpo deste Relatório estão voltadas ao aperfeiçoamento de procedimentos e visam assegurar o atendimento às normas legais e regulamentares aplicáveis.

Conclui-se que as medidas informadas pela área auditada demonstram que a Administração está adotando práticas de aprimoramento dos controles internos necessários para minimizar os efeitos potenciais dos achados deste relatório. Recomenda-se que essas medidas sejam contínuas e aplicadas em procedimentos futuros.

Diante do exposto, propõe-se o encaminhamento deste Relatório Final de Auditoria à Presidência do Tribunal e à Diretoria-Geral da Secretaria, para conhecimento, bem como à Secretaria de Tecnologia da Informação – Secin, para conhecimento e preenchimento do Plano de Providências 7280463, nos termos do Capítulo IV, item 3.1, do Estatuto de Auditoria Interna da Justiça Federal da 1ª Região, aprovado pela Resolução Presi - TRF 1ª Região n. 57/2017 (5426955), com o retorno a esta Secretaria de Auditoria Interna até **29/03/2019**.

À consideração superior.

TIAGO DINIZ BRASILEIRO LIRA
Supervisor da Seção de Auditoria Temática

MARCOS DE OLIVEIRA DIAS
Diretor da Divisão de Auditoria de Gestão Administrativa

De acordo.

À Presidência do Tribunal e à Diretoria-Geral da Secretaria, para conhecimento deste Relatório Final de Auditoria, bem como à Secretaria de Tecnologia da Informação – Secin, para conhecimento e preenchimento do Plano de Providências 7280463, com o retorno a esta Secretaria de Auditoria Interna até 29/03/2019.

MARÍLIA ANDRÉ DA SILVA MENESES GRAÇA
Diretora da Secretaria de Auditoria Interna



Documento assinado eletronicamente por **Marília André da Silva Meneses Graça, Diretor(a) de Secretaria**, em 15/03/2019, às 18:38 (horário de Brasília), conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **Marcos de Oliveira Dias, Diretor(a) de Divisão**, em 20/03/2019, às 15:44 (horário de Brasília), conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **Tiago Diniz Brasileiro Lira, Supervisor(a) de Seção**, em 20/03/2019, às 15:50 (horário de Brasília), conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site <http://portal.trf1.jus.br/portaltrf1/servicos/verifica-processo.htm> informando o código verificador **7281844** e o código CRC **434783B0**.