Matriz de Procedimentos

Gestão de Tecnologia da Informação

Questão de auditoria	Informações Requeridas	Fontes de Informação	Procedimentos	Possíveis achados:
1 – A gestão de recursos humanos de TIC atua segundo as normas e boas práticas?	• Avaliação quantitativa e qualitativa do pessoal do setor de TI; • Informações dos Departamentos Pessoais e TIC; • Documento que formalizou a política de capacitação de servidores em TIC;	• Acórdão TCU n. 1233 – Plenário. • Resolução CNJ n. 90/2009;	1. Verificar se a lotação atual de servidores na área de TIC atende ao quantitativo mínimo fixado no Anexo I da Resolução CNJ nº 90/2009. (A referida resolução estabeleceu que o quantitativo de servidores na área de TIC deve ser com base no 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); 2. Verificar a frequência com que é feita a avaliação quantitativa e qualitativa do pessoal do setor de TIC, de forma a delimitar as necessidades de recursos humanos na área de TIC do tribunal/conselho; 3. Verificar se o tribunal/conselho aprovou plano anual de capacitação na área de TIC e em que exercício houve a implantação do citado plano e se este foi integralmente implantado em 2011 e 2012; 4. Verificar se o índice de servidores capacitados é considerado satisfatório. (considera-se satisfatório o percentual mínimo de 70% de servidores capacitados em 2011 e 2012); 5. Verificar se o tribunal/conselho tem programa de capacitação em governança e em atualização em tecnologia da informação; 6. Verificar se após a Resolução CNJ nº 90/2009 houve a substituição da mão de obra, alocada no tribunal/conselho por força de contratos, cujas atividades exercidas tenham compatibilidade com as previstas no Plano de Cargos e Salários dos servidores;	• A lotação de servidores é inferior à definida na Resolução CNJ nº 90/2009, o que pode comprometer a qualidade mínima dos serviços na área de TIC; • Ausência de avaliação quantitativa e qualitativa do pessoal da área de TIC, o que pode caracterizar desatualização da demanda de pessoal de TIC; • Ausência do Plano Anual de Capacitação, o que pode pouco investimento do tribunal/conselho em ações de capacitação dos servidores da área de TIC; • O quantitativo de servidores capacitados em percentual inferior a 70% pode caracterizar falta de oferta regular de cursos de capacitação e pouco investimento por parte do tribunal/conselho; • Ausência de capacitação em governança e atualização em tecnologia da informação pode comprometer as atividades do tribunal/conselho pelo fato de os servidores não estarem atualizados com as tecnologias existentes no mercado; • Excesso de profissionais alocados na execução de contratos, cujas atividades apresentam compatibilidade com aquelas de servidores; • Demanda de serviços de TIC incompatível com o quadro de pessoal permanente;

			7. Verificar qual o percentual entre servidores do quadro e profissionais alocados por empresas contratadas pelo tribunal/conselho. 8. Verificar se o quadro atual de servidores na área de TIC é compatível com a demanda e o porte do Tribunal, com base nos critérios estabelecidos no § 4º do art. 2º da Resolução CNJ nº 90/2009; 9. Verificar se existe política para fixação de recursos humanos na área de TIC; 10. Verificar se algumas das atividades a seguir listadas estão sendo realizadas por meio de contratos firmados pelo tribunal/conselho: governança de TIC, gerenciamento de projetos de TIC, análise de negócio, segurança da informação, gerenciamento de infraestrutura, gestão dos serviços terceirizados de TIC (§ 2º do art. 2º da Resolução CNJ nº 90/2009).	• A não implantação de política para fixação de recursos humanos na área de TIC pode comprometer as atividades de TIC, a qual poderá ficar à mercê da deliberação da autoridade; • Realização de atividades por empresas contratadas quando deveriam ser feitas exclusivamente por servidores do quadro de TIC do tribunal/conselho.
2 – Existem controles que garantam a qualificação necessária para acesso às funções de liderança nos setores de TIC?	• Formas de acesso às funções de liderança nos setores de TIC, considerando as competências multidisciplinares necessárias para estas funções, que incluem, mas não se limitam a conhecimentos em TI	• Boletins internos • Diário Oficial • Acórdão TCU n. 1233 – Plenário.	1. Verificar se o tribunal/conselho regulamentou a forma de acesso às funções de liderança na área de TIC; 2. Verificar se nos critérios utilizados para seleção dos líderes da área de TIC são levadas em consideração as competências multidisciplinares necessárias para estas funções ou se limitam-se aos conhecimentos em TIC; 3. Verificar se os critérios estabelecidos são obedecidos e confirmados por comissão formalmente designada para observar as regras fixadas por ocasião da assunção de servidores às chefias na área de TIC;	• Ausência de norma que defina a forma de acesso às funções de liderança, o que pode comprometer a qualidade das indicações e nomeações de lideranças na área de TIC; • Ausência de critérios fundamentados para seleção dos líderes, o que pode desmotivar os servidores da área de TIC; • Seleção de líderes limitada ao conhecimento de TIC, sem levar em conta outras competências multidisciplinares; • Falta de comprovação do atendimento aos requisitos estabelecidos;
3 – Existem controles adotados no Tribunal para mitigar riscos na gestão TIC?	• Processo de *software;* • Processo de gerenciamento de projetos; • Processo de gestão;	• Boas práticas; • Acórdão TCU n. 1233 – Plenário. • Lei 8.666/1993, art. 6º, inciso IX	1. Verificar se o tribunal/conselho tem Planejamento Estratégico de TIC, alinhado às diretrizes estratégicas institucionais e nacionais; 2. Verificar se o tribunal/conselho tem Plano Diretor de Tecnologia da Informação e Comunicação (PDTI); 3. Verificar se existe processo de *software* definido e se foi estabelecido com base em NBR ISSO/IEC 12.207 e 15.504, MPS.BR, CMMI ou outro; 4. Verificar se o tribunal/conselho tem processo de gerenciamento de projetos; 5. Verificar se os contratos de serviços de desenvolvimento ou manutenção de *software* estão vinculados a um processo de *software*; 6. Verificar se existe modelo de processo de gestão de serviços;	• Ausência de alinhamento entre o planejamento estratégico institucional e nacional e o de TIC; • Ausência de PDTI • Ausência de processo de *software* definido na organização; • Ausência de modelo de gerenciamento de projetos; • Os contratos de serviços de desenvolvimento ou manutenção de *software* não estão vinculados a um processo de *software*, ou esta vinculação não é suficiente; • Ausência de processo de gestão de serviços; • O processo de gestão de serviços não inclui gestão de configuração, de incidentes e de mudança;

			7. Verificar se o processo de gestão de serviços inclui, pelo menos: gestão de configuração, gestão de incidentes e gestão de mudança; 8. Verificar se existe estrutura de controles internos com definição de atividades de controle para mitigar riscos 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. 9. Verificar se o tribunal/conselho tem comitê ou comissão responsável por orientar as ações e investimentos de TIC, conforme exigência constante no art. 12 da Resolução CNJ nº 90/2009.	• Os sistemas de controles internos adotados não estão adequadamente estruturados por não abrangerem a integralidade da estrutura administrativa; • A elaboração do sistema e sua forma de atuação não consideram os processos mais relevantes apontados; • Ausência de comitê ou comissão para orientar as ações e investimentos de TIC.
4 – Os mecanismos de controle adotados para garantir a segurança da informação são eficientes?	• Portarias de nomeação dos responsáveis pela segurança da informação;	• Boletins internos • Normativos internos • Resolução CNJ n. 90/2009; • NBR ISO/IEC 27.002; • NBR ISO/IEC 27.002; • NBR ISO/IEC 27005; • Decreto n. 4.553/2002, art. 6º, § 2º, inciso II, e art. 67	1. Verificar se existe nomeação de responsável pela segurança da informação no tribunal/conselho, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 6.1.3; 2. Verificar se existe comitê instituído pelo tribunal/conselho para coordenar os assuntos de segurança da informação, à semelhança das orientações contidas na NBR ISSO/IEC 27.002, item 6.1.2; 3. Verificar se existe instituído no tribunal/conselho processo de gestão de riscos de segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27005; 4. Verificar se existe instituída no tribunal/conselho política de segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 5.1; 5. Verificar se existe instituído no tribunal/conselho processo de elaboração de inventário de ativos, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 7.1; 6. Verificar se existe instituído no tribunal/conselho processo de classificação da informação, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 7.2 Decreto n. 4.553/2002, art. 6º, § 2º, inciso II, e art. 67.	• Ausência de servidor responsável formalmente pela segurança da informação do Tribunal; • Não foi criado comitê/comissão para coordenar os assuntos de segurança da informação ou este não atua como desejado; • Não existe processo de gestão de riscos de segurança da informação ou este não é eficiente para coibir os riscos existentes; • Não existe política de segurança da informação, ou esta não é eficiente para coibir os riscos existentes; • Não existe processo de elaboração de inventário de ativos, ou este não é obedecido (falta de regularidade ou formalidades estabelecidas); • Não existe processo de classificação da informação, ou é insuficiente para regulamentar a realidade, ou este não é obedecido (níveis de acesso inadequados); • A não implantação das metas de segurança pode caracterizar descumprimento às metas de nivelamento impostas pelo CNJ na Resolução

				n. 90/2009;
5 – Regularidade das doações dos bens de TIC, recebidas do CNJ.	• Inventário total dos bens doados; • Relatório das doações recebidas entre 2010 e 2012;	• Boletins internos • Normativos internos • Processos Administrativos • Termo de Doação e Termo de Cooperação.	1. Realizar inventário dos bens doados pelo CNJ, por exercício, de 2010 a 2012, mediante a seguinte diferenciação: a) bens em funcionamento; b) bens momentaneamente sem utilização, mas recuperáveis; c) bens sem utilização e irrecuperáveis; d) bens sem utilização e considerados ociosos; e) bens não localizados. 2. Verificar se foram observadas todas as formalidades cabíveis para o recebimento das doações no exercício de 2012/2013; 3. Verificar se foram adotadas as providências cabíveis para a localização destes e a apuração das responsabilidades (PAD, TCE e etc.) nos casos de não localização; 4. Verificar se os bens recebidos foram definitivamente incorporados ao patrimônio do Tribunal mediante registro contábil; 5. Verificar se os controles adotados pela área de patrimônio são eficientes. 6. Verificar se o sistema de patrimônio possibilita a correta e fácil localização dos bens; 5. Verificar se os bens doados pelo CNJ obedecem às finalidades estipuladas nos termos de doação para o seu uso, bem como à localização a que se destinaram;	• Não foram observadas todas as formalidades cabíveis para o recebimento das doações; • Não foram adotadas providências cabíveis para a localização destes e apuração das responsabilidades (PAD, TCE e etc.) nos casos de não localização; • Os bens recebidos não foram definitivamente incorporados ao patrimônio do Tribunal; • O sistema de patrimônio adotado não possibilita a fácil localização dos bens; • Os bens doados não obedecem às finalidades estipuladas nos termos de doação para o seu uso e localização; • Não foram adotadas providências para a regularização da situação; • Identificação de bens não localizados doados pelo CNJ em 2010 a 2012;
6. – Existe processo para contratação e gestão de soluções de TIC?	• Processo para contratação e gestão de soluções de TIC .	• Boletins internos • Normativos internos; • Acórdão 786/2006-TCU-Plenário;	1. Verificar se existe processo para contratação e gestão de soluções de TIC; 2. Verificar se o modelo adotado segue os moldes da IN – SLTI/MP 4/2010; 3. Verificar se na hipótese de inexistência de processo formal de contratação, adota-se, alternativamente a IN – SLTI/MP 4/2010;	• Não existe modelo de processo para contratação e gestão de soluções de TIC ajustado às boas práticas; • O modelo adotado não segue os moldes da IN – SLTI/MP 4/2010;