RELATÓRIO PRELIMINAR DE AUDITORIA

I. IDENTIFICAÇÃO:

Unidade Auditada: TRIBUNAL DE JUSTIÇA DO ESTADO DE RORAIMA

Responsável: PRESIDÊNCIA DO TRIBUNAL DE JUSTIÇA

Assunto: Auditoria Especial (coordenada pelo CNJ)
Área: TIC (Of. Circ. N.º 12/2012 – CNJ)

II. DADOS GERAIS

a) Período de Planejamento

O planejamento da auditoria foi realizado pela Secretaria de Controle Interno do Conselho Nacional de Justiça e comunicada aos Tribunais por meio do Ofício Circular n.º 12/2012 – SCI/Presi/CNJ, de 10 de dezembro de 2012.

b) Execução dos trabalhos

Os trabalhos de auditoria foram executados no período de 17 de junho de 2013 a 10 de Julho de 2013.

c) Período de Elaboração do Relatório Preliminar

No período de 11 a 13 de Agosto de 2013 foi elaborado este Relatório Preliminar da Auditoria.

d) Período de Elaboração do Relatório Final

Será elaborado Relatório Conclusivo da Auditoria após manifestação da Administração quanto ao Relatório Preliminar, que ocorrerá no período de 13 a 20 de agosto de 2013.

d) Equipe de Trabalho

A equipe de trabalho, composta por servidores do Núcleo de Controle Interno, foi definida pela Portaria n.º 955, de 24 de junho de 2013.

SERVIDORES	CARGO/FUNÇÃO	ATUAÇÃO
Maria Josiane Lima Prado	Coord. do Núcleo de Controle Interno	Supervisora
Ediel Pessoa da Silva Junior	Analista de Sistemas	Coordenador
Osmar Malucelli Filho	Assessor Jurídico	Membro

III. INTRODUÇÃO

A área de Tecnologia de Informação – TI, vem já há muito tempo galgando crescente importância dentro da estrutura da Administração Pública. Assim sendo, sua governança se tornou indispensável para que órgãos e entidades públicas cumpram suas missões institucionais.

Neste compasso, garantir que a TI agregue valor ao negócio com riscos aceitáveis, tem se tornado o grande desafio a ser enfrentado pela Alta Administração de cada organização.

Segundo palavras do *r.* Ministro Augusto Sherman, 30 Anos de TI no TCU: "***A tecnologia da informação é o coração da administração pública, podendo fazê-la parar ou avançar***".

Seguindo essa didática, impera a constatação de que, muito embora a TI seja uma atividade-meio, o amadurecimento do setor e sua atuação conjunta com a área do negócio para atingimento dos objetivos, acaba levando-a a obter tratamento de área-fim.

Dito isto, impende atestar que a TI está intimamente ligada às questões estratégicas de qualquer organização, e por conseqüência desta Corte de Justiça.

Nesta esteira, apresentamos o relatório preliminar da auditoria realizada no Tribunal de Justiça do Estado de Roraima, sob a orientação da Secretaria de Controle Interno do Conselho Nacional de Justiça - CNJ, em parceria com os demais Tribunais de Justiça Estaduais do Brasil, segundo critérios, metodologias e procedimentos previamente definidos por aquele Conselho.

A auditoria em questão, encetada por meio do Oficio n.º12/2012, - SCI/Presi/CNJ, objetiva avaliar o cumprimento das diretrizes definidas pela Resolução n.º 90/2009 e recomendações presentes no Acórdão n.º 1233/2012-TCU– Plenário, pertinente a governança de TI.

Busca-se avaliar o nivelamento da administração em atividades com criticas que envolvem processos como: funcionamento dos comitês de TI, processo de software, gerenciamento de projetos, gerenciamento de processos, gerenciamento de serviços de TI, segurança da informação, gestão de pessoal de TI e o seu alinhamento ao planejamento estratégico institucional, segundo as boas práticas parametrizadas por frameworks utilizados internacionalmente tal como Cobit 4.1, onde a maior parte das normas e orientações baseiam-se. Ademais foi realizado o levantamento dos bens de TI doados a este Tribunal.

Para viabilizar a análise, foram formuladas as seguintes questões de auditoria, que integram a Matriz de Procedimentos enviada pelo CNJ:

1. A gestão de recursos humanos de TIC atual segundo as normas e boas práticas?

2. Existem controles que garantam a qualificação necessária para acesso às funções de liderança nos setores de TIC?

3. Existem controles adotados no Tribunal para mitigar riscos na gestão de TIC?

4. Os mecanismos de controle adotados para garantir a segurança da informação são suficientes?

5. Regularidade das doações dos bens de TIC recebidas do CNJ.

6. Existe processo para contratação e gestão de soluções de TIC?

Para subsidiar os trabalhos, foram realizadas solicitações formais junto aos setores internos envolvidos quando na oportunidade da reunião de apresentação, conforme rito da Resolução n.º 171/2013.

IV. RESULTADOS DA AUDITORIA

1) DA GESTÃO DE RECURSOS HUMANOS DE TIC

Imprescindível notar que atualmente, cada vez mais as organizações tornam-se dependentes de tecnologia da informação e comunicação, deixando de considerar como mero suporte e passando a integrar a estratégia da organização. Nesse sentido é prudente manter a área de TIC com estrutura suficiente para atender ao porte da organização.

Nesta esteira, para que possamos garantir a estrutura acima citada, faz-se necessário uma periódica avaliação quantitativa e qualitativa dos recursos humanos do setor, bem como criar política para fixação destes.

Importante frisar que tal medida é preocupação latente dos órgãos de controle do judiciário. A própria Resolução n.º 90/2009, ratifica, ao determinar a implantação do plano anual de capacitação, a importância de manter os recursos humanos consoante com a necessidade da Instituição.

a) Quantitativo mínimo de servidores.

O quantitativo mínimo de servidores é a garantia de pessoal para a execução das atividades. O Acórdão n.º 1603/2008 - TCU - Plenário ressalva a importância de dotar a área de TIC de estrutura suficiente para o pleno desempenho de suas atribuições, mantendo quadro de pessoal efetivo, acompanhando o crescimento do órgão, em detrimento de colaboradores externos participando de atividades sensíveis.

Reforçando o exposto no parágrafo acima, a Resolução n.º 90/2009 - CNJ, determina ao tribunal manter quadro de pessoal permanente compatível com a demanda e o porte, adotando como critérios para fixar o quantitativo necessário, dentre outros, **o número de usuários internos de recursos de TIC, o grau de informatização, o número de estações de trabalho, o desenvolvimento de projetos na área de TIC e o esforço necessário para o atingimento das metas do planejamento estratégico**, apresentando como parâmetro mínimo a força de trabalho recomendada para TIC.

O quantitativo de força de trabalho do TJRR é apresentado na tabela abaixo:

Tabela I - Quantitativo de força de trabalho

SERVIDORES	QUANTIDADE
EFETIVOS	475
EFETIVOS COMISSIONADOS	176

REQUISITADOS	9
REQUISITADOS COMISSIONADOS	21
COMISSIONADOS	103
ESTAGIARIOS	200
TOTAL	**984**

* Informações prestadas pelo SDGP. Posição em 01.07.2013

Esclarecemos ainda que esse quantitativo é dinamicamente aumentado e deve ser então revisado periodicamente.

Nesse cenário, a Resolução n.º 90/2009 - CNJ sugere a proporção de 5% de servidores na área de TIC para atender ao porte do tribunal, considerando comissionados, terceirizados e efetivos, sendo que, dessa porcentagem pelo menos 35 deve integrar o quadro permanente de TIC.

Tabela II – Força de Trabalho total mínima recomendada para TIC

Total de Usuários de recursos de TIC	% mínimo da força de trabalho de TIC (efetivos, comissionados e terceirizados)	Mínimo necessário de profissionais do quadro permanente
Até 500	7,00%	15
Entre 501 e 1.500	5,00%	35
Entre 1.501 e 3.000	4,00%	75
Entre 3.001 e 5.000	3,00%	120
Entre 5.001 e 10.000	2,00%	150
Acima de 10.000	1,00%	200

FONTE: Anexo I da Resolução n.º 90/2009 - CNJ

Na Organização do Quadro de Pessoal e o Plano de Carreira dos Servidores do Poder Judiciário do Estado, Lei Complementar n.º 142/2009, para a área de TIC tem-se a previsão de 25 analistas de sistemas e 25 técnicos, além de cargos comissionados específicos para a área de TIC.

Atualmente, a Secretaria de Tecnologia da Informação conta com a seguinte estrutura de pessoal:

Tabela III - Quantitativo de força de trabalho da STI

SERVIDORES	**QUANTIDADE**
EFETIVOS	37
EFETIVOS COMISSIONADOS	18
REQUISITADOS COMISSIONADOS	01
COMISSIONADOS	08
ESTAGIARIOS	30
TOTAL	**94**

* Informações prestadas pelo SDGP. Posição em 01.07.2013

O setor de TIC do TJRR possui 94 servidores (ANEXO II), sendo que destes, 55 integram o quadro permanente. Conseqüentemente o quantitativo de recursos humanos está dentro do padrão mínimo recomendável pela Resolução n.º 90/2009 - CNJ.

Isto posto, observa-se que o quantitativo de servidores não compromete a qualidade dos serviços prestados pelo setor nem o alcance das metas definidas no planejamento estratégico. Cabe ressaltar que o setor de TIC pode produzir prévio levantamento da sua deficiência de recursos humanos considerando os demais critérios de que trata a Resolução n.º 90/2009 - CNJ, art. 2º, § 4º.

Critérios

Resolução – CNJ 90/2009, art. 2º, § 4º;

b) Achado I: Ausência de avaliação qualitativa e quantitativa de pessoal

A avaliação formal de adequação do quadro de pessoal do setor de TI é outro ponto a ser ressaltado, visto que uma avaliação do processo de capacidade baseado nos modelos de maturidade do CobiT é fundamental para o aprimoramento da governança de TI, pois através destes, será possível identificar as deficiências em capacidade e a sua demonstração para a alta administração. Planos de ação podem ser desenvolvidos para elevar esses processos ao desejado nível de capacidade do setor.

O item 9.2.2 do Acórdão n.º 1233/2012 - TCU - Plenário, orienta a realização de tais avaliações, sob a espeque de delimitar as necessidades de recursos humanos necessários. Consubstanciado na mesma vertente, o item 39 do Acórdão n.º 1603/2008 – TCU – Plenário, aduz em suma que verificações realizadas freqüentemente servem como ponto de partida, fornecendo subsídios ao direcionamento de ações para não deixar em deságio as necessidades de recursos humanos destes setores que realizam a gestão das atividades de TI da organização.

Pautado nas respostas encaminhadas por meio do Despacho n.º 072/2013_STI/GAB, resta evidenciada a inexistência do respectivo procedimento de avaliação quantitativa e qualitativa freqüente de seu pessoal.

Critérios

Decreto n.º 5.707/2006, art. 1º, inciso III;
Resolução – CNJ n.º 90/2009, art. 2º, § 4º;
Cobit 4.1, PO4.12 – Pessoal de TI.

Efeitos

Risco de defasagem quantitativa e qualitativa no setor de TIC para o fornecimento do devido atendimento das necessidades demandadas pelo Tribunal de Justiça de Roraima.

Proposta de encaminhamento:

Recomendar ao Tribunal de Justiça do Estado de Roraima, em atenção ao previsto na Resolução – CNJ n.º 90/2009, art. 2º, § 4º, e considerando as práticas contidas no Cobit 4.1, PO4.12 - Pessoal de TI, estabeleça a criação de avaliação frequente do quadro quantitativo e qualitativo, intuindo a delimitação das necessidades de recursos humanos demandados para o fiel cumprimento de suas atividades afetas ao órgão.

c) Achado II: Plano anual de capacitação de TIC – deficiências

A definição de capacitar é tornar o profissional habilitado para desempenhar uma função, isto é, qualificar a pessoa para determinado tipo de trabalho. Este ciclo de capacitação ora mencionado torna-se ainda mais imprescindível dentro da área de tecnologia da informação e comunicação onde a evolução tecnológica é extremamente célere.

A Resolução n.º 90/2009 – CNJ, determinou aos Tribunais pertencentes ao Poder Judiciário a elaboração de um Plano Anual de Capacitação na área de TIC, de forma a delimitar a atualização de conhecimentos úteis para desenvolver suas competências. No mesmo sentido frisou o Acórdão n.º 1233/2012 - TCU - Plenário, quando ratificou tal exigência instruindo também a capacitação em governança e gestão de TI.

No âmbito do Tribunal de Justiça de Roraima - TJRR foi publicado na intranet o Plano Anual de Capacitação para o triênio 2012/2014, abrangendo atualização de conhecimentos que promovem aprimoramento para as áreas de governança, sistemas, redes e suporte. Cumpre salientar que embora o plano tenha sido iniciado no ano previsto, 2011, a execução de alguns treinamentos previstos para 2012 atrasaram, sendo efetivados em 2013.

O objetivo 12 do Plano Diretor do TJRR estabeleceu a meta de 100% dos servidores capacitados em no mínimo 20h, percentual a ser atingido gradativamente no quinquênio 2010/2014. Conforme a tabela demonstrada abaixo o percentual mínimo exigido pelo plano diretor somente não foi atingido no ano de 2011, sendo respeitada a meta em 2012 e executados satisfatoriamente em 2013.

Tabela IV - Objetivo Estratégico 12 – Plano Diretor

Servidores	Período de Referência (Ano)		
	2011	2012	2013
Total de Servidores da STI	55	60	64
Total de Servidores da STI Capacitados (20 h/a)	15	48	56
Percentual / Servidores da STI Capacitados (%)	27,27%	80,00%	87,50%

*Informações prestadas pelo SDPG Posição em 2 de julho de 2013

Como analisado na auditoria de Política de Capacitação do TJRR, para cada ação deve ser indicada os resultados que se pretende alcançar, o universo de servidores aos quais se destina e a estimativa de investimentos, a exemplo do § 2º, art. 7º**,** da IN.º 25/09 - CNJ.

O plano de capacitação de profissionais de TI deve auxiliar no desenvolvimento das competências necessárias para a boa execução dos trabalhos. Assim, também foi avaliado se havia planejamento e se neste havia previsão de capacitação em gestão de TI (planejamento, coordenação, supervisão e controle), acórdão n.º 1233/12. Adicionalmente a isso não consta a aprovação do Plano de Capacitação de TIC, embora este já esteja sendo executado.

Critérios

Acórdão n.º 1233/2012 - TCU - Plenário;
Resolução – CNJ n.º 90/2009, art. 3º.
Acórdão n.º 1603/2008 - TCU - Plenário

Causas:

Inobservância da legislação, em especial da Resolução n.º 90/2009 do CNJ.

Efeitos:

Possível execução inócua de capacitações.
Inexecução de capacitações efetivamente pertinentes e necessárias.
Baixa qualidade dos recursos humanos de TI.

Proposta de encaminhamento:

a) Recomendar ao Tribunal de Justiça do Estado de Roraima a adequação do plano de capacitação para que indique os resultados que se pretende alcançar, o universo de servidores aos quais se destina e a estimativa de investimentos, a exemplo do § 2º, art. 7º, da IN. º 25/09.
a) Recomendar ao Tribunal de Justiça do Estado de Roraima, em atenção a Resolução – CNJ n.º 90/2009, art. 3º, proceda a aprovação do respectivo plano de capacitação.

d) Política de fixação de recursos humanos

Por se tratar de um setor estratégico, no corpo de uma instituição, setores de TI devem implementar processos para assegurar força de trabalho apropriada e com habilidades necessárias para atingir os objetivos da organização, aumentando consideravelmente sua eficiência.

Para que o resultado técnico se mantenha, precisa-se assegurar uma baixa rotatividade da equipe, o que poderá ser alcançado com aplicação de políticas de gestão de

pessoas que promova a fixação de recursos humanos nesta área, motivando-os através de planos de carreiras claros e compensatórios.

Adicionalmente, a mencionada fixação repercute de forma positiva inclusive quando aplicada para preservar o ambiente interno do referido setor, evitando ficar à mercê de deliberação da autoridade.

Dentro do Tribunal, formalmente, a Lei Complementar nº 204 de 23 de Janeiro de 2013, corroborando com a idéia de fomentar essa fixação, estabelece com o intuito de vincular os servidores oriundos da área, como uma de suas possíveis lotações a própria Secretaria de Tecnologia da Informação. Fora o critério ora suscitado, é importante ratificar, que muito embora não exista outra política expressamente formalizada para a fixação de servidores no respectivo setor, avaliando a planilha de distribuição dos cargos, nota-se especial cuidado em manter o quadro de servidores da área, com lotação no setor de TIC.

As critérios de progressão, também estabelecidos na Lei supra dita, contribuem para a fixação de servidores dentro do setor. Cuidados com ambiente positivo de trabalho e orientação são questões de cunho avaliativo complexo, e também não há um critério formal explicitado através de norma específica, o que dificulta uma análise objetiva satisfatória do tema.

Critérios:

Resolução – CNJ 90/2009, art. 2, §5º;
Cobit 4.1, PO7.1 – Recrutamento e Retenção de Pessoal;
Acórdão n.º 1603/2008 - TCU - Plenário item 49.3.a.

e) Gestão de Recursos humanos terceirizados

O Conselho Nacional de Justiça, após publicação da Resolução n.º 90/2009 - CNJ, buscou selecionar quadro de pessoal permanente, evitando que ações estratégicas de TI sejam delegadas a pessoal terceirizado em função da ausência de quadro mínimo.

Tal medida pretende ainda evitar que atividades gerenciais, como governança de TIC, gerenciamento de projetos de TIC, análise de negócio, segurança da informação, gerenciamento de infraestrutura, gestão dos serviços terceirizados, sejam delegadas a terceiros. Pois, representa um aumento do risco organizacional, visto que o fato estaria transferindo a inteligência da organização ou de atividades estratégicas por outro mediador. A transferência destes tipos de atividades para contratos firmados é forte indicio de deficiência de gestão.

Importante deixar claro que o mecanismo de terceirização deve ser efetivado somente em fases de execução da atividade, abstendo-se de realizar atividades de

planejamento. Adicionalmente a isso é prudente que a Administração não transfira as tarefas descritas no Plano de Cargos de Salários, a terceiros, conforme salientado no texto abaixo:

> ANALISTA DE SISTEMAS
>
> "(...)
>
> ***1**. Estudar as características e planos dos diversos órgãos do Tribunal de Justiça, estabelecendo contatos com o corpo diretivo para verificar as possibilidades e conveniências da sua informatização; **2**. Fazer estudos sobre a viabilidade e o custo da utilização de sistemas de processamento de dados, bem como, preparar diagramas de fluxo, levando em conta os recursos disponíveis e necessários para submetê-los a uma decisão, elaborando, segundo linguagem apropriada, orientação aos programadores e aos demais envolvidos; **3**. Examinar os dados de entrada disponíveis, estudando as modificações necessárias à sua normalização para determinar os planos e sequências de elaborações de procedimentos de operação; **4**. Estabelecer os métodos e procedimentos possíveis, idealizando-os ou adaptando os já conhecidos, segundo sua economicidade e eficiência, para obter os dados que se prestam ao tratamento em computador; **5**. Verificar o desempenho do sistema proposto, realizando experiências práticas para assegurar-se de sua eficiência e introduzir as modificações necessárias; **6**. Executar atividades correlatas*"
>
> TÉCNICO EM INFORMATICA
>
> "(...)
>
> ***1**. Instalar e operar sistemas computacionais e programas aplicativos, prestando suporte técnico aos usuários; **2**. Promover a distribuição e o acompanhamento preventivo de computadores; **3**. Identificar arquitetura de redes, promovendo a operacionalidade de cabeamentos e conexões; **4**. Fazer criação e editoração eletrônica; **5**. Testar e avaliar programas obedecendo aos projetos pré-definidos, propondo-lhes melhorias em interfaces e funcionalidades; **6**. Executar, sob supervisão e orientação, procedimento de extração e exibição de dados; **7**. Preparar a documentação e material de treinamento para ser utilizado pelos operadores, de forma compatível com os equipamentos; **8**. Organizar os procedimentos de controle de dados de entrada e saída; **9**. Executar atividades correlatas*."

No cenário atual deste Tribunal, não há mão de obra terceirizada alocada no setor de TIC. Outrossim, pautado na resposta encaminhada através do Requerimento de Solicitação/NCI n.º 001/2013, não se vislumbra nenhuma das atividades listadas no § 2º, do art. 2º, da Resolução n.º 90/2009 - CNJ, sendo realizadas por meio de contratos firmados pelo Tribunal de Justiça de Roraima.

Critérios:

Resolução – CNJ 90/2009, art. 2

Acórdão n.º 1603/2008 - TCU - Plenário item 37 e 41

Acórdão n.º 1233/2012 - TCU - Plenário

2 – DA QUALIFICAÇÃO NECESSÁRIA PARA ACESSO ÀS FUNÇÕES DE LIDERANÇA NOS SETORES DE TIC.

a) Achado III: Ausência de critérios gerenciais que defina a forma de acesso às funções de liderança

A qualificação dos profissionais em relação às atividades que deve desempenhar a área de TI dos órgãos/entidades deve ser analisada ao indicar um servidor às funções de liderança. Nesta esteira, como boa pratica deve ser considerado além dos critérios de qualificação técnica, condicionados pela Lei Complementar n.º 204/2013 para investidura em cargo, as competências gerenciais e os resultados produzidos (item 48, do Acórdão n.º 1603/2008).

No caso desta Corte de Justiça, de acordo com a resposta encaminhada pela Secretaria de Tecnologia da Informação, as indicações às funções de liderança são feitas baseadas em critérios de confiança e no requisito legal estabelecido, o qual considera apenas qualificação técnica .

O risco nesse caso é uma baixa qualificação do corpo gerencial de TI e o comprometimento dos resultados da área, desde a falta de alinhamento com os negócios até a perda de produtividade da equipe por má gestão.

Critérios:

Decreto no 5.707/2006, art. n.º 3, incisos VI e VII;
Acórdão n.º 1233/2012 - TCU - Plenário, item 9.4.1;
Acórdão n.º 1603/2008 - TCU - Plenário, item 48.

Causas:

O padrão atualmente exigido pelo CNJ é novidade e ainda não havia sido completamente difundido pelos Tribunais, incluindo este, assim, por não existir um modelo formalizado de critérios para a seleção ora discutida, tal questão não vinha sendo utilizada.

Efeitos:

Impacto negativo na produtividade da equipe de TI em função da baixa qualidade do corpo gerencial.
Falta de alinhamento da TI com o negócio da organização.
Desmotivação dos servidores da área de TIC.

Proposta de encaminhamento:

Deve o Tribunal disciplinar 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, e aperfeiçoar sua atuação, considerando as diretrizes dos Acórdãos n.º 1233/2012 - TCU - Plenário, item 9.4.1 e n.º 1603/2008 - TCU - Plenário, item 48.

Disciplinada a matéria conforme estabelecido no parágrafo acima, esta precisa ser confirmada por comissão formalmente designada observando as regras fixadas por ocasião da assunção de servidores às chefias na área de TIC.

3 – DOS CONTROLES ADOTADOS NO TRIBUNAL PARA MITIGAR RISCOS NA GESTÃO TIC

a) Achado IV: Planejamento Estratégico - Falhas no Plano Estratégico de TI e no PDTI denominado Plano de Trabalho.

Como mencionado na auditoria realizada em 2012 nos contratos de Tecnologia da Informação, o planejamento estratégico de TI é necessário para gerenciar todos os recursos de TI e garantir o seu alinhamento com as prioridades e estratégias de negócio.

A área de TI e as partes interessadas no negócio são responsáveis pela otimização do valor a ser obtido do portfólio de projetos e serviços. O plano estratégico deve melhorar o entendimento das partes interessadas no que diz respeito a oportunidades e limitações da TI, avaliar o desempenho atual e esclarecer o nível de investimento requerido.

A estratégia e as prioridades de negócio devem ser refletidas nos portfólios e executadas por meio de planos táticos de TI que estabeleçam objetivos concisos, tarefas e planos bem definidos e aceitos por ambos, negócio e TI.

Desse modo, o Cobit 4.1 PO1.4 *Strategic Plan* define as boas práticas do Planejamento Estratégico de TI:

> Criar um plano estratégico que defina, em cooperação com as partes interessadas relevantes, como a TI contribuirá com os objetivos estratégicos da organização (metas) e quais os custos e riscos relacionados. Esse plano estratégico deve contemplar **como a TI aplicará os programas de investimentos e como dará sustentação à entrega operacional de serviços**. O plano deve definir como os objetivos serão atingidos e medidos e deve ser formalmente liberado para implementação pelas partes interessadas. O plano estratégico de TI **deve contemplar o orçamento operacional e de investimento, as fontes de recursos financeiros, a estratégia de fornecimento, a estratégia de aquisição e requisitos legais e regulamentares**. O plano estratégico deve ser suficientemente detalhado para possibilitar a definição dos planos táticos de TI. (grifamos)

O planejamento estratégico de TI deve indicar os projetos e serviços de TI que receberão recursos, os custos, as fontes de recursos e as metas a serem alcançadas. Deve ser uma atividade regular e os documentos resultantes devem ser aprovados pela alta administração [Acórdão n.º 1603/2008 – TCU, item 26].

Nos planejamentos formalizados de TI (PETI e Plano de Trabalho) analisados, não há evidências das estratégias de aquisição ou de terceirização, nem a indicação de todos os projetos e serviços que receberão recursos, os custos e riscos relacionados, as metas a serem alcançadas, como a TI aplicará os programas de investimentos, como se dará sustentação à entrega operacional de serviços etc.

Os referidos instrumentos de planejamento foram elaborados em 2009 e não passaram por nenhuma alteração/adequação dos planos de curto e médio prazo no decorrer da execução, sendo que alguns deles encontram-se com os prazos expirados.

Conforme comentários do Gestor na auditoria realizada em abril de 2012, nos meses de junho e julho de 2012 foram solicitadas alterações/adequações dos prazos, custos e equipes, sendo que tais solicitações estão na fase de avaliação do Núcleo de Estatística Gestão Estratégica – NEGE e do Comitê de Planejamento de Tecnologia da Informação, sendo que até a presente data ainda não há aprovação de tais documentos.

O planejamento estratégico de TI é essencial para que as organizações possam identificar e alocar corretamente os recursos da área de TI de acordo com as prioridades institucionais e com os resultados esperados.

Critérios

Resolução n.º 90/2009 - CNJ do Conselho Nacional de Justiça;
Cobit 4.1 PO1.4 - Plano Estratégico de TI;
Acórdão n.º 1603/2008 - TCU, item 26.
Acórdão n.º 1233/2012 - TCU - Plenário item 9.1.2
Portaria n.º 1566/12 - TJRR

Evidências

Plano Estratégico de TIC do TJRR;
Plano de Trabalho (PDTI).
Procedimento Administrativo n.º 3155/2009;

Causa

Inobservância parcial da legislação, em especial da Resolução n.º 90/2009 do CNJ.

Carência de uma ação mais incisiva da Alta administração apoiada pelo comitê de TI nas ações de TIC.

Efeitos potenciais

Suporte ineficaz da área de TI na consecução da missão da organização;

Alocação indevida de recursos de TI por falta de entendimento sobre as prioridades da organização;

Desperdício de recursos decorrente da falta de planejamento na alocação de recursos de TI.

Descontinuidade de projetos de TI

Resultados da TI abaixo do esperado

Dificuldade para obtenção de recursos para a área de TI;

Proposta de encaminhamento:

Recomendar ao Tribunal de Justiça do Estado de Roraima, em atenção ao previsto Resolução n.º 90/2009 do CNJ, art. 11, parágrafo único, que aperfeiçoe seu processo de planejamento estratégico institucional e que seja dada continuidade ao processo de alteração/adequação iniciado pela Gestão em julho de 2012, salientando a necessidade da sistematização do acompanhamento, para que seja mantido o alinhamento com as diretrizes estratégicas institucionais.

b) Achado V: Inexistência de processo de software

Um processo de software é um conjunto de atividades que transformam requisitos de usuários (entrada do processo) em um produto de software. Por oportuno, chamamos a atenção para o fato de que o produto de software não é composto apenas dos programas de computadores, mas inclui outros itens. Destacamos ainda, que os diversos itens que compõem o produto de software são gerados ao longo da execução do processo de software.

Na mesma espreita o Acórdão n.º 1603/2008 - TCU - Plenário explica em síntese que uso de uma metodologia para desenvolvimento de sistemas incorpora conceitos de engenharia de software para tornar o processo de desenvolvimento de sistemas mais controlável, mensurável e eficaz. Com a metodologia, busca-se não só garantir que as várias etapas típicas do desenvolvimento (levantamento, projeto, programação, testes e homologação) sejam executadas de forma sistemática e documentada, mas também permitir a avaliação e melhoria do processo, com vistas à produção de software de qualidade

Segundo Pressman cada uma dessas etapas conta com atividades básicas a serem executadas para atingir o objetivo proposto. Essas atividades integram um conjunto mínimo na obtenção ou produção de um produto de software.

O Acórdão n.º 1233/2012 - TCU - Plenário atenta para a necessidade de formalizar a elaboração de um modelo de processo de software, isto incluso tanto para produção como para a vinculação de seus contratos de desenvolvimento e manutenção de software.

Pautado nas respostas encaminhadas por meio do Despacho n.º 072/2013_STI/GAB, resta evidenciada a inexistência de processo de software no setor de TIC do TJRR.

O achado em comento reitera o apontamento identificado em auditoria anterior, Auditoria Simultânea em contratos de TI – 2012 - Achado VIII. Inexistência de processo de desenvolvimento de software. Assim a conclusão é que, contratos de serviços de desenvolvimento ou manutenção de software, são realizados de forma irregular, em virtude da indefinição do objeto.

Critérios:

Instrução Normativa N.º 04/2008 – SLTI/MPOG, art. 12, II;
Lei 8.666/1993, art. 6º, inciso IX;
Normas NBR ISO/IEC 12.207 e 15.504;
Acórdão n.º 1233/2012 - TCU - Plenário item 9.2.3;
Cobit 4.1 AI2.7.

Causas:

Inobservância das recomendações aludidas pela norma e Acórdãos

Efeitos:

Processo de desenvolvimento de sistemas lento e sistemas de informação ineficazes.
Perda de informações por causa de sistemas pouco robustos, sujeitos a falhas de segurança, seja por fraude, seja por uso incorreto.
Execução de contratos de prestação de serviços de desenvolvimento sem métricas adequadas nem etapas claras com produtos para cada etapa.
Sistemas de difícil manutenção, sem documentação, em que apenas quem desenvolveu detém o conhecimento. Esse caso pode ser ainda mais sério se o desenvolvimento se da por meio de contratos firmados.

Proposta de encaminhamento:

Recomendar ao Tribunal de Justiça do Estado de Roraima, em atenção as determinações dadas pelo Acórdão n.º 1233/2012 - TCU - Plenário item 9.2.3, estabeleça um processo de software com base em NBR ISSO/IEC 12.207 e 15.504, MPS.BR, CMMI ou outro modelo,

com vista a melhorar e padronizar a produção de software desta corte. Adicionalmente abstenha-se de futuras contratações de desenvolvimento de software na ausência de definição de processo de software.

c) Processo de gerenciamento de projetos

Segundo o PMI (Project Management Institute), um projeto é uma reunião de esforços aplicados de forma integrada na busca de um objetivo bem definido, portanto, se gerenciado eficientemente contribuirá para o atingimento de metas da instituição. Então dada sua importância, é imprescindível a utilização de algum dos modelos de processo de gerenciamento de projetos.

Embora observada a relação desse item com o pleno funcionamento da Comissão de Gestão de Tecnologia da Informação e Comunicação, e apesar desta comissão não estar funcionando adequadamente, conforme observado no Achado X, a Secretaria de Tecnologia da Informação do Tribunal de Justiça do Estado de Roraima conta com uma parcela dos seus servidores capacitados em PMBOK - Project Management Body of Knowledge framework, e o adota atualmente como boa pratica para o gerenciamento dos seus projetos em andamento.

Critérios:

Cobit 4.1, processo PO10.2 – Estruturas de Gerência de Projetos;
PMBOK;
Acórdão n.º 1233/2012 - TCU - Plenário item 9.2.5.

d) Achado VI: O processo de gestão de serviços não inclui gestão de configuração e mudança.

O Acórdão n.º 1233/2012 - TCU - Plenário alicerçado pela NBR ISO/IEC 20.000 explica três vertentes para gestão de serviços:

Gestão de configuração – ‘definir e controlar os componentes do serviço e infraestrutura e manter informação precisa da configuração’, processo cuja importância reside em manter uma base de dados de itens de configuração do ambiente de TI, chamada CMDB (Configuration Management DataBase), que é a base para o funcionamento dos demais processos de gestão de serviços;

Gestão de incidentes – ‘restaurar o mais rápido possível os serviços acordados com a organização, ou responder às requisições dos serviços’, ou seja, processo cuja importância está ligada ao fato de que é por meio dele que é restaurado diretamente o fornecimento de serviços dos quais dependem os usuários finais;

Gestão de mudanças – 'assegurar que todas as mudanças sejam avaliadas, aprovadas, implementadas e revisadas de maneira controlada', que é considerado o processo mais crítico no modelo preconizado pelo Cobit 4.1, pois é por meio dele que a consistência dos serviços com continuidade é mantida.

Com relação a gestão de incidentes a administração possui a Seção de Service Desk, a qual é responsável pelo tratamento de incidentes e serviços.

Em sentido contrário, o cenário evidenciado e fundado nas respostas encaminhadas por meio do Despacho n.º 072/2013_STI/GAB, revela a inexistência de qualquer modelo de gestão de configuração e gestão de mudanças embora seja razoável supor a condução de tais conceitos informalmente.

Critérios:

Acórdão n.º 1233/2012 - TCU - Plenário item 9.2.7;
NBR ISO/IEC 20.000;
Cobit 4.1 DS4, DS8, DS9, DS 10, DS13, AI.

Causas:

Inobservância das recomendações aludidas pela norma e Acórdãos.
Inércia da Comissão de Gestão de Tecnologia da Informação e Comunicação.

Efeitos:

Falta de controle na informação das configurações de ativos e infraestrutura.
Risco de descontinuidade de serviços por falta de avaliação de mudanças.
Carência de uma ação mais incisiva da Alta administração apoiada pelo comitê de TI nas ações de TIC.

Proposta de encaminhamento:

Recomendar ao Tribunal de Justiça do Estado de Roraima, que em atenção ao disposto no Acórdão n.º 1233/2012 - TCU - Plenário implante um modelo de gestão de serviços e configuração com vistas a prevenir efeitos supracitados futuramente.

e) Achado VII: sistemas de controle interno inadequados

Os sistemas de controles internos adotados não estão adequadamente estruturados por não abrangerem a integralidade da estrutura administrativa.

O intuito desse item, é assegurar que os objetivos de TI sejam atingidos, visando garantir ainda a conformidade com as leis e os regulamentos relacionados à TI, bem como as

boas praticas relativas aos frameworks de processos. Assim, cabe ao próprio setor monitorar de forma integrada os processos habituais realizados, efetuando um controle interno particular das atividades de TI relacionadas a sua função, intentando identificar ações de melhorias.

O controle supra referido, segundo o Cobit 4.1, inclui o monitoramento e reporte das exceções de controle, dos resultados de autoavaliação e avaliação de terceiros. Feito isto, implemente e monitore ações corretivas com base nas avaliações e nos relatórios de seu controle.

Evidenciou-se a inobservância quanto a implantação integral de alguns dos processos descritos em outros achados desta auditoria, o que configura indicio de deficiência do controle interno administrativo pertencente ao setor.

Critérios:

Acórdão n.º 1233/2012 - TCU - Plenário item 9.13.14;

Decreto-Lei 200/1967, art. 6º, V;

Cobit 4.1 ME2;

Acórdão n.º 1603/2008 - TCU, Achado XXXII. Inexistência de equipe própria para realizar Auditoria de TI.

Causas:

Inobservância das recomendações aludidas pelas boas praticas do Cobit 4.1 ME2 e Acórdãos

Efeitos:

Área de TI com governança imatura, sem controles e indicadores que possam apontar os problemas e oportunidades de negócio para a organização

Proposta de encaminhamento:

Recomendar ao Tribunal de Justiça do Estado de Roraima, em atenção as recomendações aludidas no Cobit 4.1 ME2, implante 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:

a) planejamento estratégico institucional;

b) planejamento estratégico de TI;

c) funcionamento dos comitês de TI;

d) processo orçamentário de TI;

e) processo de software;

f) gerenciamento de projetos;

g) gerenciamento de serviços de TI;
h) segurança da informação;
i) gestão de pessoal de TI;
j) contratação e gestão de soluções de TI; e
k) monitoração do desempenho da TI organizacional.

f) Achado VIII: Inércia da Comissão de Gestão de Tecnologia da Informação e Comunicação

A existência de um comitê diretivo de TI (IT Steering Committee), que determine as prioridades de investimento e alocação de recursos nos diversos projetos e ações de TI, é de fundamental importância para o alinhamento entre as atividades de TI e o negócio da organização, bem como para a otimização dos recursos disponíveis e a redução do desperdício. O fato desse comitê ser composto por dirigentes de TI e de outras áreas da organização possibilita que as decisões de investimentos sejam obtidas a partir de uma visão mais abrangente, o que reduz os riscos de erro. Essa interpretação supracitada pelo Acórdão n.º 1603/2008 - TCU - Plenário também é sucintamente elucidado pelo Cobit 4.1, PO4.3 - Comitê Executivo de TI conforme segue.

Estabelecer um comitê executivo (ou equivalente) composto pelas Diretorias Executiva, Negócios e TI para:

- Determinar prioridades dos programas de investimentos em TI em linha com as estratégias e prioridades do negócio;

- Monitorar o estado atual dos projetos e resolver conflitos de recursos;

- Monitorar níveis de serviço e suas melhorias.

Em resposta ao requerimento de auditoria, não foram realizadas reuniões nos anos de 2011 e 2012, o que evidencia sua inércia, além disso não há deliberações formais de suas decisões. A situação ora mencionada caracteriza ausência de atuação efetiva, comprometendo as ações e investimentos para projetos do setor de TIC, podendo deixar o setor de TIC funcionando meramente a demanda de solicitações.

Critérios:

Instrução Normativa 4/2008 – SLTI/MPOG, art. 4º IV;
Cobit 4.1, PO4.2;
Cobit 4.1, PO4.3;
Resolução – CNJ 90/2009, art. 12;
Acórdão n.º 1233/2012 - TCU - Plenário item 9.2.1;
Acórdão n.º 1603/2008 - TCU - Plenário;

Acórdão n.º 2471/2008 - TCU - Plenário.

Causas:

Inobservância das recomendações aludidas pela norma e Acórdãos.

Ausência de fomento de sua importância a alta gestão.

Carência de uma ação mais incisiva da Alta administração nas ações de TIC.

Efeitos:

Apoio e envolvimento insuficientes da administração nas decisões essenciais da área de TI.

Estratégia de TI não alinhada com a estratégia da organização.

Priorização inadequada das ações de TI devido à ausência da participação das áreas de negócio do Tribunal (atividade jurisdicional).

O setor de TIC funcionando meramente a resoluções de solicitações.

Recomendação:

Recomendar ao Tribunal de Justiça do Estado de Roraima, em atenção ao disposto na Resolução nº 90/2009, do CNJ, art 12, e considerando as diretrizes da Cobit 4.1, PO4.2 – Comitê estratégico de TI e PO4.3 - Comitê diretor de TI, proceda com sua atuação e respectivas atribuições elucidadas.

4 – DOS MECANISMOS DE CONTROLE ADOTADOS PARA GARANTIR A SEGURANÇA DA INFORMAÇÃO

a) Achado IX: inexistência de designação formal de responsável pela segurança da informação

No cenário atual, as organizações tratam a informação considerando-a um ativo, e especificamente, no caso desta Corte de Justiça, este ativo está intimamente ligado ao negocio do órgão devendo ser adequadamente protegido.

No TJRR não ha designação formal dos responsáveis pela segurança da informação. Papéis críticos de segurança da informação, segurança física, processo de segurança da informação associados a cada sistema, ativos e conformidade não tem responsáveis claramente definidos. O Cobit 4.1 PO4.8 instrui a imprescindibilidade de se atribuir atividades ligadas ao negocio a responsáveis, conforme segue:

> "PO4.8 Responsabilidade por Riscos, Segurança e Conformidade Incluir nas funções de negócio a propriedade e a responsabilidade pelos riscos

relacionados a TI a um nível sênior apropriado. Definir e atribuir papéis críticos para o gerenciamento dos riscos de TI, incluindo a responsabilidade específica pela segurança da informação, segurança física e conformidade. Estabelecer responsabilidade no nível organizacional pelo gerenciamento de risco e segurança para questões de nível organizacional. Pode ser preciso atribuir responsabilidades adicionais de gerenciamento de segurança ao nível de um sistema específico para lidar com questões de segurança relacionadas. Obter direcionamento da Diretoria sobre os níveis específicos de risco de TI aceitáveis e aprovação de quaisquer riscos residuais"

Na mesma esteira, a NBR ISO/IEC 27.002, reitera a conveniência de definir claramente as responsabilidades pela segurança da informação de cada ativo, ficando a critério desse a prerrogativa de delegar atividades relacionadas e controlar a execução de tal atividade, no entanto sem isentá-lo da responsabilidade.

Critérios:

NBR ISO/IEC 27.002, item 6.1.3;

Acórdão n.º 1233/2012 - TCU - Plenário, item 9.13.9.1;

Acórdão n.º 2471/2008 - TCU - Plenário, item 10;

Cobit 4.1 PO4.8;

Causas:

Inobservância das recomendações aludidas pela norma e Acórdãos

Carência de uma ação mais incisiva da Alta administração apoiada pelo comitê de TI nas ações de TIC.

Inércia do comitê de segurança da informação.

Efeitos:

Risco de comprometer o regular exercício de determinado ativo.

Plano de continuidade pode tornar-se ineficiente.

Proposta de encaminhamento:

Tendo em vista o disposto no item 6.1.3 da NBR ISO/IEC 27.002 deve o Tribunal estabelecer em nível organizacional a atribuição clara das responsabilidades pela segurança da informação a cada ativo. Analogamente as recomendações de planejamento do Cobit 4.1 PO4.8 podem ser conferidas as responsabilidades ao gerenciamento de segurança a níveis específicos.

b) Achado X: Comitê de segurança – deficiências de atuação

A finalidade do comitê de segurança da informação é elaborar e aprovar a política de segurança da informação, documento primordial que deve ser formulado considerando o seu alinhamento aos objetivos do negocio do órgão, e por fim geri-la. Suas deliberações devem ter comprometimento e colaboração da alta administração, objetivando disseminá-la aos usuários.

É conveniente que sua composição seja formada por representantes de diferentes partes da organização com funções e papeis relevantes. São atividades inerentes ao comitê de segurança da informação de acordo com a NBR ISO/IEC 27.002: "... a promoção da conscientização da segurança da informação, garantir a conformidade das ações em relação às atividades descritas na política de segurança implantada, identificação de ameaças significativas que podem comprometer a exposição de informação da organização, a classificação da informação com base em riscos inerentes...", etc.

No âmbito do Tribunal de Justiça de Roraima – TJRR foi publicada no Diário do Poder Judiciário em 17 de Setembro de 2008 a portaria n.º 840, do dia 16 de setembro de 2008, edição 3927, que resolve constituir tal comitê e disciplinar suas incumbências. Considerando o disposto em tal portaria foi constituída a comissão de segurança da informação na portaria n.º 841, do dia 16 de setembro de 2008, e posteriormente alterada a composição dos seus membros pela portaria n.º 21, do dia 18 de Setembro de 2012, Diário da Justiça Eletrônico, Edição 4877.

Apesar de formalmente constituído, as responsabilidades instruídas nessa composição deveriam já ter sofrido modificações, visto que integrantes da referida portaria já não estão lotados em setores com representatividade que justifiquem a permanência de seus nomes na comissão.

Outrossim, as atas de reuniões de tal comissão datam de 2010, o que comprova a defasagem de sua atuação. Evidencia adicional de sua inércia é a ausência de política de segurança da informação - NBR ISO/IEC 27.002, item 5.1- conforme o **achado XIV**, o que guarda estreita relação com o achado em comento.

Critérios:

NBR ISO/IEC 27.002, item 6.1.2;
Instrução Normativa GSI/PR 1/2008, art.5º, VI;
Acórdão n.º 1233/2012 - TCU - Plenário, item 9.13.9.2
Cobit 4.1 DS5.2.

Causas:

Inobservância da legislação referente a segurança da informação.

Carência de uma ação mais incisiva da Alta administração apoiada pelo comitê de TI nas ações de TIC.

Efeitos:

Ausência de Política de segurança da informação e seus efeitos.

Falta de alinhamento com os objetivos institucionais.

Proposta de encaminhamento::

Recomendar ao TJRR que proceda com o normal funcionamento do comitê de segurança da informação, estude sua composição em atenção às recomendações estabelecidas na NBR ISO/IEC 27.002, item 6.1.2 e proceda com a finalidade do seu objetivo.

c) Achado XI: Inexistência de Processo de Gestão de Riscos

Um processo de gestão de riscos deve documentar a estrutura envolvida em riscos, as estratégias para mitigação dos riscos e os limites acordados com o usuário do serviço. O objetivo desse processo é minimizar o impacto de tais riscos ao negocio da organização.

O processo de gestão de riscos também deve ser periodicamente revisado afim de identificar novos eventos eminentes e atualizar o processo de resposta a cada tipo de risco seja decorrente de fraude ou falha. O Cobit 4.1, processo PO9 suscita os seguintes pontos necessários para elevar a maturidade no assunto:

PO9.1 Alinhamento da gestão de riscos de TI e de Negócios

PO9.2 Estabelecimento do Contexto de Risco

PO9.3 Identificação de Eventos

PO9.4 Avaliação de Risco

PO9.5 Resposta ao Risco

PO9.6 Manutenção e Monitoramento do Plano de Ação de Risco

Em resposta, a STI informa a inexistência formal de processo de gestão de riscos, contudo, é razoável imaginar a existência de parâmetros mínimos estabelecidos mesmo que informalmente, isto posto não isenta a responsabilidade da administração formalizar tal processo.

Critérios:

Instrução Normativa GSI/PR 1/2008, art. 5º, VII;

Norma Complementar 4/IN01/DSIC/GSIPR;

Cobit 4.1, processo PO9 – Avaliar e gerenciar riscos de TI;
NBR 27.005 – Gestão de Riscos de Segurança da Informação;
Acórdão n.º 1233/2012 - TCU - Plenário, item 9.13.9.3.

Causas:

Inobservância das recomendações aludidas pela norma e Acórdãos.
Falta de fomento a alta gestão sobre sua importância.
Inércia do comitê de segurança da informação.
Carência de uma ação mais incisiva da Alta administração apoiada pelo comitê de TI nas ações de TIC.

Efeitos:

Estabelecimento inadequado de prioridades para ações de segurança.
Desperdício de recursos em ações não-prioritárias, enquanto outras mais críticas deixam de ser realizadas.
Eventos eminentes que possam interromper a atividade fim.

Proposta de encaminhamento::
Recomendar ao Tribunal de Justiça do Estado de Roraima, que elabore um processo de gestão de riscos observando as boas praticas elucidadas no Cobit 4.1, processo PO9 e NBR 27.005, objetivando a prevenção de riscos iminente de sua ausência.

d) Achado XII: Inexistência de política de segurança da informação

A política de segurança da informação (PSI) é um documento que normatiza a padronização do tratamento e manipulação das informações de determinada instituição. Seu objetivo é formalizar com base nos requisitos de negocio, os procedimentos a serem adotados na manipulação e gerenciamento da informação.

É importante que a PSI tenha seus objetivos claramente definidos e divulgados dentro da organização. Suas diretrizes devem ser planejadamente revistas a fim de manter a conformidade e eficiência atualizada. A NBR – ISO/IEC 27.002, estipula que a PSI deve definir a segurança da informação e seus objetivos, as responsabilidades a nível organizacional e o comprometimento da alta administração.

De acordo com a resposta encaminhada pelo setor de TIC, através do Despacho n.º 076/2013_STI/GAB, a minuta que tratará sobre a política de segurança da informação, ainda não foi elaborada pela comissão respectiva.

Critérios:

NBR – ISO/IEC 27.002, item 5.1;

Cobit 4.1 DS5.2;

Resolução n.º 90/2009 Art. 13;

Acórdão n.º 1233/2012 - TCU - Plenário, item 9.13.9.4.

Causas:

Inércia do comitê de segurança da informação

TJRR não possui a NBR – ISO/IEC 27.002.

Carência de uma ação mais incisiva da Alta administração apoiada pelo comitê de TI nas ações de TIC.

Efeitos:

Enfraquecimento das ações de segurança, por não serem respaldadas por uma política institucional.

Falta de compromisso ou conscientização com as informações internas por partes dos usuários.

Proposta de encaminhamento::
Recomendar ao TJRR que em atenção a determinação da Resolução n.º 90/2009 Art. 13, elabore e mantenha a política de segurança da informação com base nas instruções descritas na NBR – ISO/IEC 27.002, item 5.1.

e) Processo de elaboração de inventário adequado

O objetivo da realização do inventário dar-se-á pela necessidade dos controles e segurança dos ativos do Tribunal de Justiça do Estado de Roraima. Verifica-se que o processo ocorre à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 7.1

O processo de elaboração de inventário de ativos regem as orientações estabelecidas por meio da Instrução Normativa n.º 001/2009 do Tribunal de Contas do Estado de Roraima, objeto obrigatório na composição da Prestação de Contas Anual.

A partir do exercício de 2013, o TJRR conta com um cronograma de acompanhamento das atividades de gestão patrimonial, pela Seção de Gestão de Bens Móveis, a fim de controlar todos os ativos que compõe a estrutura desta Corte.

Critérios:

IN. 001/2009 - TCERR

f) Achado XIII: Inexistência de processo de classificação da informação

O objetivo do processo de classificação da informação é garantir o tratamento adequado ao grau de sensibilidade e criticidade de determinada informação, dessa forma é prudente determinar a necessidade de tratamento especial dependendo do nível de proteção requerida.

A classificação das informações deve ser identificada levando em consideração o valor, requisitos legais e sensibilidade. Semelhante a NBR ISO/IEC 17799:2005 o Cobit 4.1 PO2.3 orienta a criação de um esquema que detalhe sobre os proprietários dos dados, definição de níveis apropriados de segurança, controle de proteção, uma breve descrição dos requisitos de retenção e destruição dos dados, importância e confidencialidade.

O Acórdão n.º 1603/2008 - TCU - Plenário, em auditoria realizada em diferentes entidades também salientou para a importância de controlar determinada informação com base na sua classificação em todos os meios envolvidos, evitando por exemplo que uma informação física seja tratada de forma diferente quando incluída em sistema.

No TJRR não há processo de classificação da informação definido, embora haja um controle informal das informações providas pelos seus sistemas. A implantação desse processo apesar de oneroso e trabalhoso deve ser fomentado à alta administração devido sua importância.

Critérios:

Cobit 4.1 PO2.3;
NBR ISO/IEC 17799:2005, item 7.2;
Decreto nº 4.553/2002, art. 6º, § 2º, inciso II, e art. 67;
Decreto nº 7.845/2012;
Acórdão n.º 1233/2012 - TCU - Plenário, item 9.15.12.6;

Causas:

Inércia do comitê de segurança da informação
Inobservância das recomendações aludidas pela norma e Acórdãos
Ausência de política de segurança da informação

Efeitos:

Informações tratadas com nível inadequado de proteção, suscetíveis à perda de integridade, confiabilidade e disponibilidade

Tratamento da segurança das informações de maneira inconsistente e dependente do meio em que transitam ou são armazenadas

Falta de amparo para responsabilização por acesso indevido a informações

Proposta de encaminhamento:

Recomendar ao Tribunal de Justiça do Estado de Roraima com fulcro nas orientações contidas na NBR ISO/IEC 17799:2005, item 7.2 que coordenada pela comissão de segurança da informação elabore e mantenha o processo de classificação das informações com vista a classificar o critério de tratamento das informações gerada pela administração.

6 - DO PROCESSO PARA CONTRATAÇÃO E GESTÃO DE SOLUÇÕES DE TIC

a) Achado XIV: Inexistência de Processo formal de trabalho para contratações de TI.

Imperiosa é a constatação premente de um planejamento para aprimorar os processos de contratações de bens e serviços de TI, buscando alavancar a entrega dos resultados almejados, oferecendo serviços de excelência desta importante área à este Tribunal, o que refletirá positivamente na prestação final de seus serviços à sociedade. Além disso, os efeitos desta gestão vão contribuir no sentido de evitar problemas corriqueiros e previsíveis, de maneira consistente e sustentável.

Neste diapasão, resta evidente que para a prestação de tal apoio à gestão do Tribunal, em busca de prosperar na efetividade de seu objetivo final, torna-se indispensável contratações de diversos produtos e serviços relacionados à TI. Contratações essas, que por envolverem recursos públicos de grande monta e esforços integrados de diversas unidades administrativas, devem ser bem concebidas, executadas e gerenciadas, o que significa que carecem de planejamento eficiente.

Atingir a maturidade deste feito requer estrita atenção aos incisos do Artigo 8º, da Instrução Normativa n.º 04/2010 – SLTI/MPOG. Desta forma, conforme recomendação proferida pelo relatório da auditoria realizada em 2012 (P.A. n.º 6769/2012), há que se confeccionar um modelo de processo, promovendo sua implementação mediante orientação normativa, que devidamente cumprida, tende a mitigar os riscos nas contratações de TI.

De outra parte, após a Auditoria nos Contratos de TI. feita em 2012 (P.A. n.º 6769/2012), passou-se a adotar os moldes elencados pela Instrução Normativa n.º 04/2010, da Secretaria de Logística e Tecnologia da Informação - SLTI do Ministério do Planejamento, Orçamento e Gestão - MPOG.

Cumpre salientar, no entanto, que a recomendação aferida no Procedimento Administrativo suscitado no parágrafo suso, mesmo após corrido um ano, ainda não se

concretizou, estando seu processo de confecção em tramitação através do Procedimento Administrativo n.º 6430/2012.

Critérios:

Cobit 4.1 AI5.1 - Procurement Control (Controle sobre aquisições);

Acórdão n.º 1603/2008 - TCU - Plenário;

Acórdão n.º 2471/2008 - TCU - Plenário;

Acórdão n.º 111/2011- TCU - 2° Câmara;

Acórdão n.º 525/2008 - TCU - Plenário;

Resolução n.º 90/2009 do Conselho Nacional de Justiça.

Causas:

Inobservância das recomendações aludidas pelas normas, Acórdãos e Auditoria realizada no ano de 2012 (P.A. n.º 6769/2012).

Efeitos:

Não ha efeito pratico, visto que na falta da normatização especifica, vem sendo usada alternativamente a da I.N. n.º 04/2010 – SLTI/MPOG.

Proposta de encaminhamento:

Reiterar recomendação manifestada no P.A. n.º 6769/20, para que o Tribunal de Justiça do Estado de Roraima institua processo formal de trabalho para contratação de bens e serviços de TI, a exemplo da Instrução Normativa n.º 04/2010 - SLTI/MPOG, para orientar os gestores a conduzirem as contratações com base em procedimentos e controles pré-definidos, que reduzem significativamente o risco de afronta aos princípios e estatutos legais que norteiam as contratações públicas.

V. CONCLUSÃO DA AUDITORIA

Diante dos trabalhos desenvolvidos na presente auditoria foram identificados 14 (quatorze) achados:

1– Da gestão de recursos humanos de TIC.

Achado I: Ausência da avaliação qualitativa e quantitativa de pessoal

Achado II: Plano anual de capacitação não aprovado

2 – Da qualificação necessária para acesso às funções de liderança nos setores de TIC.

Achado III: Ausência de critérios gerenciais que defina a forma de acesso às funções de liderança.

3 – Dos controles adotados no Tribunal para mitigar riscos na gestão TIC

Achado IV: Planejamento Estratégico - Falhas no Plano Estratégico de TI e no PDTI denominado Plano de Trabalho.

Achado V: Inexistência de processo de software

Achado VI: O processo de gestão de serviços não inclui gestão de configuração e mudança.

Achado VII: Os sistemas de controles internos adotados não estão adequadamente estruturados por não abrangerem a integralidade da estrutura administrativa.

Achado VIII: Inércia da Comissão de Gestão de Tecnologia da Informação e Comunicação

4 – Dos mecanismos de controle adotados para garantir a segurança da informação.

Achado IX: Inexistência de designação forma de responsável pela segurança da informação

Achado X: Comitê de segurança – deficiências de atuação

Achado XI: Inexistência de Processo de Gestão de Riscos

Achado XII: Inexistência de política de segurança da informação

Achado XIII: Inexistência de processo de classificação da informação

6 - Do processo para contratação e gestão de soluções de TIC?

Achado XIV: Inexistência de Processo formal de trabalho para contratações de TI.

Foi realizada a reunião de apresentação dos resultados da auditoria em 14/08/2013 na sala do Núcleo de Controle Interno, rito formal da Resolução n.º 171/2013, com representantes dos setores envolvidos e da participação da Presidente, Des. Tânia Dias, e do Juiz Auxiliar da Presidência, Dr. Breno Coutinho.

Conclui-se ao final da auditoria, que muitos dos pontos a serem trabalhados nos **achados** identificados, se devem ao atraso no implemento de metas estabelecidas, conseqüência de um interstício na interação entre a Alta Administração e a Secretaria de Tecnologia da Informação. Ou seja, vislumbra-se a carência de uma ação mais incisiva da Alta Administração apoiada pelo comitê de TI nas ações de TIC.

Constata-se uma defasagem hoje no setor de TIC, o que pode estar sendo causado por planejamento precário e/ou limitação orçamentária a contento para o setor, o que traz riscos à área fim do tribunal e à segurança de informações, caso não sejam corrigidos.

As lacunas a serem desenvolvidas, portanto, podem estar ligadas a um grau de deficiência em planejamentos por parte do setor, e um comprometimento mais intenso da Alta Administração com a missão do setor, para que este se mantenha sempre à frente das necessidades prementes do Tribunal.

Boa Vista, 14 de agosto de 2013.

Maria Josiane Prado	**Ediel Pessoa**	**Osmar Malucelli Filho**
Coord. do Núcleo de Controle Interno	Analista de Sistemas	Assessor Jurídico
Supervisora	Coordenador	Membro