RELATÓRIO DE AUDITORIA

AÇÃO COORDENADA DE AUDITORIA NA ÁREA DE TECNOLOGIA DA INFORMAÇÃO - 2018

Trata-se de ação coordenada de auditoria promovida pelo Conselho Nacional de Justiça (CNJ), no período de 02 de maio a 29 de junho de 2018, cujo objeto foi o Sistema de Governança e Gestão da Tecnologia da Informação e Comunicação (TIC).

A possibilidade de realização de ações coordenadas de auditoria está prevista na Resolução CNJ nº 171/2013, que dispõe sobre normas técnicas de auditoria, inspeção administrativa e fiscalização nas unidades jurisdicionadas ao Conselho Nacional de Justiça (CNJ).

O art. 13 da citada resolução estabelece que a realização de Ações Coordenadas de Auditoria tem 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, economicidade e efetividade.

I - Escopo da auditoria:

Exame dos conteúdos dos planos de tecnologia da informação, dos controles de governança, de gestão, de riscos e de resultados de TI no âmbito das unidades jurisdicionadas ao Conselho Nacional de Justiça.

II – Objetivo da auditoria:

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 198/2014 e nº 211/2015, além das recomendações e perfil de governança de TI traçado pelo Tribunal de Contas da União (TCU).

A auditoria buscou identificar eventuais fragilidades no Sistema de Governança e Gestão de TIC que venham expor a Instituição aos diversos riscos relacionados com a utilização de TIC. A identificação dessas fragilidades poderá orientar a ação da Presidência e das instâncias internas de Governança de TIC para, com respaldo nas normatizações e boas práticas internacionalmente reconhecidas, **avaliar, direcionar e monitorar** a TIC do Tribunal. Na mesma direção, buscou-se que as funções de gestão do Tribunal, em especial a Diretoria Geral (DG) e a Secretaria de Tecnologia da Informação (STI), baseados na avaliação e direcionamento dados pela Presidência, **planejem, construam, executem e controlem** soluções e serviços de TIC com as funcionalidades corretas, riscos mitigados e custos otimizados.

III - Área Auditada:

Área de Tecnologia da Informação

IV – Procedimentos de auditoria:

Foram colhidas as informações, conforme procedimentos elencados no Programa de Auditoria (evento 0371155) e seguindo o questionário disponibilizado pelo Conselho Nacional de Justiça (evento 0371163), por meio de entrevistas à equipe da Secretaria de Tecnologia da Informação, bem como consultas ao Sistema Eletrônico de Informações - SEI, análise documental e verificação dos procedimentos para obtenção dos elementos suficientes a formação de evidências.

Após a realização dos exames de auditoria foi selecionada uma opção de resposta para cada uma das 52 (cinquenta e duas) questões, envolvendo temas relacionados à políticas e diretrizes, planos de TI, pessoal, gestão dos processos, planejamento das contratações de TI, resultados e atuação da unidade de auditoria interna.

Nos casos em que a situação encontrada não encontrou opção de resposta próxima à realidade do Tribunal, foram acrescidos esclarecimentos complementares na forma de observação.

Boa parte das respostas exigiram a apresentação de evidência, sendo admitidas cópias de arquivos de texto, planilhas, normativos e/ou qualquer documento que permitisse comprovar a afirmação contida na resposta. Foi estabelecido que a equipe de auditoria avaliaria cada questão e caso estas não fossem suportadas por evidências, as respostas seriam fornecidas conforme convicção da equipe de auditoria.

Junto ao questionário preenchido, as evidências obtidas, num total de 108 (cento e oito) arquivos, foram encaminhadas ao Conselho Nacional de Justiça, conforme orientação e senha de acesso encaminhadas pelo Secretário de Controle Interno do Conselho Nacional de Justiça, mediante o compartilhamento de dados em nuvem (*link:* https://www.cnj.jus.br/owncloud/index.php/s/naJtqcWiHYYziIH).

Como limitações encontradas ao trabalho devemos mencionar o exíguo prazo fixado pelo CNJ para a conclusão dos trabalhos, em face da extensão do escopo da auditoria que abarcou todo o Sistema de Governança e Gestão de TIC, bem como a falta de conhecimento técnico, inexperiência e disponibilidade de recursos humanos, tendo em vista ainda, as demais atividades realizadas pela equipe de auditoria, durante o período delimitado.

Vale destacar que parte das respostas negativas do Questionário no tocante à "Atuação da Unidade de Auditoria", em relação à ausência de ações de auditoria específicas na área de TI, decorrem do fato desta Unidade não possuir força de trabalho com formação e/ou experiência em Tecnologia da Informação para o desenvolvimento dessas atividades, atualmente imprescindíveis nas áreas de auditoria.

V – Constatações:

As constatações relatadas no presente relatório foram sistematizadas, seguindo a ordem das questões do "Questionário para levantamento de informações para auditoria", para

ciência e providências cabíveis, lembrando que posteriormente deverá ser remetido relatório consolidado pelo Conselho Nacional de Justiça.

VI – Achados:

Dentre os principais Achados de Auditoria destacamos:

POLÍTICAS E DIRETRIZES

Quanto às políticas e diretrizes definidas para a Governança e Gestão de Tecnologia da Informação:

A.1) Por meio da Resolução nº 15.732 de 13/09/2016 foi instituída a Governança Corporativa de Tecnologia da Informação e Comunicação no âmbito do TRE/AL, com a composição e competência do Comitê de Governança de TIC, bem como do Comitê de Gestão de TIC; o Comitê de Governança de TIC reuniu-se apenas uma vez em 2018, conforme ata do dia 19/03/2018, **não ficando demonstrado um envolvimento e uma atuação efetiva, considerando as prioridades que envolvem a área de governança de TI;**

A.2) Quanto às diretrizes formais que direcionam o planejamento de TI no âmbito do TRE/AL, o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) para o período de 2017 e 2018 foi instituído mediante a Resolução nº 15.818 em 22/06/2017; contudo, **apesar de existir o direcionamento do planejamento de TI, não foi possível encontrar evidências no sentido de suas diretrizes serem plenamente aplicadas por este Regional;**

A.3) Ausência de diretrizes formais da alta administração que direcionem a gestão do portfólio de projetos de TI e do portfólio de serviços de TI;

A.4) Ausência de política formal de gestão de riscos de TI;

A.5) Ausência de política formal para a gestão de pessoal de TI;

A.6) Ausência de política formal para a avaliação e incentivo ao desempenho de gestores e técnicos de TI;

A.7) Ausência de política formal para a escolha dos líderes de TI;

A.8) Ausência de diretrizes formais para a comunicação dos resultados da gestão e do uso de TI para as partes interessadas (públicos interno e externo); Ausência de comunicação com partes interessadas sobre os resultados de TI; o TRE/AL divulga na página eletrônica do Tribunal os resultados de gestão e do uso de TI por meio do relatório de gestão institucional, encaminha os relatórios de governança do TCU e CNJ, além de medir os indicadores extraídos do próprio Plano Estratégico de Tecnologia da Informação (PETIC), contudo, ainda não há a definição da forma de comunicação com o público interno e externo dos resultados de TI;

A.9) Ausência de confirmação da existência de política formal para a realização de cópias de segurança *(backup)*;

PESSOAL

Quanto às necessidades relacionadas ao desenvolvimento de pessoas e à força de trabalho da área de TI:

A.10) Ausência de definição das competências necessárias para o pessoal de TI;

A.11) Ausência de avaliação específica de desempenho do pessoal de TI;

A.12) Ausência de previsão dos quantitativos ideais da força de trabalho de TI ou previsão sem embasamento técnico; não existe um estudo detalhado sobre como atender o volume de necessidades de pessoal na execução das atividades de TI;

PROCESSOS

Quanto ao gerenciamento dos processos de gestão de TI:

A.13) Ausência de processos de gerenciamento formalmente instituídos:

– do portfólio de serviços;
– de mudanças;
– de configuração e de ativos;
– de liberação e implantação;
– de eventos;
– de problemas.

Nesse quesito, foi acrescida a observação: *Foram instituídos, desde 2011, processos internos de acompanhamento de incidentes de TI, cujos registros são mantidos em pastas internas da STI do TRE/AL. Além disso, para tratar dos processos de gerenciamento, foram constituídas a Comissão de Segurança da Informação (Portaria TRE-AL nº 452/2017 - http://www.justicaeleitoral.jus.br/arquivos/tre-al-comissao-de-seguranca-da-informacao) e o Gestor de Segurança da Informação (Portaria TRE-AL nº 453/2017 - http://www.justicaeleitoral.jus.br/arquivos/tre-al-gestor-de-seguranca-da-informacao).*

Quanto ao catálogo de serviços de TI atualizado, com níveis de serviços entre a área de TI e as áreas clientes, foi acrescida a observação: *Catálogo de Serviços de TI (Existe catálogo atualizado, SEM a definição dos níveis de serviços) http://www.justicaeleitoral.jus.br/arquivos/tre-al-catalogo-de-servicos-de-tecnologia-dainformacao-e-comunicacao-versao-2-0*

A.14) Ausência de processo formalmente instituído de gestão de riscos de TI;

A.15) Os processos de gestão da segurança da informação foram formalmente instituídos, mas são parcialmente utilizados;

A.16) Ausência de ações periódicas para sensibilização, conscientização e capacitação em segurança da informação para os agentes públicos do Tribunal; em geral, somente ocorrem ações de formação inicial no período de ambientação dos agentes no órgão;

A.17) Ausência de escritório de projetos de TI (PMO) ou unidade que realize atividades equivalentes formalmente instituída;

A.18) Ausência de processo formalmente instituído para o gerenciamento do portfólio de projetos de TI;

A.19) Ausência de processo formalmente instituído para o gerenciamento de projetos de TI;

RESULTADOS

Quanto ao dimensionamento dos resultados apresentados pela TI:

A.20) Ausência de medição do grau de alcance dos objetivos e benefícios esperados para abertura dos projetos de TI;

A.21) Ausência de avaliação e acompanhamento do Plano de Trabalho previsto no art. 29 da Resolução CNJ nº 211/2015;

ATUAÇÃO DA UNIDADE DE AUDITORIA INTERNA

Quanto à realização de exames de auditoria na área de TI:

A.22) Ausência de avaliação detalhada sobre a eficácia dos controles da Governança e da Gestão de TIC;

A.23) Ausência de avaliação dos aspectos relativos a riscos afetos à segurança da informação, serviços judiciais e aos demais ativos de TIC críticos do órgão;

A.24) Ausência de avaliação detalhada sobre a eficácia dos controles das contratações de soluções de TIC; e

A.25) Ausência de avaliação dos riscos críticos para o órgão em relação às contratações.

Quanto às auditorias, foi acrescida a observação: Foi realizada avaliação sobre as diretrizes formuladas pelo CNJ em relação à Resolução CNJ nº 182/2013, nos anos de 2013,

2014, 2016 e por conta do presente trabalho, em 2017. Quanto à Resolução CNJ nº 211/2015, foi mencionada, de forma breve, em auditoria que teve foco na análise das contratações de 2016, mas que também citou o resultado do Levantamento de Governança, Gestão e Infraestrutura de TIC do Poder Judiciário - iGovTIC - JUD 2015/2016, no procedimento SEI nº 0009610-92.2017.6.02.8000.

VII – Conclusões e Recomendações:

Em face dos exames realizados, conclui-se que as deficiências nos sistemas de governança e gestão de TI podem reduzir a capacidade do TRE/AL de gerar resultados e benefícios para a sociedade, assim, foram propostas diversas recomendações, com base nos questionamentos do CNJ, decisões do TCU e princípios do COBIT, no intuito de auxiliar o aperfeiçoamento dos referidos sistemas, de modo a contribuir para a consecução da estratégia organizacional.

A título de esclarecimento, o COBIT 5 conhecido como *Control Objectives for Information and related Technology* (Objetivos de Controle da Informação e Tecnologia relacionada), fornece um modelo abrangente que auxilia as organizações a atingirem seus objetivos de governança e gestão de TI, ajudando-as a criarem valor por meio da TI, mantendo o equilíbrio entre a realização de benefícios e a otimização dos níveis de risco e de utilização dos recursos.

O COBIT descreve cinco princípios e sete habilitadores que apoiam as organizações no desenvolvimento, implementação, melhoria e monitoramento contínuos das boas práticas de governança e gestão de TI. O modelo de referência de processos do COBIT 5 divide os processos de governança e gestão de TI da organização em dois domínios de processos principais:

- Governança – Contém 05 processos de governança e dentro de cada processo são definidas práticas para Avaliar, dirigir e monitorar (*Evaluate, Direct and Monitor* - EDM);
- Gestão – Contém 32 processos de gestão que compõem 04 domínios, conforme as áreas responsáveis por planejar, construir, executar e monitorar (*Plan, Build, Run and Monitor* - PBRM), e oferece cobertura de TI de ponta a ponta. São eles:
  Alinhar, Planejar e Organizar (*Align, Plan and Organise* – APO);
  Construir, Adquirir e Implementar (*Build, Acquire and Implement* – BAI);
  Entregar, Servir e Suportar (*Deliver, Service and Support* – DSS);
  Monitorar, Avaliar e Medir (*Monitor, Evaluate and Assess* – MEA).

Considerando as fragilidades detectadas, recomendamos:

POLÍTICAS E DIRETRIZES

R.1) Atuação efetiva do Comitê de Governança de TIC com reuniões periódicas para impulsionar o Tribunal na busca dos objetivos organizacionais, tendo em vista o art. 7º da Resolução nº 211/2015 e o teor da Resolução TRE-AL nº 15.732/2016:

> ***Resolução CNJ nº 211/2015:***
>
> *Art. 7º Cada órgão deverá constituir um Comitê de Governança de Tecnologia da Informação e Comunicação que ficará responsável, entre outros, pelo estabelecimento de estratégias, indicadores e metas institucionais, aprovação de planos de ações, bem como pela orientação das iniciativas e dos investimentos tecnológicos no âmbito institucional.*
> *Parágrafo único. Recomenda-se que a composição do Comitê de Governança seja multidisciplinar, e com a participação das principais áreas estratégicas do órgão, incluindo Magistrados dos diversos graus de jurisdição e a área de Tecnologia da Informação e Comunicação.*

R.2) Garantir efetividade as ações traçadas no planejamento estratégico de TI, conforme as diretrizes estabelecidas pela alta administração no Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC - Resolução TRE/AL nº 15.818/2017). Há necessidade do regular acompanhamento e aperfeiçoamento das atividades aprovadas pela alta administração.

> ***Acórdão TCU nº 1.603/2008 – 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:*
>
> *9.1.1. 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;*

R.3) Sejam estabelecidas pela alta administração com o apoio do Comitê de Governança de Tecnologia da Informação e Comunicação (CGTIC) as diretrizes formais direcionando a gestão do portfólio de projetos de TI e do portfólio de serviços de TI alinhadas com a estratégia da organização, para garantir a obtenção de benefícios e contribuir de forma efetiva com o alinhamento estratégico do Órgão.

Segundo a biblioteca da ITIL o portfólio é "um conjunto completo de serviços que serão entregues pelo provedor. São agrupados por tamanho, disciplina e valor estratégico". Em outras palavras, o Portfólio engloba todos os serviços entregues pelo departamento de TI; Contém todos os serviços, inclusive os propostos e obsoletos. O processo de gerenciamento do Portfólio de Serviços é estratégico.

A ITIL V3 define o catálogo se serviços como "parte do Portfólio disponível para um cliente." São os serviços ativos na visão de um cliente em específico. Na gestão do catálogo, o objetivo é que todas as informações dos serviços ativos estejam claramente disponíveis e

especificadas para seus clientes. O gestor deste processo tem um papel tático na prestação dos serviços de TI.

COBIT 5:

APO 05 (Gerência de Portfólio): *Executa o conjunto de orientações estratégicas para os investimentos alinhados com a visão de arquitetura corporativa e as características desejadas do investimento e considera as restrições de recursos e de orçamento. Avalia, prioriza programas e serviços, gerencia demanda dentro das restrições de recursos e de orçamento, com base no seu alinhamento com os objetivos estratégicos e risco. Move programas selecionados para o portfólio de serviços para execução. Monitora o desempenho de todo o portfólio de serviços e programas, propondo os ajustes necessários em resposta ao programa e desempenho do serviço ou mudança de prioridades da organização.*

BAI01 (Gerenciar Programas e Projetos): *Gerenciar todos os programas e projetos do portfólio de investimentos em alinhamento com a estratégia da organização e de forma coordenada. Inicia, planeja, controla e executa programas e projetos, e finaliza com a revisão pós-implementação.*

R.4) Seja constituído o Comitê de Gestão de Riscos de TI para a implantação da gestão de riscos de TI, estabelecendo claramente os objetivos e o comprometimento da organização em relação à gestão de riscos, conforme ISO 31000/2009, COBIT 5 e Acórdão TCU nº 1.603/2008 – Plenário.

COBIT 5:

APO 12 (Gerenciar os Riscos): *Identificar continuamente, avaliar e reduzir os riscos relacionados a TI dentro dos níveis de tolerância estabelecidos pela diretoria executiva da organização.*

Acórdão TCU nº 1.603/2008 – 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.

R.5) Sejam estabelecidas diretrizes que orientem a política de gestão de pessoal de TI abordando aspectos relacionados à retenção de pessoal, adoção de práticas gerenciais de avaliação e incentivo ao desempenho de gestores e técnicos, diretrizes para a escolha de

líderes na área de TI e para a identificação dos perfis adequados para atuar na área de TI, buscando o gerenciamento do quadro de pessoal de TI;

COBIT 5:

APO07 (Gerenciar Recursos Humanos): *Fornece uma abordagem estruturada para garantir a estruturação ideal, colocação, direitos de decisão e as habilidades dos recursos humanos. Isso inclui a comunicação de papéis e responsabilidades definidas, planos de aprendizagem e de crescimento, e as expectativas de desempenho, com o apoio de pessoas competentes e motivadas.*

Acórdão TCU nº 1.603/2008 – 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. 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;

Acórdão TCU nº 1.233/2012 – 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);
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);
(...)
9.13.10. 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);
(...)
9.13.14. 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;
(...)
9.13.14.11. monitoração do desempenho da TI organizacional;

Resolução CNJ nº 211/2015:

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. 15. Deverá ser elaborado e implantado Plano Anual de Capacitação para desenvolver as competências gerenciais e técnicas necessárias à operacionalização da governança, da gestão e do uso da Tecnologia da Informação e Comunicação.
Parágrafo único. O Plano Anual de Capacitação deverá promover e suportar, de forma contínua, o alinhamento das competências gerenciais e técnicas dos servidores lotados na área de TIC às melhores práticas de governança, de gestão e de atualização tecnológica.

Acórdão TCU nº 2.308/2010 – Plenário:

9.1. recomendar ao Conselho Nacional de Justiça – CNJ, (...) 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;

R.6) A alta administração defina diretrizes para comunicação com as partes interessadas sobre os resultados da gestão e do uso de TI, considerando o público interno e externo, contemplando divulgação, conteúdo, frequência e formato das comunicações, conforme recomendado no Acórdão TCU nº 2.585/2012 – Plenário:

Acórdão TCU nº 2.585/2012 – Plenário:

"ACORDAM os Ministros do Tribunal de Contas da União, reunidos em sessão do Plenário, ante as razões expostas pelo Relator, em:
9.1. recomendar ao Conselho Nacional de Justiça, (...), 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;"

R.7) Seja confirmada ou implementada a existência de política formal de cópias de segurança (*backup*);

Embora tenhamos respondido à questão 15 do Questionário como "Existe política formal plenamente aplicada", observamos que este Regional formalizou a Comissão de Segurança da Informação (Portaria TRE-AL nº 452/2017), bem como nomeou e estabeleceu as responsabilidades do Gestor de Segurança da Informação (Portaria TRE-AL nº 453/2017), assim como, a STI informou: *"A política de backup é formalizada no âmbito da STI, com publicação do documento em uma página própria de suporte (documento SEI nº 0388455)"*.

Contudo, a nosso ver, analisando mais detidamente, o documento mais se assemelha a descrição de procedimentos técnicos, não parecendo tratar-se de política formal da Instituição.

A ISO 27002:2005 indica que a PSI *seja apoiada por políticas de tópicos específicos, que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos.*

Dentre os tópicos específicos das políticas de segurança da informação, temos: controle de acesso, classificação e tratamento da informação, segurança física e do ambiente, *backup*, segurança nas comunicações e outros.

A política de cópias de segurança tem como objetivo proteger a Instituição contra a perda de dados, estabelecendo diretrizes para a implementação do plano de *backup*, buscando definir os requisitos para proteção e retenção, devendo levar em consideração:

***ISO 27002:2005** (substituída pela 27002:2013):*
12.3.1 Cópias de Segurança das Informações
Diretrizes para implementação
Quando da elaboração de um plano de backup, convém que os seguintes itens sejam levados em consideração:
a) registros completos e exatos das cópias de segurança e documentação apropriada sobre os procedimentos de restauração da informação, os quais convém que sejam produzidos;
b) a abrangência (por exemplo, completa ou diferencial) e a freqüência da geração das cópias de segurança reflitam os requisitos de negócio da organização, além dos requisitos de segurança da informação envolvidos e a criticidade da informação para a continuidade da operação da organização;
c) convém que as cópias de segurança sejam armazenadas em uma localidade remota, a uma distância suficiente para escapar dos danos de um desastre ocorrido no local principal;
d) convém que seja dado um nível apropriado de proteção física e ambiental das informações das cópias de segurança (ver 11), consistentes com as normas aplicadas na instalação principal;
e) convém que as mídias de backup sejam regularmente testadas para garantir que elas são confiáveis no caso do uso emergencial; Convém que isto seja combinado com um teste de restauração e checado contra o tempo de restauração requerido. Convém que os

testes da capacidade para restaurar os dados copiados sejam realizados em uma mídia de teste dedicada, não sobrepondo a mídia original, no caso em que o processo de restauração ou backup falhe e cause irreparável dano ou perda dos dados;
f) em situações onde a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de encriptação.

PESSOAL

R.8) Sejam formalizadas/definidas as competências necessárias para o pessoal de TI; a ausência de definição das competências necessárias para os servidores, incluindo o pessoal de TI, pode impor ao Regional o risco de ineficiência na aplicação dos recursos, não obtenção dos benefícios esperados dos investimentos em tecnologia e não realização dos objetivos estratégicos do órgão. Recomenda-se que os responsáveis pela gestão de TI com o apoio da Secretaria de Gestão de Pessoas estabeleçam uma abordagem estruturada para a gestão de pessoas, com definição e comunicação dos papéis e responsabilidades, capacitação, expectativas e avaliações de desempenho.

COBIT 5:

APO07 – Gerenciar Recursos Humanos *- Fornece uma abordagem estruturada para garantir a estruturação ideal, colocação, direitos de decisão e as habilidades dos recursos humanos. Isso inclui a comunicação de papéis e responsabilidades definidas, planos de aprendizagem e de crescimento, e as expectativas de desempenho, com o apoio de pessoas competentes e motivadas.*
Explica como o desempenho dos indivíduos deve ser alinhado aos objetivos corporativos, como as habilidades dos especialistas em TI devem ser mantidas, e como as responsabilidades devem ser definidas.

Acórdão TCU 1.233/2012 – 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);

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);

R.9) Seja estabelecida a avaliação específica de desempenho do pessoal de TI, devendo ser implementadas avaliações em relação a objetivos individuais derivados dos objetivos do órgão, responsabilidades específicas do trabalho e estrutura de competências e habilidades;

R.10) ***Sejam previstos pela administração os quantitativos ideais da força de trabalho de TI,*** *conforme consta no § 1º do art. 13 da Resolução do CNJ nº 211/2015, assim como no Item 9.1.2. do Acórdão TCU nº 1.603/2008 – Plenário:*

Resolução CNJ nº 211/2015:

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.

Acórdão TCU nº 1.603/2008 – 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. 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;

Acórdão TCU 1.233/2012 – 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);

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);

GESTÃO DOS PROCESSOS

R.11) Avaliar a necessidade de formalização de processos de gestão de portfólio de serviços, de mudanças, de configuração, de liberação e implantação, de eventos, de problemas, se ainda não contemplados;

Acórdão TCU nº 1.603/2008 – 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;

Acórdão TCU nº 1.233/2012 – 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:
(...)
9.13.5. 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);
9.13.7. 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);
9.13.9. crie procedimentos para orientar os entes sob sua jurisdição na implementação dos seguintes controles (subitem II.8):
(...)
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;

R.12) Implementação do processo de Gerenciamento de Riscos de TIC formalmente instituído para continuamente identificar, avaliar e responder aos riscos relacionados à TIC, conforme as diretrizes estabelecidas pela governança de TIC;

COBIT 5:

APO12 – Gerenciar os riscos: *Identificar continuamente, avaliar e reduzir os riscos relacionados a TI dentro dos níveis de tolerância estabelecidos pela diretoria executiva da organização.*

EDM03 – Assegurar a otimização de riscos: *Assegura que o apetite e tolerância a riscos da organização são compreendidos, articulados e comunicados e que o risco ao valor da organização relacionado ao uso de TI é identificado e controlado.*

Acórdão TCU nº 1.233/2012:

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):
(...)
9.13.9.3. 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;
(...)
9.13.14. 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):
9.13.14.1. planejamento estratégico institucional;
9.13.14.2. planejamento estratégico de TI;
9.13.14.3. funcionamento dos comitês de TI;
9.13.14.4. processo orçamentário de TI;
9.13.14.5. processo de software;
9.13.14.6. gerenciamento de projetos;
9.13.14.7. gerenciamento de serviços de TI;
9.13.14.8. segurança da informação;
9.13.14.9. gestão de pessoal de TI;
9.13.14.10. contratação e gestão de soluções de TI;
9.13.14.11. monitoração do desempenho da TI organizacional;
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);
(...)

R.13) Recomendar que os processos de gestão da segurança da informação já formalizados sejam utilizados plenamente, tendo em vista o que recomenda o domínio APO13 do COBIT 5 e os Acórdãos do TCU nº 1.233/2012 e 1.603/2008 – Plenário:

COBIT 5:

APO13 – Gerenciar a segurança: *Define, opera e monitora um sistema para a gestão de segurança da informação.*

Acórdão TCU nº 1.233/2012:

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;
(...)
9.13.14. 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;
(...)

Acórdão TCU nº 1.603/2008 – 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 ricsos de TI, a área específica para gerenciamento da segurança da informação, a política de segurança da informação e os procedimentos de controle de acesso;

R.14) A promoção periódica de ações de sensibilização, conscientização e capacitação em segurança da informação para os agentes públicos da instituição como prática do processo de gerenciamento de riscos de TI. O gerenciamento de riscos, para ser efetivo, deve ser composto por práticas que promovam a cultura da segurança no ambiente organizacional. Efetuar ações de conscientização e capacitação em segurança da informação é um meio eficaz de reforçar os comportamentos desejados e reduzir os indesejados.

R.15) Instituir formalmente as atividades de escritório de projetos de TI (PMO);

O PMO (Project Management Office) é definido como uma estrutura de gerenciamento que padroniza os processos de governança relacionados a projetos e facilita o compartilhamento de recursos, metodologias, ferramentas e técnicas, conforme o guia PMBOK 5ª edição (fonte: *https://amauroboliveira.files.wordpress.com/2015/11/fundamentos-em-gerenciamento-de-projetos.pdf*)

Um escritório de projetos (Project Management Office - PMO) é um corpo ou entidade organizacional cujas responsabilidades estão relacionadas ao gerenciamento centralizado e coordenado dos projetos sob seu domínio. É uma unidade organizacional com o objetivo de conduzir, planejar, organizar, controlar e finalizar as atividades do projeto. Devendo abrigar pessoas com conhecimentos de Gerenciamento de Projetos, capazes de prestarem todo o suporte necessário aos gerentes de projeto e sua equipe. (fonte: *https://projetoseti.com.br/o-que-um-pmo-escritorio-de-projetos-introducao/*)

R.16) Instituir formalmente processo para o gerenciamento do portfólio de projetos de TI bem como para o gerenciamento de projetos de TI;

O gerenciamento de projetos é a aplicação de conhecimentos, habilidades, ferramentas e técnicas adequadas às atividades do projeto, para atender aos seus requisitos, conforme o guia PMBOK 5ª edição. [PMI 2012, p. 5]

Trata-se de uma competência estratégica para organizações, permitindo a união dos resultados dos projetos com os objetivos do negócio.

O gerenciamento dos portfólios de serviços e projetos de TIC deve ser continuamente avaliado pela função de governança para determinar a probabilidade de atingir os objetivos do órgão e agregar valor a um custo razoável. Na avaliação, deve-se identificar quaisquer mudanças de direção que precisem ser dadas à administração para otimizar a criação de valor.

Acórdão TCU nº 1.233/2012:

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);
(...)

RESULTADOS

R.17) Crie mecanismos de controle, definindo indicadores que mensurem o desempenho para acompanhar o grau de alcance dos objetivos e benefícios estimados nos projetos específicos de TI, atuando para garantir que o desempenho, a medição e os relatórios de desempenho e conformidade da TI sejam transparentes.

Acórdão TCU nº 2.308/2010 – Plenário:

9.1. recomendar ao Conselho Nacional de Justiça – CNJ, (...) 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;

Acórdão TCU nº 1.233/2012 – 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:
9.13.14. 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):
(...)
9.13.14.11. monitoração do desempenho da TI organizacional.

R.18) Cumpra as iniciativas programadas constantes no Plano de Trabalho previsto no art. 29 da Resolução nº 211/2015;

Os resultados encontrados demonstram que este Regional atendeu, em sua maioria, aos critérios referentes ao Grupo 1 do Plano, evidenciando que as diretrizes estabelecidas pela Resolução CNJ nº 211/2015 estão sendo implementadas em boa parte, por esse Tribunal. Contudo, ainda existem diversas ações a serem adotadas, portanto, devem ser impulsionadas as ações pendentes, em observância aos prazos definidos no Plano de Trabalho constante no SEI nº 0003396-85.2017.6.02.8000, evento 0237034.

Lembramos que as ações envolvem não somente iniciativas da Secretaria de Tecnologia da Informação, mas também, da CODES/SGP, da Secretaria Judiciária, da Assessoria Jurídica da Presidência e da Presidência.

Resolução Nº 211 de 15/12/2015:

Art. 29. Cada órgão deverá elaborar um Plano de Trabalho, para atendimento aos critérios estabelecidos nesta Resolução, conforme modelo a ser disponibilizado pelo Conselho Nacional de Justiça.
§ 1º O Plano de Trabalho deverá ser entregue ao CNJ até o dia 31 de março de 2016 e seguir a estrutura de grupos de entregáveis, com previsão de atendimento integral dos critérios até dezembro de 2020, com os seguintes prazos de atendimento intermediário para adequação:

I – Grupo 1: da governança e da gestão de Tecnologia da Informação e Comunicação o prazo é de até 1 (um) ano, contado após a vigência desta Resolução;
II – Grupo 2 dos padrões de desenvolvimento e de sustentação de sistemas de informação é de até 2 (dois) anos, contados após a vigência desta Resolução;
III – Grupo 3: da infraestrutura tecnológica o prazo é de até 3 (três) anos, contados após a vigência desta Resolução;
IV– Grupo 4: do quadro permanente de servidores e da elaboração de política de gestão de pessoas prazo é de até 4 (quatro) anos, contados após a vigência desta Resolução.
§ 2º O Conselho Nacional de Justiça realizará no final do prazo de conclusão de cada grupo de entregáveis do Plano de Trabalho, uma avaliação do cumprimento dos itens constantes desta Resolução.
(...)

Art. 32. O CNJ realizará anualmente diagnósticos para aferir o nível de cumprimento das Diretrizes Estratégicas de Nivelamento constantes desta Resolução, especialmente no que se refere aos domínios Governança e Gestão de, e Infraestrutura de TIC, bem como em outras Resoluções, recomendações e políticas estabelecidas para os órgãos do Poder Judiciário.

Parágrafo único. Os diagnósticos descritos no caput deste artigo serão realizados a partir de questionários e outros procedimentos de acompanhamento que permitam realizar o levantamento de informações relacionadas à evolução dos Viabilizadores de Governança de Tecnologia da Informação e Comunicação nos órgãos do Poder Judiciário.

ATUAÇÃO DA UNIDADE DE AUDITORIA INTERNA

R.19) Recomendar que a Unidade de Auditoria Interna elabore seu Plano Anual de Auditoria considerando os temas governança de TI, riscos de TI e controles de TI, diante das recomendações do TCU, a exemplo:

Acórdão TCU nº 1.233/2012:

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);

Em relação às auditorias ressaltamos que foi realizada avaliação sobre as diretrizes formuladas pelo CNJ em relação à Resolução CNJ nº 182/2013, nos anos de 2015 e 2016, e por conta do presente trabalho, em 2017. Ao compararmos o trabalho realizado na presente auditoria com a auditoria anterior na área de Tecnologia da Informação realizada em 2017, no que diz respeito à Resolução nº 182/2013 - CNJ, constatamos que foram adotadas várias medidas no decorrer de 2017.

Quanto à instrução adequada dos procedimentos de contratações de soluções de TIC, reiteramos as recomendações já constantes no SEI nº 0009610-92.2017.6.02.8000, especialmente no Anexo II (evento 0334556) do Relatório de Auditoria, que indica as sugestões de conteúdo para o atendimento de cada requisito da Resolução CNJ nº 182/2013.

Nesse sentido, no que diz respeito aos procedimentos verificados na presente auditoria, SEI nº 0004338-20.2017.6.02.8000, SEI nº 0009704-40.2017.6.02.8000 e SEI nº 0001041-05.2017.6.02.8000, convém destacar a necessidade constante de aperfeiçoamento da instrução processual. É possível observar, por exemplo, que alguns aspectos deixaram de ser verificados, tais como: papéis a serem desempenhados pelos atores do órgão e da empresa envolvidos; acompanhamento em relação ao atendimento aos prazos de garantia; comunicação e acompanhamento da execução do contrato; transferência de conhecimento entre contratante e contratado, quando houver; qualificação técnica ou formação dos profissionais alocados na execução do contrato.

Quanto à Resolução CNJ nº 211/2015, foi mencionada, de forma breve, diante do Levantamento de Governança, Gestão e Infraestrutura de TIC do Poder Judiciário - iGovTIC - JUD 2015/2016, no procedimento SEI nº 0009610-92.2017.6.02.8000, quando o TRE-AL obteve como nota do nível de maturidade: 0,58 (Satisfatório). A STI destaca que houve um avanço no índice do resultado no iGOVTIC-JUD2017, evoluindo o índice de maturidade de "baixo" para "satisfatória", ocupando no iGovTIC-JUD 2017: o 52º lugar na Classificação Geral; o 20º lugar na Classificação dos Órgãos de Pequeno Porte; e o 11º lugar na Classificação por segmento: TREs; (fonte: http:// www.cnj.jus.br/files/conteudo/arquivo/2017/11/6aecee94b2023b5e1c125c1b4865bf39.pdf)

A Unidade de Auditoria Interna (UAI) não realizou, no período de 2015 a 2017, exames de auditoria para aferir o estágio da governança de TI, vindo realizar breve verificação por meio da presente Ação Coordenada de Auditoria.

Conforme ressaltado no Achado 1, não foi constatada um atuação efetiva do Comitê de Governança de Tecnologia da Informação e Comunicação (CGOVTIC), de acordo com o ato que o instituiu:

> ***A.1)*** *Por meio da Resolução nº 15.732 de 13/09/2016 foi instituída a Governança Corporativa de Tecnologia da Informação e Comunicação no âmbito do TRE/AL, com a composição e competência do Comitê de Governança de TIC, bem como do Comitê de Gestão de TIC; o Comitê de Governança de TIC reuniu-se apenas uma vez em 2018, conforme ata do dia 19/03/2018,* ***não ficando demonstrado um envolvimento e uma atuação efetiva, considerando as prioridades que envolvem a área de governança de TI;***

Cumpre lembrar que são competências do Comitê, previstas no art. 7º da referida Resolução:

> *I - definir princípios e diretrizes que orientem a forma de utilização da TIC no TRE-AL;*
> *II - estabelecer objetivos de TIC, bem como deliberar e priorizar planos deles decorrentes;*
> *III - definir as prioridades de investimentos em TIC;*

IV - deliberar acerca dos relatórios de análise de riscos, de níveis de serviço, de capacidade ou de disponibilidade, entre outros;
V - aprovar a alocação dos recursos orçamentários destinados à TIC, bem como alterações posteriores;
VI - deliberar e priorizar planos submetidos pelo CGTIC;
VII - acompanhar, periodicamente, a execução dos planos e a evolução dos indicadores de desempenho de TIC, para ratificar ou reavaliar as prioridades, identificar eventuais desvios e determinar correções necessárias;
VIII - divulgar aspectos da Governança Corporativa de TIC, como princípios, diretrizes, objetivos, planos.

A Resolução definiu, ainda, a periodicidade das reuniões do aludido Comitê (ordinariamente, uma vez a cada trimestre), o que não vem sendo observado:

Art. 8º O CGOVTIC será conduzido pelo Presidente ou Corregedor Regional Eleitoral, ou, ainda, pelo Diretor-Geral, e reunir-se-á ordinariamente, uma vez a cada trimestre, e extraordinariamente, sempre que necessário.
§ 1º Além dos assuntos relacionados às competências listadas no art. 7º, poderão ser incluídos na pauta das reuniões outras matérias relevantes.

Desta feita, justifica-se a recomendação 01 do presente relatório, com o intuito de estimular a atuação do Comitê de Governança de Tecnologia da Informação e Comunicação (CGOVTIC) deste Tribunal.

Sendo estas as observações, ressaltamos que as recomendações propostas buscam contribuir para o aperfeiçoamento da governança e gestão de TIC, com o objetivo de promover maior alinhamento entre a TIC e os objetivos e necessidades do Tribunal, gerenciamento de riscos relacionados com o uso da tecnologia e otimização dos recursos investidos, de modo a gerar maior eficiência na prestação dos serviços.

Maceió/AL, 31 de agosto de 2018.

Waleska Silva de Carvalho Cardoso
Assistente IV / Assessoria de Auditoria

Giane Duarte Coêlho Moura
Coordenadora de Controle Interno e Auditoria