TRIBUNAL REGIONAL ELEITORAL DE SERGIPE
CENAF, Lote 7, Variante 2 - Bairro Capucho - CEP 49081-000 - Aracaju - SE - http://www.tre-se.jus.br

RELATÓRIO DE AUDITORIA 6/2018 - SEAUG

RELATÓRIO		**Preliminar**	X	**Conclusivo**		**Monitoramento**

INTERESSADO(S)	Secretaria de Tecnologia da Informação

RELATÓRIO DE AUDITORIA COORDENADA DO CNJ

PREÂMBULO

Processo: 0003564-14.2018.6.25.8000

Ato originário: Parecer 7/2014 do Conselho Nacional de Justiça

Objetivo: Realizar exames de auditoria de tecnologia da informação, com escopo na avaliação de conteúdos estabelecidos para governança, riscos e controles de TI e TIC e na verificação dos sistemas desenvolvidos, objetivando análise de controles e conformidade com padrões e modelos internacionalmente aceitos como o COBIT, CMMI, ISO 17799, ISO 27001 e com o Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Judiciário Brasileiro - MoReq-Jus.

Ato de designação: Plano Anual de Auditoria

Período de realização: Planejamento (20/02/18 - 01/03/18) e Execução (02/03/18 - 21/06/18)

Unidade(s) Auditada(s): Secretaria de Tecnologia da Informação e Secretaria de Gestão de Pessoas

RESUMO

O Conselho Nacional de Justiça - CNJ determinou a realização de Ação Coordenada de Auditoria a fim de avaliar os conteúdos estabelecidos para a governança e gestão de TI.

As ações coordenadas têm por objetivo a gestão concomitante, tempestiva e padronizada sobre questões de relevância e criticidade para o Poder Judiciário, bem como o atendimento aos princípios de eficiência, eficácia e efetividade.

A Auditoria Coordenada de Governança e Gestão de TI foi executada a partir do Programa e dos Pontos de Auditoria disponibilizados pelo CNJ e constatou a necessidade de aperfeiçoamento: nas realizações periódicas das reuniões do Comitê de Governança de TI, do Comitê de Gestão de TI e do Comitê de Segurança da Informação, na instituição formal dos processos de: formulação do Plano Estratégico de Tecnologia da Informação e Comunicação (PETIC) e do Plano Diretor de Tecnologia da Informação e Comunicação (PDTI), de gestão de portfólios de serviços, de eventos e de vulnerabilidades técnicas de TI.

Quanto à ausência de definição das competências necessárias para o pessoal de TI, ausência de acompanhamento do desempenho do pessoal de TI e ausência de previsão dos quantitativos ideais da força de trabalho de TI, a SGP e a STI já possuem Plano de Ação em andamento.

A Unidade de Auditoria Interna também já adotou providências no sentido de aperfeiçoar sua atuação, mediante a conclusão desta Auditoria; a execução dos programas de auditoria relacionados à

segurança da informação (0548087) e a governança e gestão aplicada às contratações de TIC (0576511), além de levantamento de informações para avaliar outros temas relativos à TI.

SUMÁRIO

I. INTRODUÇÃO

O Parecer 7/2014 - SCI/Presi/CNJ definiu a realização, dentre outras, da Ação Coordenada de Auditoria na área de tecnologia da informação, com escopo na avaliação de conteúdos estabelecidos para governança, gestão, riscos e controles de TI e TIC, considerando projetos, processos, riscos e resultados de TI em comparação com padrões internacionalmente aceitos como COBIT, PMBOK, ITIL, CMMI, ISO 17799 e ISO 27001, bem como com as Resoluções CNJ nº 182/2013, nº 211/2015 e nº 91/2009.

O Programa e os Pontos de Auditoria, levando também em consideração o perfil de governança de tecnologia da informação e comunicação traçado pelo Tribunal de Contas da União - TCU, foram disponibilizados no sítio eletrônico do CNJ, para as Unidades de Controle Interno do Poder Judiciário.

Compuseram a equipe de auditoria do Tribunal Regional Eleitoral de Sergipe - TRE/SE os servidores: Ana Maria Rabelo de Carvalho Dantas, Cassia Maria Carvalho Polito Alves e Jurene Barreto Santos.

Encaminhou-se para a Unidade Auditada o Programa de Auditoria e o "Questionário para Levantamento de Informações" subdividido em: Políticas e Diretrizes; Planos de TI; Pessoal; Gestão dos Processos; Planejamento das Contratações e Resultados.

Após respostas da Unidade Auditada, a Equipe de Auditoria realizou as análises pertinentes e reuniões para alguns esclarecimentos. As conclusões desta Unidade de Controle relativas ao "Questionário para Levantamento de Informações" (0583948) foram encaminhadas ao CNJ, via Compartilhamento de Dados em Nuvem.

As principais inconformidades foram destacadas neste Relatório Conclusivo de Auditoria.

Todos os exames realizados se pautaram em procedimentos e técnicas de auditoria aplicáveis à Administração Pública e nenhuma restrição nos foi imposta quanto ao método ou à extensão dos trabalhos realizados.

II. VISÃO GERAL DO OBJETO AUDITADO

O objeto auditado pode ser observado em duas dimensões, às quais contemplam fatores que têm a capacidade de, individualmente ou coletivamente, influenciar o funcionamento da governança da TI organizacional (ISACA, 2012a, p. 27).

São estas as dimensões:

a) Governança e Gestão: abrange aspectos relacionados às Políticas e Planejamento, Estruturas Organizacionais e Macroprocessos, e Pessoas

A política de governança de TI contempla princípios, diretrizes, papéis e responsabilidades necessárias para desempenhar as funções de avaliar, dirigir e monitorar a gestão e o uso de TIC.

As estruturas organizacionais desempenham papel fundamental na tomada de decisão na medida em que norteiam a atuação da gestão e viabilizam a governança de TI.

Os macroprocessos constituem-se num conjunto organizado de práticas e atividades para alcançar certos objetivos e produzir um conjunto de saídas de forma a suportar o alcance das metas de TI de uma organização (ISACA, 2012a, p.27).

Os recursos humanos em TI devem ser em número suficiente para executar as funções relacionadas à TI, com as habilidades e competências necessárias.

b) Infraestrutura de TIC: abrange aspectos relacionados a Sistemas de Informação, Integração de Sistemas e Disponibilização de Informações, e Nivelamento Tecnológico

Os sistemas de informação devem adequar-se a padrões de desenvolvimento, suporte operacional, segurança da informação, gestão documental, interoperabilidade e outros recomendados pelo Comitê Nacional de Gestão de Tecnologia da Informação e Comunicação do Poder Judiciário.

A integração de sistemas entre primeiro e segundo graus e a disponibilização de informações na rede mundial de computadores favorecem a celeridade na prestação jurisdicional e a transparência dos atos.

O nivelamento tecnológico da infraestrutura de TIC consiste numa série de requisitos mínimos tecnológicos traçados pelo CNJ para o Poder Judiciário.

III. OBJETIVO DA AUDITORIA

Esta auditoria teve por 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.

IV. ESCOPO

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

V. CRITÉRIOS

Referencial Básico de Governança do TCU
Guia de boas práticas em contratação de soluções de tecnologia da informação do TCU
ABNT NBR ISO 31000:2009 – Gestão de riscos – princípios e diretrizes
ABNT NBR ISO 22313:2015 – Sistemas de gestão de continuidade de negócios
ABNT NBR ISO 38500:2009 – Governança corporativa de tecnologia da informação
ABNT NBR ISO 12207:2009 – Engenharia de sistemas e software – Processos de ciclo de vida de software
ABNT NBR ISO 20000-2:2013 – Tecnologia da Informação – Gerenciamento de serviços – Parte 2: Guia de aplicação do sistema de gestão de serviços
ABNT NBR ISO 27001:2013 – Tecnologia da Informação – Sistemas de gestão da segurança da informação – Requisitos
ABNT NBR ISO 27002:2013 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para controles de segurança da informação
ABNT NBR ISO 27005:2011 – Tecnologia da Informação – Técnicas de Segurança – Gestão de riscos de segurança da informação
COBIT 5 – Control Objectives for Information and related Technology
ITIL 3.0 – Information Technology Infrastructure Library
PMBoK – A Guide to the Project Management Body of Knowledge
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
Resolução CNJ nº 211/2015
Resolução CNJ nº 182/2013
Resolução CNJ nº 198/2014
Decreto-Lei nº 200, de 25 de fevereiro de 1967
Lei nº 12.527/2011 – Lei de Acesso a Informações (LAI)
Decreto nº 5.707/2006
Medida Provisória nº 2.200-2, de 24 de agosto de 2001 (ICP-Brasil)
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
Norma Complementar nº 04/IN01/DSIC/GSIPR – Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC
Norma Complementar nº 05/IN01/DSIC/GSIPR – Criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR
Norma Complementar nº 07/IN01/DSIC/GSIPR – Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações
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
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
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
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
Orientações para preenchimento e envio do Questionário

VI. 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?

VII. AVALIAÇÃO DAS QUESTÕES DE AUDITORIA

A apreciação das Questões de Auditoria estão consubstanciadas no Papel de Trabalho 1.01 - Avaliação da COCIN.

Ao CNJ foram enviadas apenas as respostas a cada uma das indagações contidas no Questionário para Levantamento de Informações (0583948), consoante o padrão de preenchimento e envio de respostas exigido:

a) A Unidade de Auditoria Interna do tribunal (UAI), após realização dos exames de auditoria, marcará uma das opções de resposta. É importante observar as opções de respostas que exigem apresentação de Evidência;

b) São admitidas como Evidência cópias de arquivos de texto, planilhas, normativos e/ou qualquer documento que permitam comprovar a afirmação contida na resposta;

c) Documentos que servirem de Evidência devem ser identificados e objetivamente relacionados à Questão respectiva;

d) As respostas somente serão aceitas se acompanhadas da respectiva Evidência, quando exigida, ou seja, o encaminhamento do questionário sem a Evidência inviabiliza a aceitação da resposta oferecida pela UAI.

VIII. INCONFORMIDADES DE AUDITORIA

Após execução dos procedimentos de análise, previstos no Programa de Auditoria disponibilizado pelo CNJ, foram detectadas algumas inconformidades, às quais elencamos a seguir, subdivididas por tema: Políticas e Diretrizes, Planos de TI, Pessoal, Gestão dos Processos, Planejamento das Contratações, Resultados e Atuação da Auditoria Interna.

Políticas e Diretrizes

Ausência de reuniões periódicas do Comitê de Governança de TI e do Comitê de Gestão de TI.

Planos

Ausência de processos formalmente definidos para formulação do Plano Estratégico de Tecnologia da Informação e Comunicação (PETIC) e do Plano Diretor de Tecnologia da Informação e Comunicação (PDTI).

Pessoal

Ausência de definição das competências necessárias para o pessoal de TI.

Ausência de acompanhamento do desempenho do pessoal de TI.

Ausência de previsão dos quantitativos ideais da força de trabalho de TI.

Gestão dos Processos

Ausência de processos de gestão de portfólios de serviços e de eventos formalmente instituídos.

Ausência de aplicação do Plano de Continuidade de Serviços.

Ausência de Acordos de Nível de Serviço (ANS).

Ausência de reuniões periódicas do Comitê de Segurança da Informação.

Ausência de processo de vulnerabilidades técnicas de TI.

Atuação da Auditoria Interna

Ausência de avaliação detalhada sobre a eficácia dos controles da Governança e da Gestão de TIC nos anos de 2015, 2016 e 2017;

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 nos anos de 2015, 2016 e 2017;

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;

Ausência de avaliação e acompanhamento do Plano de Trabalho previsto no art. 29 da Resolução CNJ nº 211/2015.

IX. CONCLUSÃO

Em face da análise realizada nos conteúdos dos planos de tecnologia da informação, nos controles de governança, de gestão, de riscos e de resultados de TI, concluiu-se pela necessidade de aperfeiçoamentos mediante:

a) Realizações periódicas das reuniões do Comitê de Governança de TI, do Comitê de Gestão de TI e do Comitê de Segurança da Informação, com registro e divulgação das deliberações;

b) Instituição formal dos processos: de formulação do Plano Estratégico de Tecnologia da Informação e Comunicação (PETIC) e do Plano Diretor de Tecnologia da Informação e Comunicação (PDTI); de gestão de portfólios de serviços; de eventos; de vulnerabilidades técnicas de TI, sempre considerando a ordem de prioridade dos processos considerados críticos pela Secretaria de Tecnologia da Informação;

Para as melhorias quanto à definição das competências necessárias para o pessoal de TI, acompanhamento do desempenho do pessoal de TI e previsão dos quantitativos ideais da força de trabalho de TI, a SGP e a STI já possuem Plano de Ação em andamento.

A Unidade de Auditoria Interna também já adotou providências para sanar as inconformidades, elencadas no tópico anterior, mediante a conclusão desta Auditoria, execução dos programas de auditoria relacionados à segurança da informação (0548087) e governança e gestão aplicada às contratações de TIC (0576511), além de levantamento de informações para avaliar outros temas relativos à TI.

Posteriormente, o CNJ apresentará a consolidação das respostas dos Tribunais e Conselhos desta Auditoria Coordenada, ficando a seu critério, diante das evidências apresentadas por cada Tribunal emitir as devidas recomendações.

X. PROPOSTA DE ENCAMINHAMENTO

Diante do exposto, submete-se o presente Relatório Conclusivo de Auditoria à consideração da Presidência, propondo o encaminhamento para ciência à Secretaria de Tecnologia da Informação e à Secretaria de Gestão de Pessoas.

Documento assinado eletronicamente por **CASSIA MARIA CARVALHO POLITO ALVES**, **Técnico Judiciário**, em 14/09/2018, às 09:23, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **JURENE BARRETO SANTOS**, **Assistente**, em 14/09/2018, às 09:24, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **IVANILDO ALVES DE MEDEIROS**, **Chefe de Seção**, em 14/09/2018, às 09:54, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **ANA MARIA RABELO DE CARVALHO DANTAS**, **Coordenador**, em 14/09/2018, às 09:58, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://apps.tre-se.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0533355** e o código CRC **0053E09E**.