# SUMÁRIO EXECUTIVO

## Ações Coordenadas de Auditoria CNJ 2018

## Sistema de Governança da Tecnologia da Informação

Documento de Referência: Relatório de Auditoria n. 5/2018 (0515934).

Conclusão: Em face da avaliação e dos exames realizados, conclui-se que o TRE/MS apresenta baixa maturidade da governança de TI, vez que não estabeleceu alguns dos processos e políticas recomendados para uma boa governança corporativa de TI.

Achados: Foram encontrados 33 achados de auditoria, posteriormente reduzidos a 30, em razão do atendimento de algumas propostas de encaminhamento até a conclusão do relatório final. Os achados estão relacionados abaixo e encontram-se descritos de forma completa no Relatório de Auditoria n. 5/2018.

**A1 – Ausência de diretrizes formais para planejamento de TI, gestão do portfólio de projetos e de serviços de TI, contratação de bens e serviços de TI e avaliação do desempenho dos serviços de TI.**

Situação encontrada: Não existe política formal instituída para planejamento de TI; gestão do portfólio de projetos e de serviços de TI; contratação de bens e serviços de TI; avaliação do desempenho dos serviços de TI.

Proposta de Encaminhamento: Instituir política formal para as seguintes áreas: a) Planejamento de TI; b) Gestão do portfólio de projetos e de serviços de TI; c) Contratação de bens e serviços de TI; e d) Avaliação do desempenho dos serviços de TI.

**A2 – Ausência de política de gestão de riscos de TI.**

Situação encontrada: Inexistência de política de gestão de riscos de TI definida para o TRE/MS.

Proposta de Encaminhamento: Instituir política de gestão de riscos de TI que contemple a definição de papéis e responsabilidades e sua comunicação formal; níveis de risco aceitáveis; e que as tomadas de decisões estratégicas considerem os níveis de risco de TI definidos.

**A3 – Ausência de incentivos para desenvolvimento e retenção de pessoal de TI.**

Situação encontrada: Inexistência de política formal para a gestão de pessoal de TI, para a avaliação e incentivo ao desempenho de gestores e técnicos de TI e para a escolha dos líderes de TI.

Proposta de Encaminhamento: Instituir políticas formais para: a) Gestão de pessoas, de forma a promover o desenvolvimento de competências e a retenção de gestores e técnicos de TI; b) Avaliação e incentivo ao

desempenho de gestores e técnicos de TI; c) Escolha dos líderes da área de TI, ocupantes de cargos de chefia e de assessoramento.

**A4 – Ausência de comunicação com partes interessadas sobre os resultados de TI.**

Situação encontrada: Inexistência de diretrizes formais para comunicação dos resultados da gestão e do uso de TI para as partes interessadas (públicos interno e externo).

Proposta de Encaminhamento: Instituir diretrizes formais para comunicação com as partes interessadas, considerando os públicos interno e externo, sobre os resultados da gestão e do uso de TI que contemple: a) Divulgação; b) Conteúdo; c) Frequência; e d) Formato das comunicações.

**A5 – Ausência de avaliação da governança e/ou gestão de TI.**

Situação encontrada: Inexistência de diretrizes para avaliação da governança e da gestão de TI.

Proposta de Encaminhamento: Instituir diretrizes para avaliação da governança e da gestão de TI, com realização de avaliações periódicas de: a) Governança e gestão de TI; b) Sistemas de informação; c) Segurança da informação; e d) Contratos de TI.

**A6 – Ausência de políticas de controle de acesso aos recursos de TI.**

Situação encontrada: Inexistência de política formal para o controle de acesso à informação e aos recursos e serviços de TI.

Proposta de Encaminhamento: Instituir política formal de controle de acesso à informação, aos recursos e serviços de TI.

**A7 – Ausência de políticas de cópia de segurança (backup).**

Situação encontrada: Inexistência de política formal para a realização de cópias de segurança (backup).

Proposta de Encaminhamento: Instituir política formal para a realização de cópias de segurança (backup).

**A8 – Ausência de acompanhamento e revisão do Plano Estratégico de Tecnologia da Informação e Comunicação (PETIC).**

Situação encontrada: Embora exista PETIC vigente, ele não é acompanhado e revisado periodicamente e a proposta orçamentária de TI não é feita com base nos objetivos estratégicos nele definidos.

Proposta de Encaminhamento: Efetuar o efetivo acompanhamento da execução do PETIC, conforme determinado no artigo 2º, da Resolução TRE/MS n. 557/2016; promover sua revisão periódica e considerar o PETIC para fundamentar as propostas orçamentárias de TI para os exercícios 2020 e seguintes.

**A9 – Ausência de Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC).**

Situação encontrada: O Plano Diretor de Tecnologia da Informação do TRE/MS (0109348) está vencido e não há previsão de elaboração do próximo.

Proposta de Encaminhamento: Instituir formalmente Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) que: a) Contemple as ações a serem desenvolvidas com vinculação às estratégias institucional e nacional do Poder Judiciário; b) Vincule as ações e projetos a indicadores e metas de negócio; c) Cuja execução seja periodicamente acompanhada; e d) Haja revisão periódica.

**A10 – Ausência de definição das competências necessárias para o pessoal de TI.**

Situação encontrada: Não há definição de quais são as competências necessárias para o pessoal de TI.

Proposta de Encaminhamento: Definir as competências necessárias para o pessoal de TI executar suas atividades e apresentar relação à Secretaria de Gestão de Pessoas (SGP), para que tal definição seja considerada no projeto de Gestão por Competências.

**A11 – Ausência de Plano Anual de Capacitação para o pessoal de TI (PAC-TI) e de acompanhamento dos resultados do PAC-TI.**

Situação encontrada: Inexistência de Plano Anual de Capacitação para o pessoal de TI vigente e com revisão periódica.

Proposta de Encaminhamento: Apresentar minuta de Plano Anual de Capacitação para o pessoal de TI à SGP que contemple: a) Previsão para sua revisão periódica; b) Diretrizes para avaliação e atendimento aos pedidos de capacitação em TI; c) Desenvolvimento de competências em governança e gestão de TI; d) Desenvolvimento de competências em contratação de bens e serviços de TI e em gestão de contratos de TI; e) Previsão para acompanhamento da execução do Plano, inclusive dos objetivos e resultados esperados.

**A12 – Ausência de acompanhamento do desempenho do pessoal de TI.**

Situação encontrada: Inexistência de avaliação de desempenho específica para o pessoal de TI.

Proposta de Encaminhamento: Estabelecer metas de desempenho para o pessoal de TI e acompanhá-las periodicamente.

**A13 – Ausência de previsão dos quantitativos ideais da força de trabalho de TI.**

Situação encontrada: Não há previsão do quantitativo ideal da força de trabalho de TI.

Proposta de Encaminhamento: Apresentar à SGP os quantitativos ideais de força de trabalho de TI, estimados com base: a) Em estudo técnico que indique o número de usuários internos e externos de recursos de TI; e b) No anexo da Resolução CNJ n. 211/2015.

**A14 – Ausência de processos de gestão de serviços formalmente instituídos.**

Situação encontrada: Não há processos de gerenciamento formalmente instituídos no âmbito do TRE/MS.

Proposta de Encaminhamento: Instituir processos de gerenciamento de: a) Portfólio de serviços; b) Catálogo de serviços; c) Continuidade dos serviços de TI; d) Mudanças; e) Configuração e de ativos; f) Liberação e implantação; g) Incidentes; h) Eventos; i) Problemas; e j) Acesso.

**A15 – Ausência de Plano de Continuidade de serviços essenciais de TI.**

Situação encontrada: Inexistência de Plano de Continuidade de Serviços Essenciais de TI.

Proposta de Encaminhamento: Instituir e aplicar Plano de Continuidade de Serviços Essenciais de TI.

**A16 – Ausência de Acordos de Níveis de Serviço (ANS) e de gerenciamento dos níveis de serviço.**

Situação encontrada: Inexistência de catálogo de serviços e TI, com níveis de serviço entre a área de TI e as áreas clientes.

Proposta de Encaminhamento: Instituir catálogo de serviços de TI com os níveis de serviço entre a área de TI e as áreas clientes formalmente definidos (Acordo de Nível de Serviço – ANS) e que: a) Os ANS incluam indicador de grau de satisfação dos usuários; b) Os níveis de serviço definidos sejam monitorados; c) Previsão de ações corretivas para as situações de não alcance dos níveis definidos; d) Comunicação periódica às áreas clientes dos resultados do monitoramento.

**A17 – Ausência de processos de gestão de riscos de TI.**

Situação encontrada: Inexistência de processo formalmente instituído de gestão de riscos de TI.

Proposta de Encaminhamento: Instituir processo de gestão de riscos de TI, em que os riscos de TI dos processos críticos de negócio sejam: a) Identificados; b) Avaliados; e c) Tratados com base em plano de tratamento de riscos.

**A18 – Ausência de Comitê Gestor de Segurança da Informação.**

Situação encontrada: Inexistência de Comitê Gestor de Segurança da Informação formalmente instituído no TRE/MS.

Observação: Comitê Gestor de Segurança da Informação constituído pela Portaria Presidência n. 170/2018, publicada no DJE/MS n. 2002, de 18.7.2018, pág. 2/3, e Gestor de Segurança da Informação no TRE/MS designado pela Portaria Presidência n. 178/2018, publicada na mesma edição do DJE/MS, pág. 3.

**A19 – Ausência de política de segurança da informação.**

Situação encontrada: Inexistência de Política de Segurança da Informação (PSI) formalmente instituída para o TRE/MS.

Observação: Adoção da PSI do TSE pela Resolução TRE/MS n. 616/2018, publicada no DJE/MS n. 1958, de 11.5.2018, pág. 12.

**A20 – Ausência de processos de gestão da segurança da informação.**

Situação encontrada: Inexistência de processos de gestão da segurança da informação formalmente instituídos.

Proposta de Encaminhamento: Instituir processos de gestão da segurança da informação que englobem: a) Classificação e tratamento de informações, com controles que garantam a proteção adequada ao grau de confidencialidade de cada classe de informação; b) Riscos; c) Vulnerabilidades técnicas de TI; d) Monitoramento do uso dos recursos de TI; e e) Incidentes de segurança da informação.

**A21 – Ausência de Equipe de Resposta a Incidentes de Segurança em Redes Computacionais (ETIR).**

Situação encontrada: Inexistência de ETIR instituída no TRE/MS.

Observação: ETIR criada pela Portaria Presidência n. 206/2018, publicada no DJE/MS n. 2021, de 14.8.2018, pág. 3/6.

**A22 – Ausência de ações de conscientização dos colaboradores quanto à segurança da informação.**

Situação encontrada: Não são realizadas ações de sensibilização, conscientização e capacitação em segurança da informação para os agentes públicos do TRE/MS.

Proposta de Encaminhamento: Realizar, periodicamente, ações de conscientização, educação (capacitação) e treinamento em segurança da informação para os agentes públicos do TRE/MS. Para tal fim, entende-se como agente público, "todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função no TRE/MS."

**A23 – Ausência de processo de software instituído.**

Situação encontrada: Inexistência de processo de software formalmente instituído.

Proposta de Encaminhamento: Instituir processo de software que seja: a) Acompanhado por meio de mensurações, com indicadores quantitativos e metas; b) Periodicamente revisado; e c) Gerenciado por pessoal próprio e capacitado.

**A24 – Ausência de gerenciamento do portfólio de projetos de TI.**

Situação encontrada: Inexistência de processo de gerenciamento do portfólio de projetos de TI.

Proposta de Encaminhamento: Instituir formalmente processo de gerenciamento de portfólio de projetos de TI.

**A25 – Ausência de acompanhamento no processo de gerenciamento de projetos de TI.**

Situação encontrada: Não há acompanhamento no gerenciamento de projetos de TI.

Proposta de Encaminhamento: Acompanhar, por meio de mensurações, o gerenciamento de projetos de TI e revisá-lo periodicamente.

**A26 – Ausência de Plano de Contratações de TI.**

Situação encontrada: Inexistência de plano de contratações de soluções de tecnologia da informação e comunicação formalmente instituído.

Proposta de Encaminhamento: Instituir plano de contratações de soluções de tecnologia da informação e comunicação que: a) Inclua as contratações necessárias ao alcance dos objetivos estabelecidos nos planejamentos estratégicos e institucional de TI; b) Seja revisado periodicamente para incluir novas contratações pretendidas; e c) Contenha prazos de entrega dos Estudos Preliminares e dos Projetos Básicos ou Termos de Referência.

**A27 – Ausência de medição dos resultados dos objetivos estratégicos.**

Situação encontrada: Inexistência de monitoramento, com medições periódicas e revisões, nos objetivos estratégicos e táticos de TI.

Proposta de Encaminhamento: Monitorar, com medições periódicas e revisões, os objetivos estratégicos e táticos de TI que constam no PETIC e no PDTIC.

**A28 – Ausência de divulgação dos resultados dos objetivos, das ações e dos projetos de TI.**

Situação encontrada: Os resultados dos objetivos, das ações e dos projetos de TI não são divulgados.

Proposta de Encaminhamento: Divulgar informações sobre os resultados dos objetivos de TI e o acompanhamento das ações e projetos de TI que constam no PETIC e PDTIC.

**A29 – Ausência de medição do grau de alcance dos objetivos e benefícios esperados nos projetos de TI.**

Situação encontrada: Não há medição do grau de alcance dos objetivos e benefícios que justificaram a abertura de projetos de TI.

Proposta de Encaminhamento: Implementar medição do grau de alcance dos objetivos e benefícios que justificam a abertura de projetos de TI e verificar se os resultados são satisfatórios.

**A30 – Ausência de estimativa orçamentária nos projetos de TI.**

Situação encontrada: Os projetos de TI não possuem orçamento estimado.

Proposta de Encaminhamento: Estimar o orçamento dos projetos de TI no início e acompanhá-lo durante a sua execução, verificando se há diferenças significativas entre a estimativa inicial e o valor real obtido ao final e levantar os motivos para as eventuais diferenças significativas encontradas.

**A31 – Ausência de avaliação periódica da efetiva utilização dos sistemas informatizados que suportam o negócio.**

Situação encontrada: Não existe levantamento dos processos críticos que dependam de sistemas de TI.

Proposta de Encaminhamento: a) Implementar verificação se os processos críticos de negócio são suportados por sistemas informatizados; b) Designar formalmente os responsáveis da área de negócio para a gestão dos respectivos sistemas informatizados; c) Implementar avaliação periódica da efetiva utilização dos sistemas informatizados que suportam o negócio.

**A32 – Implantação incompleta das ações previstas para os Grupos 1 e 2 do Plano de Trabalho a que se refere o art. 29 da Resolução CNJ n. 211/2015.**

Situação encontrada: Não foram implementadas todas as iniciativas programadas no Plano de Trabalho previsto no art. 29 da Resolução CNJ n. 211/2015.

Proposta de Encaminhamento: Implementar todas as ações programadas e constantes do Plano de Trabalho 0456374 em relação aos Grupos 1 e 2, conforme especificado no § 1º do art. 29 da Resolução CNJ n. 211/2015.

**A33 – Falhas na atuação da unidade de Auditoria Interna.**

Situação encontrada: Ausência de exames de auditoria para aferir o estágio de Governança de Gestão de TIC no TRE/MS.

Proposta de Encaminhamento: Recomenda-se à Administração do TRE/MS que lote ao menos um servidor da área de TIC na Auditoria Interna, a fim de viabilizar que a unidade elabore o Plano Anual de Auditoria considerando os diversos riscos de TIC aos quais o Regional está exposto e insira a execução de exames de auditoria nos controles de governança e gestão de TIC. Dessa maneira, a unidade de Auditoria Interna atuará de forma a gerar valor para os tomadores de decisão, com a emissão de recomendações assertivas que assegurem a redução dos riscos relacionados com TIC, bem como a obtenção dos resultados e benefícios almejados com tais investimentos. É imperioso destacar que a área de TIC é a que o TCU e o CNJ mais têm cobrado ações de controle e atividades de auditoria interna. A relevância da tecnologia da informação e a criticidade dos processos a ela relacionados recomendam inserir nas prioridades institucionais a disponibilização de um servidor da área de TIC para estar em exercício na unidade de auditoria interna.

Elaborado por: Adriana Morales Alencar (Líder de equipe).

Revisado por: Nivaldo Azevedo dos Santos (Supervisor da Auditoria).