TRIBUNAL REGIONAL ELEITORAL DA BAHIA
SECRETARIA DE CONTROLE INTERNO E AUDITORIA
COORDENADORIA DE AUDITORIA, ACOMPANHAMENTO E ORIENTAÇÃO DA GESTÃO
SEÇÃO DE AUDITORIA

RELATÓRIO DE AUDITORIA Nº 03/2013

OBJETO: TECNOLOGIA DA INFORMAÇÃO

Auditoria Coordenada – CNJ/TSE/TRE-BA

Agosto/2013

RELATÓRIO DE AUDITORIA Nº 03/2013

OBJETO: Tecnologia da Informação

I INTRODUÇÃO

Em atendimento ao Ofício Circular nº 12/2012 – SCI/Presi/CNJ, do Conselho Nacional de Justiça, que propôs a realização de Ações Coordenadas de Auditoria, bem como a inclusão de áreas específicas no Plano Anual de Atividades de Auditoria – PAAA/2013 deste Tribunal, realizou-se a presente auditoria com a finalidade de verificar a aderência da área de Tecnologia da Informação às diretrizes estabelecidas na Resolução CNJ n° 90/2009 e nas recomendações constantes dos subitens 9.13.14 e 9.13.15 do Acórdão nº 1.233/2012 - TCU-Plenário.

Preliminarmente, cabe ressaltar que este Tribunal tomou conhecimento apenas na data de 29.07.13, quanto aos pontos de auditoria constantes da Matriz de Procedimentos elaborada pelo CNJ, fato esse que limitou a metodologia e técnicas de auditoria utilizadas. Dessa forma, as fases de planejamento, execução e apresentação do relatório para fins deferimento por parte da Administração se processaram todas no exíguo prazo de 16 (dezesseis) dias corridos.

Registre-se, ainda, que o reduzido número de servidores alocados nas atividades de auditoria, a exigüidade do tempo para a realização dos trabalhos, a concomitância da execução das auditorias de gestão para fins do processo de contas, e a inexistência de servidor lotado no Controle Interno com formação na área de TI, foram fatores que ocasionaram restrições aos trabalhos. Dessa forma, a aderência da área TI

às regras estabelecidas nas Resoluções CNJ nº 90/2009 e Acórdão TCU nº 1.233/2012 - Plenário foi avaliada a partir da análise das informações prestadas pelas áreas competentes.

II OBJETIVO

Avaliar os critérios estabelecidos em governança, riscos e controles de TI e a existência dos controles internos definidos para mitigar os riscos das atividades nos processos relacionados à área de TI, tais como Planejamento Estratégico Institucional, Planejamento Estratégico de TI e funcionamento dos Comitês de TI, dentre outros.

III METODOLOGIA

O escopo e as questões de auditoria foram delimitados a partir das instruções encaminhadas pelo CNJ, por meio do Tribunal Superior Eleitoral (TSE), no Ofício-Circular n° 12/2012-SCI/Presi/CNJ de 10.12.2012, e na mensagem eletrônica de 29.07.2013, acima referidos, estruturando-se na “Matriz de Procedimentos para Realização de Auditoria na Área de Tecnologia da Informação”, anexa e que faz parte integrante do presente relatório.

Na presente auditoria foi aplicada a técnica de aplicação de questionários dirigidos à área fim, ou seja, à Secretaria de Tecnologia da Informação (STI) e à Comissão de Segurança da Informação, utilizando-se, ainda, o exame documental e a correlação de dados.

A partir dos quesitos propostos foram expedidas Solicitações de Auditoria

às unidades conforme suas competências regimentais relativas à instrução e gestão de Tecnologia da Informação, com aplicação de questionários.

A partir da análise das informações recebidas e da correlação dos dados procedeu-se ao preenchimento da matriz e a avaliação da necessidade de exame documental direto, ressalvando-se, contudo, no que concerne aos aspectos relativos à Segurança da Informação, que a opinião da auditoria fundamentou-se nas informações prestadas pela Comissão de Segurança da Informação, que detém a competência específica na área.

Em decorrência da avaliação acima informada foram expedidas solicitações adicionais, com requisição de documentos para análise quando necessário.

Analisados os documentos requisitados, em confronto com as informações anteriormente obtidas, foram concluídos os trabalhos de auditoria, conforme resultados abaixo registrados.

IV FONTES CONSULTADAS

Os trabalhos de auditoria fundaram-se na aplicação das técnicas de auditoria acima relatadas a partir dos normativos e documentos abaixo relacionados:

a. Resolução CNJ n° 90/2009, de 29.09.2009;
b. Acórdão nº 1.233/2012-TCU -Plenário- subitens 9.13.14 e 9.13.15;
c. Respostas às Solicitações de Auditoria n°s 56/2013, 59/2013, 61/2013 e 62/2013;

V CONCLUSÃO

Dos exames realizados, foi verificado que, no tocante ao perfil dos recursos humanos envolvidos, a força de trabalho empregada na área de TI deste Tribunal é ainda insuficiente para o atendimento da crescente demanda, quer em termos quantitativos, quer em relação aos cargos específicos da área de TI.

Consoante informação prestada pela Secretaria de Tecnologia da Informação – STI, a força de trabalho na área de TI conta com um quadro efetivo de 50 (cinqüenta) servidores, dos quais apenas 22 (vinte e dois) são ocupantes de cargo específico de TIC. Existem, ainda, mais 10 colaboradores terceirizados e 8 estagiários, totalizando 68 (sessenta e oito) pessoas.

Destaque-se, entretanto, que dos 22 (vinte e dois) servidores ocupantes de cargos especializados em TI, 01 (um) pertence ao quadro do TRE-PE e refere-se a uma servidora removida para este Tribunal para acompanhar o cônjuge.

Além disso, não foram computados outros 02 detentores de cargos específicos pelo fato de não comporem atualmente a força de trabalho da STI, visto que um dos servidores se encontra lotado em outra Secretaria, enquanto que o outro foi cedido para outro Regional, se encontrando esta vaga, portanto, “presa”.

Vale ressaltar que de acordo com o Anexo I da Resolução CNJ nº 90/09, considerando-se a quantidade de usuários de TIC do TRE-BA, seriam necessários 75 servidores do quadro permanente lotados na área de TIC.

No que concerne ao quesito capacitação, foi verificado que este Tribunal aprovou Plano Anual de Capacitação específico para área de TIC, contudo, este não foi ainda, implantado, em que pese a participação eventual de alguns servidores em programa de treinamento da área. Foi detectado que não possui também Programa de Capacitação em Governança e em Atualização em TIC.

Relativamente à seleção de líderes na área de TI, restou configurado que a mencionada área analisa as competências para a seleção de líderes, entretanto, não utiliza critérios formalmente estabelecidos.

Por outro lado, dos testes realizados, verificou-se que este Tribunal busca melhorar a gestão de TI através da execução do Planejamento Estratégico 2010-2014 e do Planejamento Estratégico de TI - PETI, aprovado e instituído pela Res. Administrativa nº 3/2010, os quais se encontram devidamente alinhados às diretrizes estratégicas institucionais e nacionais.

Foi observado, entretanto, que não constam mecanismos, no Planejamento existente, para que a Alta Administração acompanhe o desempenho de TI da instituição, bem assim, que o citado planejamento não vem sendo aperfeiçoado continuamente com base na análise dos seus indicadores.

Com relação ao processo de formalização dos planos vinculados à área de TI, foi constatado que há previsão de elaboração do Plano Diretor de TI (PDTI), ainda sem definição de prazo para sua publicação. Foi, inclusive, solicitado orçamento na Proposta Orçamentária 2012, para fins de contratação de Consultoria com o objetivo de auxiliar a Secretaria de Tecnologia da Informação na sua elaboração, vez que os servidores daquela secretaria não possuem a *expertise* necessária para assumirem tal projeto.

Foi detectado, ainda, que conquanto este Tribunal não disponha de Processo de Gestão de serviços, existe previsão de implantação por meio de projeto a ser entregue pela consultoria em Soluções de TI, prevista para finalizar-se até o dia 30 de agosto de 2013.

Da análise da estrutura de controles internos, restou evidenciado que os seguintes processos não possuem atividades de controle com vistas à mitigação dos riscos envolvidos: Planejamento Estratégico Institucional, Planejamento Estratégico de TI, Funcionamento de Comitês de TI, Processo Orçamentário de TI, Processo de *Software*, Gerenciamento de projetos, Gerenciamento de Serviços de TI, Segurança da Informação, Contratação e Gestão de Soluções de TI e Monitoração do desempenho da TI organizacional.

Saliente-se, contudo, com referência à implementação do processo de gerenciamento de riscos, visando à identificação e mitigação dos riscos associados às atividades críticas deste Tribunal, que se trata de meta definida para após o processo de levantamento de ativos de informação, definido no plano plurianual para 2014.

Há, ainda, como meta formalmente definida para o exercício 2015, a proposta de implantação do Plano de Continuidade de Negócio para as atividades críticas deste Tribunal. Entretanto, a meta 2013 estabelece que a STI já deve criar medidas iniciais de proteção aos seus ativos de informação em 2013.

Verificou-se também que em que pese a inexistência de Comitê instituído especificamente para coordenar os assuntos de Segurança da Informação, este Tribunal dispõe de Comissão de Segurança da Informação, instituída através da Portaria nº 573/2009, de 02.10.09, com vistas à adoção de princípios e valores para

assegurar a integridade, confiabilidade e a disponibilidade das informações no âmbito deste Tribunal.

Pontue-se, ainda, a instituição formal, através do art. 2º da Resolução TRE nº 03/2010, de 26.04.10, de Comitê Gestor do Planejamento Estratégico em Tecnologia da Informação com a finalidade de acompanhar a execução do Planejamento Estratégico de TI, adotando as providências cabíveis para o cumprimento das suas metas.

Destaque-se, contudo, que o referido Órgão ainda não atua de forma plena, de acordo com as suas atribuições descritas na referida Resolução, prejudicando assim o alinhamento dos investimentos de Tecnologia da Informação com os objetivos do Tribunal.

No que diz respeito à Política de Segurança da Informação, restou configurado que este Tribunal adota a estabelecida pelo TSE, conforme Resolução nº 22.780/08, de 27/06/2008, aplicável a toda Justiça Eleitoral, não dispondo, portanto, de política própria na área.

Sobre a citada Política de Segurança, cabe destacar que esta foi amplamente divulgada à época da sua publicação, contudo, atualmente não tem sido difundida entre os co-responsáveis (servidores, estagiários e prestadores de serviço).

No tocante às falhas na Segurança da Informação, foi observado que estas ainda não são formalmente registradas e notificadas ao gestor do ativo e/ou à Comissão de Segurança da Informação, bem assim, que no caso de afastamento

provisório ou desligamento do usuário, suas permissões de acesso não são automaticamente bloqueadas.

Acerca da existência de sistema para classificação das informações, sistemas e equipamentos quanto à necessidade de sigilo, confidencialidade e disponibilidade, foi verificado que este Tribunal possui meta de implantação ainda neste exercício, após o final do processo de levantamento de ativos.

Cabe ressaltar, que foi realizado no exercício 2012 projeto piloto de levantamento de ativos da informação, exclusivamente na Coordenadoria de Produção e Suporte - CODEPS. Entretanto, existe meta para levantamento de todos os ativos da informação das outras unidades ainda para este ano de 2013, podendo este processo vir a ser adiado em razão do processo de reestruturação deste Tribunal.

Examinou-se, em seguida, o processo de contratação e gestão de bens e serviços de TI, verificando-se que este Tribunal ainda não adota processo de trabalho formalizado, baseado em estudos técnicos preliminares a fim de avaliar a necessidade e viabilidade da contratação, nem possui área específica de gestão de contratos de bens e serviços de TI para gerir adequadamente os riscos inerentes às atividades de TI. Realiza, contudo, estudos técnicos preliminares para elaboração dos seus Termos de Referência e Projetos Básicos, ainda que inexistam controles formalizados que comprovem tais pesquisas.

ACHADOS:

1) Insuficiência de pessoal de cargo privativo da área de TI;

2) Lotação de servidor de cargo específico da área de TI em unidade diversa da de Tecnologia da Informação;
3) Não implantação do Plano Anual de Capacitação de Pessoal específico para gestão de TI e inexistência de Programa de Capacitação em Governança e em Atualização em Tecnologia da Informação;
4) Ausência de critérios formalmente estabelecidos para análise das competências multidisciplinares para seleção de líderes na área de TIC;

7) Ausência de mecanismos de controle, no Planejamento existente, para que a Alta Administração acompanhe o desempenho de TI da instituição, bem assim, ausência de aperfeiçoamento contínuo do citado planejamento com base na análise dos seus indicadores;

8) Ausência de Plano Diretor de Tecnologia da Informação e Comunicação, de Processo de software definido, de Processo de Gerenciamento de Projetos e de Modelo de Processo de Gestão de Serviços;
9) Ausência de atividades de controle para fins de mitigação dos riscos relacionados aos processos de: Planejamento Estratégico Institucional, Planejamento Estratégico de TI, Funcionamento de Comitês de TI, Processo Orçamentário de TI, Processo de Software, Gerenciamento de Projetos, Gerenciamento de Serviços de TI, Segurança da Informação, Contratação e Gestão de Soluções de TI e Monitoração do Desempenho da TI Organizacional;
10) Ausência de divulgação da Política de Segurança da Informação adotada entre os servidores, estagiários e prestadores de serviços;

11) Inexistência de registro formal das falhas de Segurança da Informação e ausência de notificação das mencionadas falhas ao gestor do ativo e/ou à Comissão de Segurança da Informação;
12) Não adoção da sistemática de bloqueio automático das permissões de acesso no caso de afastamento provisório ou desligamento do usuário;
13) Inatividade do Comitê que decide sobre a priorização das ações e investimentos de TI;
14) Inexistência de processo de gestão de risco de Segurança da Informação, de Plano de Continuidade do Negócio, de Política de Segurança da Informação própria e de Processo de Classificação das informações, sistemas e equipamentos quanto à necessidade de sigilo, confidencialidade e disponibilidade;
15) Ausência de levantamento do Inventário de Ativos de TI no exercício 2012 em todas as unidades do Tribunal;
16) Ausência de processo de trabalho formalizado ou de área específica de gestão de contratos de bens e serviços de TI;

RECOMENDAÇÕES À ADMINISTRAÇÃO:

1- Que determine à SGP a lotação exclusiva dos servidores ocupantes de cargo da área específica de TI na Secretaria de Tecnologia da Informação, adotando, inclusive, providências no sentido de identificar o servidor da área de TI lotado em secretaria diversa, lotando-o de imediato na STI;

2- Que determine à STI que oriente os servidores de cargo privativo, no sentido de que priorizem a realização das atividades pertinentes à área de TI, em detrimento das de cunho administrativo;

3- Que determine a STI, SGP, SOF e SGA a adoção das providências pertinentes a cada área, e necessárias à implantação, já no exercício 2014, do Plano Anual de Capacitação de Pessoal específico para gestão de TI;

4- Que determine à SGP, que em parceira com a STI, elabore, a fim de ser implementado já no exercício 2014, o Programa de Capacitação em Governança e em Atualização em Tecnologia da Informação deste Tribunal;

5- Que determine à SGP, que em parceria com a STI, estabeleça formalmente critérios para análise das competências multidisciplinares para seleção de líderes na área de TIC;

6- Que determine à DG/COPEG, que em parceria com a STI, crie mecanismos de controle, no Planejamento de TI existente, para que a Administração acompanhe o desempenho de TI da instituição, bem assim, mecanismos de aperfeiçoamento contínuo do citado planejamento com base na análise dos seus indicadores;

7- Que determine a STI, que em parceria com os membros da Comissão de Segurança da Informação e SOF, elabore e submeta à apreciação superior, no prazo de 60 (sessenta) dias, cronograma para cumprimento de todas prescrições contidas na Resolução CNJ nº 90/2009;

8- Que determine à STI, que em parceria com a DG/COPEG e Comissão de Segurança da Informação, defina as atividades de controle necessárias com vistas à mitigação dos riscos nos seguintes processos: Planejamento Estratégico Institucional, Planejamento Estratégico de TI, Funcionamento de Comitês de TI, Processo Orçamentário de TI, Processo de Software, Gerenciamento de

projetos, Gerenciamento de serviços de TI, Segurança da Informação, Contratação e gestão de soluções de TI e Monitoração do desempenho da TI organizacional;

9- Que determine à Comissão de Segurança da Informação que: promova ações no sentido de divulgar a Política de Segurança da Informação adotada neste Tribunal entre os servidores, estagiários e prestadores de serviços; bem como, que expeça orientação a todas as unidades deste Tribunal, no sentido de informarem, àquela Comissão, bem assim, ao gestor do ativo, para fins de registro, as falhas de segurança da informação que tiverem conhecimento, determinando, ainda, que a citada Comissão mantenha registro formal das mencionadas falhas;

10-Que determine à STI que, em parceria com a SGP, adote providências com vistas ao bloqueio automático das permissões de acesso no caso de afastamento provisório ou desligamento do usuário;

11-Que determine ao Comitê Gestor do Planejamento Estratégico de Tecnologia da Informação que adote as medidas necessárias no sentido de efetivação de suas ações;

12-Que determine à Comissão de Segurança da Informação que, conforme prescrição do art. 23, da Resolução TSE nº 22.780/08, elabore formalmente e submeta à apreciação da Presidência desta Casa, no prazo máximo de 90 (noventa) dias:

1. Processo formal de gestão de riscos de Segurança da Informação;
2. Plano de Continuidade do Negócio;

3. Política de Segurança da Informação própria para este Tribunal, levando em consta suas características e peculiaridades, e tendo como fundamento as diretrizes estabelecidas na Resolução TSE nº 22.780/08.
4. Processo de classificação das informações, sistemas e equipamentos deste Tribunal, quanto à necessidade de sigilo, confidencialidade e disponibilidade;

13- Que determine à STI que, em parceria com a Comissão de Segurança da Informação, adote as providências com vistas ao levantamento do inventário de ativos de TI em todas as unidades do Tribunal, a ser realizado ainda no presente exercício;

14-Que determine à STI, que em parceria com a SGA/COGELIC, elabore processo de trabalho formalizado com vistas à gestão de contratos de bens e serviços de TI, submetendo-o em seguida à apreciação superior;

15-Que determine à STI, SGA, SGP, SOF, COPEG e Comissão de Segurança da Informação que mantenham esta Secretaria informada acerca de todas as providências adotadas com vistas ao atendimento das presentes recomendações, de modo especial, através da utilização do e-mail desta Seção de Auditoria, seaud@tre-ba.gov.br.

Do exposto, concluímos pela aderência parcial da Gestão de Tecnologia da Informação (TI) do TRE/BA às diretrizes estabelecidas pela Resolução CNJ nº 90/2009 e às recomendações constantes dos subitens 9.13.14 e 9.13.15 do Acórdão nº 1.233/2012 - TCU-Plenário, com esforços no sentido da sua integral implementação, classificando-a, contudo, em nível insuficiente, visto que requer aprimoramentos, notadamente no que concerne à inexistência de Plano Diretor de TI, de Processo de

Gestão de Serviços, de Processo para Contratação e Gestão de Solução de TI, ausência de controles internos para mitigar riscos na área, programa de capacitação em governança e em atualização em TI, e demais itens constantes dos achados supra relatados.

Dessa forma, propomos as recomendações acima com vistas à minimização e/ou correção das não conformidades detectadas, sem prejuízo, contudo, de ulteriores recomendações a serem propostas pelo CNJ/TSE.

Sugere-se o encaminhamento do presente Relatório à Presidente desta Casa, a quem compete a apreciação e a autorização de remessa ao TSE para que promova o encaminhamento ao CNJ, ressaltando o prazo limite de 14 de agosto corrente para a remessa das informações, em observância ao cronograma fixado pelo CNJ. É o relatório. À consideração superior.

Salvador, 12 de agosto de 2013.

Rita Dantas Freitas Vigas
Auditora

De acordo. À SCI.
Em 12.08.13.

Ana Rejane Catunda de Carvalho
Chefe da Seção de Auditoria
e Coordenadora da COGES Substituta