JUSTIÇA DO TRABALHO
TRT da 24ª Região (MS)

ACOMPANHAMENTO DAS RECOMENDAÇÕES DE AUDITORIA
TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÕES
(Atualizado em 13/03/2023)

Relatório de Auditoria	Assunto	Recomendação	Providências e Evidências de Atendimento	Situação
5/2014 **PROAD 4088/2014**	Avaliação de informações prestadas pela STI referentes ao Plano de Ação que trata da auditoria realizada pela CCAUD-CSJT em novembro de 2010.	14. Implantar efetivamente os testes com regularidade, conforme definido no Plano de Testes do Plano de Continuidade de Negócios (PCN), documentando-os para efeito de comprovação.	Está proposto no Projeto **20210429.1 - Aprimorar Processos de Segurança da Informação**, no PDTIC 2021/2022 .	Pendente
		21a. Implantar efetivamente os Planos de Testes em ambos os casos: a) Plano de Continuidade de Negócios (PCN).	Após a conclusão do projeto 20210429.1, ocorrerá a implantação efetiva do Plano de Testes.	Pendente
		23. Em favor da confiabilidade da real continuidade do negócio, recomenda-se a adoção de testes periódicos de restauração completa dos backups, conforme previsto no Plano de Testes já definido, documentando tais testes para efeito de comprovação.	Após a conclusão do projeto 20210429.1, ocorrerá a implantação efetiva do Plano de Testes.	Pendente
		16. Conforme já havia constado na auditoria do CSJT de novembro de 2010, recomenda-se à STI que apresente plano de ação indicando prazo e providências a serem adotadas com vistas à implantação do Processo Cobit4.1 ”PO2.3 Esquema de Classificação de Dados”.	Este tema deverá ser abordado no PDTIC 2023/2024, uma vez que a equipe de segurança já está sobrecarregada com diversos projetos planejados no PDTIC 2021/2022	Pendente
		17. Conforme já havia constado na auditoria do CSJT de novembro de 2010, recomenda-se à STI a implantação do Processo Cobit4.1 ”PO2.2 Dicionário de Dados Corporativos e Regras de Sintaxe de Dados”.	Este tema deverá ser abordado no PDTIC 2023/2024, uma vez que a equipe de segurança já está sobrecarregada com diversos projetos planejados no PDTIC 2021/2022	Pendente
		18. Forme especialista em Arquitetura da Informação para definir e implantar o processo Cobit4.1 ”PO2 Definir a Arquitetura da Informação”, conforme já havia constado na auditoria do CSJT de novembro de 2010, bem como para criar e manter o Modelo de Dicionário de Dados e criar e manter o Dicionário de Dados Unificado de toda a corporação.	A arquitetura utilizada nos sistemas desenvolvidos pelo TRT24 está definida pela CSAN, do CSJT. O modelo de dicionário de dados será definido no projeto “20210303.1 - Aprimorar processo de software”.	Pendente
		19. A partir da formação de especialista em Arquitetura da Informação de que trata o item 18 (acima) deste Relatório, promova a: a) Criação e manutenção do Modelo de Dicionário de Dados; b) Criação e manutenção do Dicionário de Dados Unificado de toda a corporação.	A SETIC já possui um setor com atribuição de dar apoio em questões de arquitetura de software. O modelo de dicionário de dados será definido no projeto “20210303.1 - Aprimorar processo de software”.	Pendente

Relatório de Auditoria	Assunto	Recomendação	Providências e Evidências de Atendimento	Situação
		22. Apresente plano de ação indicando prazo e providências a serem adotadas com vistas à implantação do processo Cobit4.1 " DS3 – Gerenciar Capacidade de Desempenho".	O projetos para implantação do processo de gerenciamento de capacidade está previsto para o PDTIC 2023/2024	Pendente
13/2014 **PROAD 5788/2014**	Adoção de procedimentos para registro contábil de softwares desenvolvidos internamente pela Secretaria de Tecnologia da Informação.	a) Adote providências para que, doravante, seja enviado ao Serviço de Orçamento e Finanças – SOF, os processos relativos a desenvolvimento de softwares, com as demonstrações dos respectivos custos de produção, para fins de contabilização.	Providência deste tipo será viável apenas após a conclusão do projeto de revisão do processo de desenvolvimento de software, existente no PDTIC2021/2022 e sua devida implantação. Neste sentido, tal medida será viável apenas no ano de 2023.	Pendente
		b) Avalie a conveniência e a oportunidade de expedir norma interna dispondo sobre o registro e o licenciamento de uso de soluções de tecnologia da informação desenvolvidas no âmbito deste Tribunal.	Avaliamos como inconveniente esta recomendação	Atendido Não implementado
7/2015 **PROAD 1662/2015**	Auditoria sobre gestão de Tecnologia da Informação, com ênfase no processo de desenvolvimento de softwares utilizados pelo TRT.	63. Normatize a "Metodologia de Análise por Pontos de Função" com vistas a exigir seu uso pelos profissionais desenvolvedores de softwares, tanto para softwares próprios, quanto para adquiridos e/ou desenvolvidos por terceiros.	Equipe de desenvolvimento da SETIC trabalha utilizando metodologias ágeis. E o Ponto de Função não faz parte dos princípios que estamos adotando.	Atendido Não implementado
05/2017 **PROAD 549/2017**	Auditoria no sistema corporativo interno utilizado na gestão da folha de pagamento.	a) Elabore o "Documento de Visão" para os novos sistemas que venham a ser desenvolvidos/adquiridos. (Achado 2.1)	Serão implementados a partir do momento que novos sistemas estiverem sendo desenvolvidos Previsão: fevereiro/2021.	Pendente
		c) Adote as providências necessárias para incluir na Metodologia de Produção de Software (MPS-TRT24) e no Processo Gerenciar Software (PGS-TRT24) atividades de controles internos que verifiquem a elaboração obrigatória do Dicionário de Dados para todos os sistemas a serem desenvolvidos/adquiridos, com um padrão mínimo pré-definido de seu conteúdo, de acordo com a Ordem de Serviço CTIC/GSI Nº 6/2016 (interna). (Achados 2.1 e 2.3)	Será incluído no processo de desenvolvimento de software que está em andamento no projeto "20210303.1 - Aprimorar processo de software".	Pendente
		d) Estabeleça e documente critérios para definição dos LOGs deste e de todos os sistemas informatizados do TRT-24ª Região, conforme as boas práticas de engenharia de Software e da norma ABNT ISO-IEC 27001/2006, procurando sempre envolver todas as áreas que poderão fazer uso dessas informações no futuro, como, por exemplo, a área de Auditoria de Sistemas de TIC. (Achado 2.4)	Será incluído no processo de desenvolvimento de software que está em andamento no projeto "20210303.1 - Aprimorar processo de software".	Pendente

Relatório de Auditoria	Assunto	Recomendação	Providências e Evidências de Atendimento	Situação
		e) Adote as providências necessárias para inserir na Metodologia de Produção de Software a elaboração do Manual de Normas e Procedimentos do sistema para que seja fornecido ao usuário final na fase de implantação. Sugere-se como modelo para adoção como padrão para este TRT o Manual da Secretaria de Gestão e Recursos Humanos do Estado do Espírito Santo, "CÁLCULO, AUDITORIA E CONSOLIDAÇÃO DA FOLHA DE PAGAMENTO", o qual apresenta um bom exemplo de registro das atividades não-informatizadas e informatizadas. E está disponível no endereço: (Achado 2.5)	A SETIC está seguindo o manual de práticas do CSAN, e o processo de software do TRT está em implementação. Manuais de utilização assim como treinamentos devem ser previstos na concepção de um novo produto. O cliente e o PO deverão fazer tal planejamento. O manual pode ser construído pelo PO a medida que novas funcionalidades forem entregues pelos times de desenvolvimento.	Pendente
		f) Estenda as recomendações das alíneas "a" a "e", acima, para os sistemas classificados como "nacionais".	A SETIC não tem gerência sobre os artefatos de sistemas nacionais	Não Atendido
5/2019 **PROAD 2017/2018**	AÇÃO COORDENADA DE AUDITORIA - CNJ - Avaliar os conteúdos estabelecidos para a governança e gestão de TI, considerando projetos, processos, riscos e resultados de TI em comparação com padrões internacionalmente aceitos, como COBIT, PMBOK, ITIL, CMMI, ISO 17799, ISO 27001, as Resoluções CNJ nº 91/2009, nº 182/2013, nº 198/2014 e nº 211/2015 e o perfil de governança de TI traçado pelo TCU.	a) Efetue a designação do desembargador indicado pela Presidência para compor o Comitê de Governança de TI, nos termos do art. 3º, item IV da Portaria TRT/GP nº 50/2016, ou, alternativamente, avalie a real necessidade dessa exigência no regulamento. Caso a Administração julgue desnecessária, retifique a Portaria TRT/GP nº 50/2016;	A portaria 50/2016 foi substituída pela portaria 221/2021. Por sua vez, a portaria 221/2021 será substituída em função da implantação da Resolução Administrativa 122/2021, relativa a Governança de Colegiados Temáticos no âmbito do TRT24. As minutas das novas portarias já foram encaminhadas e aguardam as providências de publicação.	Atendido
		c) Atualize a Portaria TRT/GP nº 50/2016 no que se refere aos cargos que compõem o Comitê de Gestão de TI, tendo em vista a reestruturação organizacional promovida pelas Portarias nº 47/2017 e 27/2018;	A portaria 50/2016 foi substituída pela portaria 221/2021. Por sua vez, a portaria 221/2021 será substituída em função da implantação da Resolução Administrativa 122/2021, relativa a Governança de Colegiados Temáticos no âmbito do TRT24. As minutas das novas portarias já foram encaminhadas e aguardam as providências de publicação.	Atendido
		d) Avalie a possibilidade de adotar regras para a análise e deliberação de propostas nas reuniões dos comitês de Governança de TI e de Gestão de TI, estabelecendo quórum mínimo para deliberação e quantidade de votos necessários para aprovação das propostas, tendo em vista que nem todas as decisões são tomadas pela composição plena dos respectivos comitês;	As regras para análise e deliberação de propostas pelos Comitês estão contidas no modelo de Gestão de Colegiados Temáticas definido pela Resolução Administrativa 122/2021. As minutas das novas portarias já foram encaminhadas e aguardam as providências de publicação	Atendido
		e) Estabeleça calendário anual visando dar cumprimento à periodicidade para reuniões dos comitês estabelecida nos artigos 4º e 7º da Portaria TRT/GP nº 50/2016.	No ano de 2021 os comitês de Governança de TI e de Segurança da Informação passaram a se reunir com uma maior frequência. Para o ano de 2022 será estabelecido um calendário conforme sugere este item	Atendido
		f) Avalie a possibilidade de estabelecer diretrizes formais que direcionem:		-

Relatório de Auditoria	Assunto	Recomendação	Providências e Evidências de Atendimento	Situação
		f.1) o planejamento de TI;	Portaria 202/2021	Atendido
		f.2) a gestão do portfólio de projetos de TI e do portfólio de serviços de TI;	Portaria 258/2021 e portaria 192/2021	Atendido
		f.3) as contratações de bens e serviços de TI;	Portaria 189/2021	Atendido
		f.4) as avaliações de desempenho dos serviços de TI;	Portaria 221/2021	Atendido
		f.5) comunicação dos resultados da gestão e do uso de TI para as partes interessadas;	Portaria 221/2021	Atendido
		f.6) avaliação da governança e da gestão de TI;	Portaria 221/2021	Atendido
		g) Inclua no Plano Anual de Contratações de TI o mesmo código utilizado para identificar a despesa na Proposta Orçamentária e no PETIC, conforme recomendação constante do subitem 7.1.3 do Relatório Final da 2ª Ação Coordenada de Auditoria na área de TI realizada em 2015;	Este procedimento já vem sendo empregado no plano de contratações de TI	Atendido
		h) Instituir política formal para a avaliação e incentivo ao desempenho de gestores e técnicos de TI;	Este tema deverá ser abordado no PDTIC 2023/2024	Pendente
		i) Criar política formal para a escolha dos líderes de TI;	Este tema deverá ser abordado no PDTIC 2023/2024	Pendente
		j) Criar planos, além do PETIC ou PDTIC, voltados a atender aos objetivos estratégicos institucionais vinculados à área de TI da organização;	A SETIC, obedecendo o que determina a resolução 370 do CNJ, passou a elaborar apenas o plano tático (PDTIC). A resolução estabelece ainda a necessidade de um Plano de Transformação Digital – PTD. Este último está sendo elaborado pelo CSJT para basear os demais planos dos regionais. Além destes, não temos pretensão de elaborar qualquer outro plano, sob a justifiva de pulverizar as ações da TI em diferentes plano e então dificultar o controle.	Atendido
		k) Avaliar o desempenho do pessoal de TI;	Este tema deverá ser abordado no PDTIC 2023/2024	Pendente
		l) Instituir e definir autonomia da Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais (ETIR);	Este tema deverá ser abordado no PDTIC 2023/2024	Pendente

Relatório de Auditoria	Assunto	Recomendação	Providências e Evidências de Atendimento	Situação
		m) Medir grau de alcance dos objetivos e benefícios que justificaram a abertura de projetos de TI;	Este tema deverá ser abordado no PDTIC 2023/2024	Pendente
1/2020 **PROAD 6773/2018**	Auditoria no processo de segurança da informação.	a) Implante perfis individuais de acesso ao banco de dados pelos administradores (DBA's) visando evitar a utilização de senha única. (Achado 3.1);	Conclusão do acesso individualizado no ano de 2022.	Atendido
		b) Adote, doravante, na definição das Regras do Negócio de cada sistema, regras detalhadas para trilhas de auditoria (log's), para todos os acessos ao Banco Oracle por usuários com privilégio de administrador, onde fique registrado, além da data e hora do acesso, também a íntegra dos comandos executados. (Achado 3.1);	Será incluído no processo de desenvolvimento de software que está em andamento no projeto "20210303.1 - Aprimorar processo de software".	Pendente
		c) Determine a periodicidade necessária e efetue levantamento para verificar a existência de ex-colaboradores que continuam com direito de acesso a sistemas, efetuando a sua exclusão, caso constatadas situações positivas. (Achado 3.2);	A cada alteração de lotação o servidor perde todos acessos de todos sistemas locais. Como o acesso aos sistemas nacionais não é centralizado, cabe à área de negócio (usuário) solicitar a revogação de acesso. Cabe ao sistema bloquear acessos antigos que não são usados. Geralmente as áreas possuem gestores e estes têm direitos de conceder/revogar acessos.	Não Atendido
		d) Estabeleça controles internos a fim de assegurar que o desligamento de colaboradores seja comunicado pelos gestores de contratos à Coordenadoria de Gestão de Pessoas imediatamente após o término do vínculo; (Achado 3.2);	A área de de negócio deve comunicar do desligamento. Ao mudar a lotação (desligamento encerra acesso à localidade) os sistemas locais têm os acessos revogados destes usuários.	Não atendido
		e) Doravante, na definição da arquitetura de cada sistema, registre clara e detalhadamente todos os campos passíveis de alteração que constarão das trilhas de auditoria (log's) de cada sistema, gravando os conteúdos anteriores e posteriores a movimentações que causem alterações nos mesmos. Convém que para essas definições seja consultada a Coordenadoria de Auditoria Interna. (Achado 3.4);	A arquitetura a ser utilizada é aquela definida pela CSAN. Ao utilizar a geração de LOG's precisamos focar não só na usabilidade do sistema, mas também sua performance. Esta necessidade seria um "requisito" do sistema, ou seja, uma funcionalidade a ser implementada. Deverá ser prevista e priorizada pelo PO no backlog do produto. A forma de implementar tal funcionalidade, ou seja, "como" fica totalmente a cargo dos times de desenvolvimento. O PO (junto ao cliente) deverá especificar quais informações serão armazenadas, quando e etc,. Também definirão quem pode acessar e como acessar e consumir tais dados.	Pendente

Relatório de Auditoria	Assunto	Recomendação	Providências e Evidências de Atendimento	Situação
		f) Implante no sistema SCMP as funções "Estorno de Requisição" e "Devolução ao Almoxarifado" para permitir a alteração na composição dos itens ou quantitativos nas requisições demandadas pelo Setor de Almoxarifado, ocasionada por erro em seu lançamento e possíveis devoluções ao almoxarifado. (Achado 3.5);	Alterações do sistema dependem do de autorização e priorização do comitê regional. Não cabendo à SETIC inferir nas decisões do que será ou não implementado. Por decisão da CSAN, o sistema atual não terá novidades implementadas. Por conta do desenvolvimento da versão 2, efetivamente nacional.	Não Atendido
		g) Encaminhe, como sugestão, as recomendações "a", "b", "e" e "f" ao Comitê Gestor dos sistemas "nacionais" para considerá-las nas definições de regras de negócio nos sistemas em elaboração/manutenção, como os sistemas "SCMP" e "FOLHAWEB", os quais são oriundos deste TRT. (Achados 3.1, 3.4 e 3.5);	Não faz parte das atribuições da SETIC fazer recomendações a outros órgãos. No caso de recomendações de auditoria, o próprio setor pode fazer diretamente aos comitês.	Não atendido
2/2020 **PROAD 20170/2019**	Auditoria no processo de gestão de riscos de TIC.	a) Avalie a possibilidade de revisar e reeditar a PORTARIA TRT/GP/DG Nº 61/2020, que revogou a Portaria TRT/GP/DGCA Nº 176/2016 (Política de Segurança da Informação) para contemplar a classificação de ativos em críticos e não críticos (ou de suporte), conforme preceitua a Norma ABNT ISO-NBR-27005/2008 - Gestão de Riscos de TI – no Anexo B.	Após a conclusão do projeto **20210429.1 - Aprimorar Processos de Segurança da Informação**, ocorrerá o mapeamento de ativos críticos no plano de gerenciamento de riscos.	Pendente
		b) Sugere-se que sejam designados formalmente os responsáveis pelos ativos de TIC, estabelecendo seus papéis e responsabilidades no gerenciamento de riscos de TIC.	Após a conclusão do projeto **20210429.1 - Aprimorar Processos de Segurança da Informação**, ocorrerá o mapeamento de ativos críticos e então formalizaremos seus responsáveis.	Pendente
		c) Adote procedimentos de controle para, doravante, manter atualizada a gestão dos ativos e respectivos responsáveis, com vistas a evitar responsabilização indevida por qualquer incidente de TIC a servidor do quadro ou já desligado, bem como possíveis fraudes.	Após a implantação de ferramenta ITSM, prevista no projeto **20210318.1 - Adquirir Solução de Gerenciamento de Serviços de TI.**	Pendente