PODER JUDICIÁRIO - JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO
SECRETARIA DE CONTROLE INTERNO – SCI
SEÇÃO DE CONTROLE DE GESTÃO ADMINISTRATIVA E PATRIMONIAL - SCGAP

RELATÓRIO DE AUDITORIA

I. IDENTIFICAÇÃO	
Nº do Processo	Proad nº 95/2019
Nº da Ordem de Serviço	SCI.SCGAP nº 1/2019
Seção Responsável pela Auditoria	Seção de Controle de Gestão Administrativa e Patrimonial - SCGAP
Unidade Auditada	Secretaria de Tecnologia da Informação e Comunicação
Tipo de Auditoria	Conformidade
Objeto da Auditoria	Gestão e Governança de tecnologia da informação e comunicação, estabelecida no TRT 7ª Região, notadamente ***o processo de implantação da Gestão de Riscos de TIC e a estratégia de tratamento de incidentes de segurança de TIC***

1. Introdução:

1.1. O presente Relatório apresenta os resultados da ação de controle de auditoria realizada no período de **9/1/2019 a 11/3/2019**, em cumprimento ao contido na Ordem de Serviço em epígrafe, com o objetivo de avaliar a conformidade da atuação da Gestão e da Governança de TIC do TRT7, quanto à Gestão de Riscos de TIC e ao tratamento de incidentes de segurança de TIC de acordo com o previsto no Plano Anual de Auditoria (PAA/2019).

1.2. Os trabalhos foram conduzidos em estrita observância às normas de auditoria aplicáveis ao Serviço Público Federal, não tendo sido imposta qualquer restrição a sua realização.

1.3. Os documentos referenciados neste Relatório integram o Proad nº 95/2019.

2. Escopo:

Os exames da equipe de auditoria foram desenvolvidos sobre projetos, plano de ação, ações já implementadas e informações decorrentes da auditoria em governança e gestão de TI do CNJ - PROAD nº 861/2018, tendo como parâmetro a Política de Gestão de Risco Institucional (Ato TRT7 nº 61/2018), a Política de Gestão de Risco de Segurança da Informação (Ato TRT7 nº 106/2018), a Resolução TRT7 nº 278/2017 e o Ato TRT7 nº 152/2018.

2.1 O exame de conformidade contemplou os seguintes assuntos / pontos de controle: a) implantação da gestão de risco; a.1) plano estratégico de TIC; a.2) diretrizes e regulamentação; a.3) papéis e responsabilidades; a.4) capacitação; a.5) metodologia e ferramentas; a.6) plano de ação; b) tratamento de incidentes de segurança de TI; b.1) processo de gestão de incidentes; b.2) comunicação formal de incidentes; b.3) registro de incidentes; b.4) tratamento de incidentes; b.5) capacitação.

2.2 Esta auditoria, incluiu, ainda, análise das informações disponíveis na *intranet* referentes ao Plano Estratégico de TIC e ao PDTIC 2018-2020 (Plano Diretor de Tecnologia da Informação e Comunicação).

2.3 A fase de audiência desta auditoria foi substituída pelas respostas registradas na RDI TRT7.SCI.SCGAP nº 01/2019 (doc 15) e pelas entrevistas realizadas no período de 4 a 6/2/2019 com o servidor especializado Edvaldo Bezerra Pereira Junior, designado para subsidiar de informações a equipe de auditoria.

3. Resultados dos Exames:

3.1. O resultado dos exames realizados encontra-se registrado sob os títulos "Constatações" e "Informações" deste Relatório de Auditoria, juntamente com as respectivas recomendações para aprimoramento do procedimento.

3.2. Com a presente auditoria, evidencia-se a necessidade da adoção de práticas mais efetivas para a gestão de riscos de TIC e tratamento de incidentes de segurança da informação, de forma a assegurar o cumprimento dos normativos vigentes e a continuidade e a segurança dos serviços de tecnologia da informação e comunicação.

II. CONSTATAÇÕES

Ponto de Controle: Implantação da gestão de riscos de TIC

Dados da Constatação

Nº 1.

Descrição Sumária:

Ausência de apuração dos indicadores relacionados ao Objetivo 3 (Implementar a gestão de Riscos de TI) do Plano Estratégico de TIC - PETIC 2015-2020.

Fato:

Consta no Portal da TI: Início>Planejamento TI> Indicadores e metas>indicadores estratégicos, quadro resumo para demonstrar o acompanhamento dos objetivos estratégicos de TIC previsto no PETIC 2015-2020. Todavia não houve apuração dos indicadores relacionados a seguir, responsáveis pela medição dos resultados referente ao objetivo 3: **"Implementar a gestão de riscos de TI"**.

ISCTI - Índice de soluções críticas de TI do TRT7 com riscos mapeados

META	Percentual dos riscos de soluções de TI do TRT7, consideradas críticas, mapeados					
	2015	2016	2017	2018	2019	2020
	-	Definir soluções críticas	LB	Definir metas e mensurar		

ISCNTI - Índice de soluções nacionais críticas de TI com riscos mapeados

META	100% dos riscos de soluções nacionais, consideradas críticas, mapeados					
	2015	2016	2017	2018	2019	2020
	LB	50%	75%	100%	100%	100%

Manifestação da unidade auditada: (Resposta à RDI)

Em resposta à RDI TRT7.SCI. SCGAP Nº 1/2019, a unidade auditada informou:

Questão 1.1 Foram identificadas as soluções críticas, conforme previsto no PETI?

"1.1 Não houve até o momento definição pelo CSJT de quais as soluções nacionais de TI seriam consideradas críticas para fins de mapeamento de riscos. Na reunião do Comitê de Governança de TIC do TRT7 de 26/10/2016 (RAE de TIC) deliberou-se, no contexto da análise do referido objetivo estratégico de TIC, que o Comitê de Gestão de Riscos do TRT7 faria a indicação dos sistemas críticos, o que não

ocorreu até o momento. Mesmo assim, a SETIC deliberou na reunião de 23/01/2017 pelo início da elaboração dos Planos de Continuidade dos Serviços Essenciais de TIC. Para essa atividade, seriam considerados essenciais os mesmos serviços elencados na RAE para cálculo dos indicadores de monitoramento de SLA e/ou de indisponibilidade não programada. Embora conduzido antes do próprio processo de gerenciamento de riscos o Plano de Continuidade de TIC é reconhecidamente uma das principais medidas de mitigação de riscos. A Gestão de Riscos voltou à pauta do Comitê de Governança de TIC na reunião do dia 29/08/2018 que deliberou pelo início do mapeamento de riscos pelos soluções nacionais PROAD, Sistema de RH/Folha (SIGEP), PJe e AUD e pelas soluções de ambiente do TRT7 site institucional e Portal de Serviços."

Análise da Equipe:

A Secretaria de Tecnologia de Informação e Comunicação informou em sua resposta que foi iniciada, em 2017, a elaboração dos Planos de Continuidade dos Serviços Essenciais de TIC *(Item 4 da RDI TRT7.SCI.SCGAP nº 01/2019)* como a principal medida de mitigação de risco. Em 2018, foram elencadas as soluções críticas nacionais (PROAD, Sistema de RH/Folha (SIGEP), PJe e AUD) para início do mapeamento de riscos, conforme exigido para o cálculo dos indicadores o ISCTI e o ISCNTI.

Informou, ainda, que em razão da indefinição de quais soluções críticas nacionais seriam mapeadas, os indicadores não foram aferidos, determinando o não cumprimento do calendário.

Registre-se que os indicadores e metas são partes integrantes de um sistema de acompanhamento de gestão que ajuda a direcionar o administrador a um melhor desempenho na busca de melhores resultados, seja pela comparação com indicadores de outros órgãos, seja por meio do contraste com indicadores calculados para o próprio órgão, mas relativos a períodos distintos.

Isto posto, entende esta unidade de controle que não é possível assegurar que o objetivo estratégico está sendo alcançado se os indicadores não estiverem sendo medidos periodicamente e de forma pontual e específica para este Regional.

Tendo em vista a dificuldade de medição dos indicadores supracitados e a previsão, em 2019, de início dos trabalhos para a elaboração do PETIC referente ao quinquênio 2021-2026, sugere-se que sejam revistos ou alterados os indicadores e metas para formatos passíveis de monitoramento conforme a realidade do Tribunal, de modo que não haja descontinuidade no acompanhamento do alcance do Objetivo 3.

Recomendação:

1.1 Elaborar proposta de revisão dos indicadores e metas definidos no PETIC 2015-2020 referente ao objetivo 3: "Implementar a gestão de riscos de TI."

Prazo	120 dias

Ponto de Controle: Implantação da gestão de riscos de TIC
Dados da Constatação
Nº 2.
Descrição Sumária:
Ausência de plano de ação contendo cronograma para mapeamento dos riscos de processos.

Fato:

No portal interno deste Tribunal, foi identificado plano de ação em segurança da informação referente ao exercício de 2017 (*link*: *http://intranet/sti/files/seguranca_informacao/planos_acao/PLANO_DE_AO_EM_SI_-_v3.pdf*, porém não para os anos seguintes.

O Comitê Gestor de TIC, em reunião realizada no dia 29/8/2018, indicou para quais serviços essenciais deverá ser realizado o mapeamento de risco, conforme planilha do Quadro resumo para acompanhamento dos indicadores estratégicos disponibilizado na *intranet* do Tribunal. Verificou-se que alguns processos no âmbito da SETIC foram mapeados. No entanto, os processos mapeados não são os selecionados como essenciais.

A SETIC adquiriu a ferramenta Risk Management,em 2015, para auxiliar a implantação da Gestão de Riscos de Segurança da Informação e Comunicações, porém a mesma não está sendo utilizada, conforme manifestação da unidade auditada (item 3 da RDI *TRT7.SCI.SCGAP nº 01/2019).*

Manifestação da unidade auditada: (Resposta à RDI)

Em resposta à RDI TRT7.SCI. SCGAP Nº 1/2019, a unidade auditada informou:

Questão 2.1 Há planos de ação em segurança da informação para os anos seguintes a 2017? Em caso afirmativo, apresentar evidências.

"2.1 - Sim, há ações de aprimoramento da segurança da informação presente no portfólio de projetos PDTIC 2018/2020 aprovados formalmente pelo Comitê de Governança de TIC na reunião de 24/07/2018 (documentos 15 e 16 do PROAD 6057/2017), de onde se extrai os projetos:

Plano de Continuidade de TI
Revisar a norma de backup e arquivamento
Implantar a Gestão de Incidentes de Segurança da Informação
Revisão da norma gestão de riscos em SI
Implantação do Sistema de Gestão da SI
Implantar a Gestão de Riscos de TIC
Campanha institucional de conscientização em SI
Implantação da Gestão de Controle de Acesso
Implantação do Monitoramento de uso dos recursos de TI
Avaliar o processo de gerenciamento de vulnerabilidades técnicas
Implantar a Gestão de Ativos de TIC
Apoiar a elaboração de norma sobre classificação de informações
Revisar normas de controle de acesso e de uso de recursos de TIC
Adequação da estrutura organizacional da área responsável pela SI

Destaca-se que em 2018 não foi elaborado um documento formal "PLANO DE AÇÃO EM SEGURANÇA DA INFORMAÇÃO" como o de 2017, mas todas as atividades de trabalho que compõem um plano de ação foram cadastradas e organizadas em portfólio de projetos no software JIRA (de acordo com os projetos aprovados e priorizados pelo CGTIC):

https://jira.trt7.jus.br/jira/secure/RapidBoard.jspa?rapidView=1539&selectedIssue=NGTICP-7&quickFilter=1998

Em tempo, informamos que o site 'plano de ação em segurança da informação' presente na intranet foi atualizado, considerando a nova prática.

Cumpre ainda informar que o plano de ação de segurança da informação de 2017 é desdobramento do PDTIC vigente à época e foi acompanhado pela SETIC desde sua criação, como evidenciado na reunião de 25/08/2016."

Questão 3.1 Quais os processos de TIC que já foram mapeados?

"3.1 - Há alguns processos de TIC mapeados (Planejamento, Gestão de Serviços, Contratações e Desenvolvimento de Software).

Contudo, considerando a maturidade e condições operacionais da SETIC para condução do processo de gestão de riscos, bem como os indicadores e metas do objetivo estratégico n. 3 do PETI 2015/2020, a gestão de riscos foi iniciada a partir da definição de "soluções críticas" para mapeamento de riscos. As atividades estão agrupadas no projeto "Implantar a Gestão de Riscos de TIC" presente no PDTIC 2018/2020, identificada pelo código NGTICP-7 na ferramenta de gerenciamento de demandas, de onde se extrai as seguintes atividades programadas:

NIDGDRDS-3	Montar base de conhecimento sobre gestão de riscos	RESOLVIDO	Alexandre de Andrade Barbosa
NIDGDRDS-4	Elaborar minuta de documento (template) de Análise de Contexto	EM EXECUÇÃO	Alexandre de Andrade Barbosa
NIDGDRDS-2	Analisar uso do software "Ágatha - Sistema de Gestão de Riscos"	ABERTO	Edvaldo Bezerra Pereira Junior
NIDGDRDS-1	Implantar o Processo de Gestão de Riscos de Segurança da Informação	ABERTO	Alexandre de Andrade Barbosa

Questão 3.2 Há um cronograma estabelecido para o mapeamento dos demais processos? Em caso afirmativo, apresentar o cronograma.

"3.2 - Ainda não há um cronograma definido."

Questão 3.3 A ferramenta *Risk Management* está sendo efetivamente utilizada com esse propósito?

"3.3 - A ferramenta Risk Management não está sendo utilizada para a gerência dos riscos, pois o mapeamento dos riscos das soluções de TI selecionadas ainda está em andamento. Outro impeditivo para sua utilização é que, no ano de 2016, em face de restrições orçamentárias severas, o respectivo contrato de suporte foi suspenso e posteriormente cancelado. Para sua colocação em uso, faz-se necessária a recontratação do suporte para a ferramenta em tela, visando sua atualização em face de alterações nas bibliotecas utilizadas como referência para avaliação dos riscos (Ex: COBIT, etc). Por outro lado, smj, para que a ferramenta em questão alcance maior efetividade, é imprescindível a sua disseminação por outras áreas do Tribunal que tenham demanda correlata, por exemplo, o uso pelas entidades e unidades incumbidas da Governança no Regional e pela Secretaria de Controle Interno."

Questão 6.1 Essa resposta *(a SETIC informou que não há processo de gestão de risco de TIC formalmente instituído (Questão 33, Proad 861/2018))* continua atual? Caso haja processo(s) de gestão de risco já instituído(s), relacionar e indicar a fase em que se encontra(m).

"6.1 - O processo de gestão de risco de TIC foi formalmente instituído pelo ATO TRT7 106/2018 e descrito em seus anexos. Atualmente, está sendo estabelecido o contexto de cada um dos sistemas nacionais: PROAD, Sistema de RH/Folha (SIGEP), PJe e AUD. As atividades estão sendo conduzidas pelo servidor Alexandre Barbosa e registradas no projeto "Implantar a Gestão de Riscos de TIC" do PDTIC 2018/2020, identificado no Jira pelo código NGTICP-7.

Cabe destacar que o documento chamado de "contexto" é um dos artefatos previstos no referido processo estabelecido pelo Ato 106/2018."

Análise da Equipe:

Apesar da existência de projetos aprovados no PDTIC 2018-2020, em especial o projeto cadastrado no JIRA NGTICP-7 para "Implantar a Gestão de Riscos de TIC", não está configurado plano formalmente articulado para corresponder ao plano de ação em gestão de riscos e segurança da informação, com o estabelecimento de diretrizes gerais e específicas.

Apesar de formalmente instituído o processo de gestão de riscos de TIC, Ato TRT7 n. 106/2018 , não há, ainda, um cronograma do projeto 'implantar a gestão de riscos de TIC'. Para os quatro sistemas nacionais, selecionados pelo Comitê de Governança de TIC, os trabalhos nessa área se encontram na fase de **definição do contexto**, que constitui apenas um dos artefatos do mencionado processo.

Uma das etapas definidas no Anexo A do Ato TRT7 n. 106/2018, que regulamenta a Gestão de Riscos de Segurança da Informação e Comunicações, consiste em **analisar e avaliar os riscos.** Esta unidade entende que o mapeamento de processos constitui requisito para a efetiva implantação dessa etapa, pois permite que toda a sistemática de um determinado processo possa ser compreendida facilitando a identificação dos riscos.

Apesar da necessidade de uma ferramenta para apoiar a implantação da gestão de risco na TIC e da solução Risk Management ter sido adquirida desde de 2015, ainda continua pendente a definição de qual ferramenta será utilizada pela SETIC.

Conforme noticiado pela unidade auditada, existe estudo para avaliar a utilização do software "Ághata - sistema de gestão de risco" em substituição a ferramenta Risk Management.

Recomendações:

2.1 Elaborar Plano de Ação e cronograma para o mapeamento de riscos dos processos essenciais de TIC.

2.2 Definir ferramenta para apoiar a implantação da gestão de riscos na TIC.

Prazos	60 dias (para 2.1) 90 dias (para 2.2)

Ponto de Controle: Implantação da gestão de riscos de TIC
Dados da Constatação
Nº 3
Descrição Sumária:

Ausência de Plano de Continuidade de Serviços Essenciais de TI ou Gestão de Continuidade de TIC (Ato TRT7 n. 02/2017).

Fato:

A Gestão de Continuidade de TIC do TRT da 7ª Região foi estruturada conforme a norma complementar 07/NC/STI/SESEG, instituída pelo Ato TRT7 n. 02/2017. Verificou-se que em resposta ao questionário elaborado pelo CNJ na Ação Coordenada sobre Governança e Gestão de Tecnologia da Informação e Comunicação realizada no período de 2/5/ a 29/6/2018 (Proad nº 861/2018), a SETIC informou que não existia um Plano de Continuidade de Serviços Essenciais de TI (Questão 29), em que pese a existência de normativo definindo o processo de implementação.

Ressalte-se que referido normativo, publicado em 3/1/2017, no seu Art 2º determinou o prazo de 180 dias para elaboração do processo de Gestão de Continuidade de TIC.

O processo visa especificar os requisitos para planejar, estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar continuamente um sistema de gestão documentado para proteger-se, reduzir a possibilidade de ocorrência, preparar-se, responder e recuperar-se de incidentes de interrupção quando estes ocorrerem.

Foram definidas as seguintes fases para implementação da Gestão de Continuidade de TIC:

1. Aspectos da Segurança da Informação na Gestão da Continuidade do Negócio
2. Análise de Impacto em caso de interrupção nos serviços de TIC
3. Planos de Contingência Operacional
4. Planos de Recuperação de Desastres
5. Padrão de Nomenclatura dos Planos

Manifestação da unidade auditada: (Resposta à RDI)

Em resposta à RDI TRT7.SCI. SCGAP Nº 1/2019, a unidade auditada informou:

Questão 4.1 Essa resposta *(a SETIC informou que não existe um Plano de Continuidade de Serviços Essenciais de TI (Questão 29, Proad 861/2018)* continua atual? Se já houver plano, apresentar evidência.

"4.1 Na reunião do Comitê Gestor de TIC do dia 29/08/18[1], ficou deliberado que o primeiro serviço essencial que teria um plano formalizado de continuidade seria o PJ-e. Referido plano já está escrito e está em fase de teste. Link para acesso:

http://wiki/STI/Escrit%C3%B3rio_de_Seguran%C3%A7a/Gest%C3%A3o_de_continuidade_de_TIC/Planos_de_Conting%C3%AAncia_Operacional_de_TIC/PCO_-_PJe"

Análise da Equipe:

Registre-se que foram definidos pelo Comitê Gestor de TIC em reunião realizada no dia 29/8/2018, os seguintes serviços de TI como essenciais: PROAD, e_mail, Site Institucional, Sistema RH/folha(SIGEP), Portal de Serviços, Pje, AUD, Certificado digital, E-jus, Estações de Trabalho e Sistema de Ponto.

1 http://intranet/sti/files/reunioes/atas/2018/comite-governanca-ti/20180829-CGOVTI-Ata_da_Reunio.pdf

Além desta definição, o Comitê indicou que o processo do PJe deverá conter o plano de continuidade, conforme planilha do Quadro resumo para acompanhamento dos indicadores estratégicos .

Analisando a resposta e o *link*, verificou-se a existência do Plano de Contingência Operacional do PJe e que o mesmo encontra-se em fase de teste. Está em fase de elaboração o **Plano de Recuperação de Desastres**, uma das fases integrantes do processo da Gestão de continuidade de TIC.

Durante a fase de entrevista com o servidor especializado Edvaldo, foi relatada a dificuldade de simulação e teste do plano, em função da impossibilidade de realização de horas extraordinárias. A atividade demanda dois dias de trabalhos com paralisação do sistema o que impossibilita sua realização em dias úteis.

A inexistência do Plano de Recuperação de Desastres e dos Planos de Contingência para os demais serviços considerados essenciais fragiliza os mecanismos de controle dos riscos, uma vez que a Gestão de Continuidade de TIC visa garantir a disponibilidade e a integridade dos sistemas aplicativos, dados e documentos digitais do TRT7.

Recomendações:

3.1 Concluir os testes do plano de contingência do PJe, o que demanda a solução, por parte da Administração, da questão da necessidade da realização do trabalho em dias não úteis.

3.2 Elaborar Plano de Recuperação de Desastres para conclusão da Gestão de Continuidade de TIC, pelo menos para o PJe.

3.3 Apresentar cronograma para elaboração de Planos de Contingência para os demais serviços essenciais, além do PJe.

Prazos	120 dias (para 3.1 e 3.2) 180 dias (para 3.3)

Ponto de Controle: Implantação da gestão de riscos de TIC

Dados da Constatação

Nº 4.

Descrição Sumária:

Descumprimento de periodicidade de reunião conjunta do CGSI (Comitê Gestor de Segurança da Informação) com a CSI (Comissão de Segurança Institucional).

Fato:

De acordo com a Res. TRT7 278/2017, "Art. 13. O CGSI se reunirá ordinariamente com a Comissão de Segurança Institucional, pelo menos duas vezes por ano, e de forma extraordinária, quando se fizer necessário."

Em resposta ao CSJT (Proad nº 861/2018), a SETIC informou que o CGSI foi formalmente instituído, mas não realiza reuniões periódicas.

Essa situação de inconformidade com o normativo interno ainda persiste.

Manifestação da unidade auditada: (Resposta à RDI)

Em resposta à RDI TRT7.SCI. SCGAP Nº 1/2019, a unidade auditada informou:

Questão 5.1 Essa resposta *(a SETIC informou que o CGSI foi formalmente instituído, mas não realiza reuniões periódicas (Questão 32, Proad 861/2018))* continua atual? Caso se realizem reuniões periódicas, apresentar evidências (atas). "5.1 - O CGSI realizou uma reunião em 26/10/2018, conforme ata disponibilizada no seguinte endereço eletrônico em nota de rodapé.[2] Marcou-se nova reunião para 16/11/2018, mas essa reunião não se realizou. Em 2019, pretende-se realizar ordinariamente, no mínimo, 01 (uma) reunião por semestre, além de reuniões extraordinárias para atender às demandas relacionadas à Segurança da Informação. Ainda não há calendário divulgado para essas reuniões."
Análise da Equipe: O descumprimento de determinação da Res. TRT7 nº 278/2017 pode ocasionar prejuízo ao desempenho do CGSI. Essa desconformidade com o comando do normativo já havia sido registrada no PROAD nº 861/2018. A Ata da reunião encaminhada pela SETIC em resposta à RDI permite concluir que não houve participação da Comissão de Segurança Institucional naquele encontro. A propósito, não está sequer mencionada essa Comissão, tampouco estiveram presentes (ou foram convocados) seus Desembargadores membros, nomeados por meio da Resolução TRT7 200/2018. Necessário, portanto, enquanto vigente o normativo referido, que se promovam reuniões para a adequado alinhamento das ações encetadas por esses dois colegiados.
Recomendação: **4.1** Promover reuniões conjuntas periódicas do CGSI e da CSI, conforme definido na Res. TRT7 nº 278/2017, ou avaliar a conveniência de alterar a norma nesse aspecto.

Prazos	Não se aplica.

Ponto de Controle: Implantação da gestão de riscos de TIC
Dados da Constatação
Nº 5.
Descrição Sumária: Falta de ação institucional de sensibilização, conscientização e capacitação em segurança da informação de TIC.
Fato: Em resposta ao CSJT (Proad nº 861/2018), a SETIC informou que ações de sensibilização, conscientização e capacitação em segurança da informação para os agentes públicos da instituição nunca foram realizadas, porém havia estudos para a implementação dessas ações. Desde 2017, no entanto, ações de capacitação estavam previstas no plano de ação em segurança da Informação.informação para os agentes públicos da instituição nunca foram realizadas, porém havia estudos para a implementação dessas

[2] https://extranet.trt7.jus.br/sti/files/reunioes/atas/2018/cgsi/002_-_DOCUMENTO_-_Ata_de_reunio_-_26-10-2018.pdf

ações. Desde 2017, no entanto, ações de capacitação estavam previstas no plano de ação em segurança da Informação.

Essa situação de inconformidade com o normativo interno ainda persiste.

Manifestação da unidade auditada: (Resposta à RDI)

Em resposta à RDI TRT7.SCI. SCGAP Nº 1/2019, a unidade auditada informou:

Questão 7.1 Essa resposta *(referida no fato)* continua atual? Em caso negativo, apresentar evidências das ações realizadas

"7.1 - Para dar suporte às ações de sensibilização, conscientização e capacitação previstas no plano de 2017 a SETIC elaborou cartilhas acerca de diversos assuntos relacionados ao tema. Tais conteúdos foram apresentados à Divisão de Comunicação Social conforme email abaixo como subsídio para produção de vídeos. Porém, não houve continuidade.
E-mails e cartilhas da campanha institucional de conscientização em SI:
https://drive.google.com/drive/u/0/folders/1r6X5vOW2ZooiKxqN1ykY9VOqyOyaxhAO"

Análise da Equipe:

A segurança da informação requer, além dos instrumental tecnológico, ações efetivas de sensibilização, conscientização e capacitação dos agentes públicos da instituição. Todavia, isso não tem sido, de fato, observado no TRT7 - a propósito, ações dessa natureza não vêm sendo realizadas. Apesar disso, não houve progresso, desde o PROAD nº 861/2018, quanto à sensibilização, conscientização e capacitação em segurança da informação para os agentes públicos da instituição.
De acordo com Edvaldo Bezerra Pereira Júnior (servidor da SETIC), em entrevista à SCGAP realizada no dia 5/2/2019, a proposta das cartilhas não foi bem assimilada pela Divisão de Comunicação Social, que propôs, como alternativa, a produção de vídeo. Isso, porém, não evoluiu - nenhum vídeo chegou a ser produzido.

Recomendação:
5.1 Estabelecer plano ação para a sensibilização, conscientização e capacitação, referentes à segurança da informação, dos usuários no âmbito do TRT7.

Prazos	30 dias

Ponto de Controle: Tratamento de incidentes de segurança de TIC

Dados da Constatação

Nº 6.

Descrição Sumária:

Não cumprimento integral pelo NGTIC (Núcleo de Apoio à Gestão de TIC e Segurança da Informação) e pela ETIR (Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais) de suas atribuições, no que concerne a esse ponto de controle.

Fato:

Conforme manifestação da unidade auditada, em resposta ao item 7 da RDI TRT7.SCI.SCGAP nº 01/2019, não há atuação específica do NGTIC no apoio ao TRT7 nas atividades de capacitação e tratamento de incidentes de segurança em sua rede de computadores (item 7.2.7 do Ato nº 152/2018) e na disseminação de cultura voltada para comunicação de incidentes de segurança da informação (item 7.2.8 do Ato TRT7 nº 152/2018

O Regulamento Geral, por sua vez, estabelece para o NGTIC, dentre outras atribuições, "promover cultura de segurança da informação" (Art 42, RG).

Manifestação da unidade auditada:

Em resposta à RDI TRT7.SCI. SCGAP Nº 1/2019, a unidade auditada informou:

Questão 13.1 Todas as atribuições do NGTIC estão sendo exercidas, em especial 7.2.7. e 7.2.8? Em caso afirmativo, apresentar evidências.

"13.1 - O Núcleo de Apoio à Gestão de TIC e Segurança da Informação está desempenhando as atribuições previstas no Ato 106/2018 (Equipe e Processo de Tratamento e Resposta a Incidentes na Rede de Computadores do Tribunal Regional do Trabalho da 7ª Região), conforme a capacidade operacional disponível. Constam no portfólio do NGTIC formalmente aprovados e priorizados pelo Comitê de Governança os seguintes projetos que possuem relação direta com as atribuições em questão:

Implantar a Gestão de Incidentes de Segurança da Informação
Campanha institucional de conscientização em SI
Adequação da estrutura organizacional da área responsável pela SI

Especificamente quanto à atribuição "7.2.7. Apoiar o TRT7 nas atividades de capacitação e tratamento de incidentes de segurança em sua rede de computadores." incluímos, na pasta compartilhada indicada abaixo, dois relatórios de incidentes de segurança da informação confeccionados pelo NGTIC.

Relatórios técnicos de Incidente de Segurança da Informação:

https://drive.google.com/drive/u/0/folders/1Ju8G-0sNrnxtrMgb4NWu42-Q_cxdP0gs

Especificamente quanto à atribuição "7.2.8. Disseminar cultura voltada para comunicação de incidentes de segurança da informação." não houve, ainda, atuação específica, além da instrução presente e publicada na própria norma, reproduzida a seguir:

> "2.1. Registrar incidente de segurança A comunicação de ocorrência ou suspeita de incidente de segurança da informação pode ser feita por qualquer magistrado, servidor, estagiário ou colaborador por meios dos seguintes canais:
>
> a) Registro na Central de Serviços de TIC, disponível na intranet (https://centraldeservicos.trt7.jus.br) ou;
>
> b) Diretamente ao Gabinete da SETIC: pelo e-mail setic@trt7.jus.br, telefone ou pessoalmente, ou ainda;
>
> c) Diretamente à equipe responsável pelo tratamento de incidentes de segurança: pelo e-mail etir@trt7.jus.br; "

Análise da Equipe:

As atribuições do NGTIC estabelecidas pelo Ato nº 152/2018 não estão perfeitamente alinhadas com aquelas previstas no Regulamento Geral deste TRT7.

Em que pese a apresentação de alguns relatórios técnicos que evidenciam um esforço no amadurecimento do processo de gestão de incidentes, nem NGTIC, nem ETIR cumprem integralmente as atribuições que lhe são próprias.

Recomendação:	
6.1 Adotar providências para o integral cumprimento das atribuições do NGTIC e da ETIR, conforme o Ato nº 152/2018 (tratamento de incidentes de segurança).	
Prazos	180 dias

Ponto de Controle: Tratamento de incidentes de segurança de TIC
Dados da Constatação
Nº 7.
Descrição Sumária: Falta de divulgação quanto ao procedimento para registro de incidentes de segurança de TIC.
Fato: O Ato nº 152/2018 estabelece, entre as atribuições do NGTIC, "disseminar cultura voltada para comunicação de incidentes de segurança da informação." Esse normativo, em seu Anexo A, esclarece que o procedimento para o registro de incidente de Segurança: "A comunicação de ocorrência ou suspeita de incidente de segurança da informação pode ser feita por qualquer magistrado, servidor, estagiário ou colaborador por meios dos seguintes canais: a) Registro na Central de Serviços de TIC, disponível na *intranet* (https://centraldeservicos.trt7.jus.br) ou; b) Diretamente ao Gabinete da SETIC: pelo e-mail setic@trt7.jus.br, telefone ou pessoalmente, ou ainda; c) Diretamente à equipe responsável pelo tratamento de incidentes de segurança: pelo e-mail etir@trt7.jus.br;..." No entanto, falta divulgação quanto ao procedimento para registro de incidentes.
Manifestação da unidade auditada: (Resposta à RDI) Em resposta à RDI TRT7.SCI. SCGAP Nº 1/2019, a unidade auditada informou: Questão 12.1 É feita divulgação orientativa para que os usuários reportem incidentes? Em caso positivo, de que modo? "12.1 - Não há nenhuma ação da central de serviços, até o momento, incentivando os usuários a registrarem os incidentes específicos relacionados à segurança da informação. A divulgação do canal de comunicação da Central de Serviços para o registro de incidentes de TI, de forma geral, é realizada através de *link* permanente na página inicial da intranet e de vídeos orientativos: http://intranet/files/publicacoes/videos/assyst_02_abrir_chamado.mp4" Questão 12.2 As etapas previstas do processo de gestão de incidentes de segurança estão sendo implementadas? Em caso afirmativo, apresentar evidências. "12.2 - O Ato 152/2018 foi instituída em 27 de setembro de 2018, porém as ações não foram implementadas integralmente. Como evidência apresentamos no tópico 12.3 dois relatórios de incidentes de segurança construídos que contempla vários aspectos previstos no referido ato normativo." Questão 12.3 Há exemplo concreto de aplicação dessa rotina processual? Em caso afirmativo, apresentar evidências (relatórios de incidentes e de seu tratamento). "12.3 - Relatórios técnicos de Incidente de Segurança da Informação: https://drive.google.com/drive/u/0/folders/1Ju8G-0sNrnxtrMgb4NWu42-Q_cxdP0gs"

Análise da Equipe: De acordo com resposta à RDI TRT7.SCI.SCGAP nº 01/2019, constata-se que inexiste trabalho com o fito de promover a divulgação orientativa para que os usuários reportem incidentes. Ademais, quanto ao processo de gestão de incidentes de segurança, não estão sendo implementadas todas as etapas previstas, como informa a unidade auditada em resposta ao item 12 da RDI desta Secretaria.	
Recomendação: **7.1** Estabelecer plano de ação (incluindo cronograma) para as implementações pendentes ao cumprimento integral do que dispõe o Ato nº 152/2018, incluindo ações para que os usuários de TIC possam conhecer os canais de registro e operacionalizá-los adequadamente.	
Prazos	30 dias

III. INFORMAÇÕES

Informação
Nº 1
Descrição Sumária: Divergências entre normativos deste Tribunal (Item 8 da RDI TRT7.SCI.SCGAP nº 01/2019).

Fato:

Há uma aparente superposição entre o art. 8º do Ato TRT7 nº 61/2018 e o modelo de processo de gestão de risco de segurança da informação, referido no item 2 do Anexo A do Ato TRT7 106/2018.

Exemplificativamente, o processo de gestão de riscos de segurança da informação contempla oito etapas, enquanto o Ato TRT7 nº 61/2018 prevê 6 etapas. Há ainda diferenciação nos parâmetros adotados na definição de contexto.

Tendo o Ato TRT7 nº 61/2018 estabelecido a Política de Gestão de Riscos do TRT7, não se observa padronização do processo (art. 8º) em comparação ao definido no Ato TRT7 106/2018 para a segurança da informação.

Em resposta ao item 8 da RDI TRT7.SCI.SCGAP nº 01/2019, a SETIC estabeleceu a correspondência entre as duas normas, informando que algumas atividades se adequaram ao fluxo de trabalho, conforme demonstrado no quadro abaixo:

Art. 8º do Ato TRT7 nº 61/2018 - Gestão de riscos	**Item 2 do Anexo A do Ato TRT7 nº 106/2018 - Gestão de Riscos de Segurança da Informação.**
I - estabelecimento do contexto;	Definir o contexto;
II - identificação dos riscos;	Analisar e avaliar os riscos;
III - análise dos riscos;	Analisar e avaliar os riscos;
IV - tratamento dos riscos;	Tratar os riscos; Aceitar os riscos;

	Implementar o Plano de Tratamento de Riscos;
V – monitoramento e análise crítica;	Monitorar os riscos; Analisar criticamente os riscos;
VI - comunicação e consulta	Item 2.9 do Anexo A estabelece que será utilizado o processo de comunicação da SETIC
Não contemplado	Melhorar o Processo de Gestão de Riscos de Segurança da Informação.

Analisando a relação estabelecida entre as normas, verificou-se que a fase não contemplada no Art. 8º (conforme o quadro acima) pode ser compreendida como inserida no Art. 9º do Ato TRT7 nº 61/2018 (revisão) "*O processo de gestão de riscos deve ser realizado em ciclos não superiores a 6 seis) anos, abrangendo os processos de trabalho das áreas de gestão orçamentária,gestão processual, gestão de pessoas, tecnologia da informação, comunicação e aquisições".*

Assim sendo, esta unidade coaduna-se com a SETIC no entendimento que as diretrizes gerais do Ato TRT7 nº 61/2018, que instituiu a Política de Gestão de Riscos no Tribunal, estão mantidas.

Informação

Nº 2.

Descrição Sumária:

Normativos internos em desacordo com a estrutura organizacional do TRT7 (item 9, 10 e 11 da TRT7.SCI.SCGAP nº 01/2019).

Fato:

1. De acordo com o Ato TRT7 nº 106/2018 (Gestão de risco da segurança da informação), "8.3. Cabe a Seção de Segurança da Informação: 8.3.1. Gerir e executar o Processo de Gestão de Riscos no TRT junto aos gestores dos riscos."

Todavia, não consta no Regulamento Geral do TRT7 a Seção de Segurança da Informação.

Tendo sido extinta a SSI (Seção de Segurança da Informação), as suas atribuições foram, ao que noticia a unidade auditada, transferidas para o NGTIC (Núcleo de Apoio à Gestão de TIC e Segurança da Informação).

2. De acordo com a Resolução TRT7 nº 278/2017**,** "Art. 8º A Segurança da Informação do Tribunal Regional do Trabalho possui a seguinte estrutura:

I - Comissão de Segurança Institucional (CSI);

II - Comitê Gestor de Segurança da Informação (CGSI);

III - Gestor de Segurança da Informação e Comunicações (GSI);

IV - Seção de Escritório de Segurança da Informação (ESI);

V - Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais (ETIR)."

Todavia, não consta no Regulamento Geral do TRT7 a Seção de Escritório de Segurança da Informação. A unidade auditada informou que a Seção Escritório de Segurança da Informação não existe mais, pois tais atribuições foram herdadas pelo Núcleo de Apoio à Gestão de TIC e Segurança da Informação.

Diante do exposto, conclui-se que a nomenclatura constante no Resolução TRT7 nº 278/2017 não está sintonizada com o Regulamento Geral.

3.A Res. TRT7 nº 278/2017 menciona a Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais (ETIR) e o Ato TRT7 nº 152/2018, por sua vez, menciona Equipe de Tratamento e Resposta a Incidentes na Rede de Computadores (ETIR). A Unidade auditada informou que se trata da mesma equipe, apesar das distintas nomenclaturas.

Mencionadas algumas divergências nas nomenclaturas dos normativos vigentes que tratam da gestão de risco no âmbito deste TRT7, sugerem-se ajustes na Res.TRT7 nº 278/2017 e no Ato TRT7 nº 106/2018 para que os mesmos se tornem compatíveis com a atual estrutura organizacional do TRT7.

Informação

Nº 3

Descrição Sumária:

Quadro de pessoal e estrutura insuficientes do NGTIC (Núcleo de Apoio à Gestão de TIC e Segurança da Informação) para fazer frente às suas atribuições.

Fato:

1. Em entrevista, os servidores do NGTIC relataram frequentemente que a lentidão no adimplemento das providências a seu cargo era diretamente vinculada à escassez de pessoal. Em consulta ao Mentorh, constata-se a lotação do NGTIC e de Seção vinculada (Seção de Apoio às Contratações de TI):

NGTIC	Seção de Apoio às Contratações de TI
Reginaldo Garcia Dupin - Coordenador	Fernando José Sales Monteiro - Coordenador
Edvaldo Bezerra Pereira Júnior	-

O servidor Edvaldo, porém, vinculado ao quadro de pessoal do TRT9 e lotado neste Tribunal em decorrência de remoção por permuta (TRT7 - TRT9), por meio da Portaria TRT7.GP 296/2017. Essa portaria, entretanto, teve seus efeitos cessados pela Portaria TRT7.GP 48/2019, após a quebra da permuta, conforme se verifica do Proad 7136/2018, o que redundará no seu retorno ao tribunal de origem.

De outra parte, conforme art.12 da Res. CNJ 211/2015, a coordenação do macroprocesso governança e gestão de TIC[3] deve se dar, preferencialmente, com dedicação exclusiva, o que torna relevante a assunção, pela NGTIC, das atribuições do Escritório de Segurança da Informação, após sua extinção.

Ante a situação relatada, e a relevância da Governança de TIC para o TRT7, seja sob aspecto material (porte dos investimentos), seja sob o aspecto da criticidade, sugere-se a efetiva estruturação da unidade com mais servidores, bem como a avaliação da conveniência em reconstituição do Escritório de Segurança da Informação.

[3] Razão da criação do NGTIC.

IV. CONCLUSÃO

Concluídos os trabalhos de auditoria, na extensão definida no escopo, foram relacionadas sete constatações que expõem o grau de maturidade deste TRT7 no tocante à gestão de riscos de TIC, bem como do tratamento de incidentes de segurança da Informação.

1. Ausência de apuração dos indicadores relacionados ao Objetivo 3 (Implementar a gestão de Riscos de TI) do Plano estratégico de TIC - PETIC 2015-2020;
2. Ausência de plano de ação contendo cronograma para mapeamento dos riscos de processos;
3. Ausência de Plano de Continuidade de Serviços Essenciais de TI ou Gestão de Continuidade de TIC (Ato TRT7 n. 02/2017);
4. Descumprimento de periodicidade de reunião conjunta do CGSI (Comitê Gestor de Segurança da Informação) com a CSI (Comissão Permanente de Segurança de Informação);
5. Falta de ação institucional de sensibilização, conscientização e capacitação em Segurança da Informação de TIC;
6. Não cumprimento integral pelo NGTIC (Núcleo de Apoio à Gestão de TIC e Segurança da Informação) e pela ETIR (Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais) de suas atribuições, no que concerne ao ponto de controle "Tratamento de Incidentes de Segurança de TIC";
7. Falta de divulgação quanto ao procedimento para registro de incidentes de segurança de TIC.

Nesse contexto, foram propostas dez recomendações para o efetivo cumprimentos dos normativos vigentes, com vistas ao aprimoramento das ações e o consequente alcance de metas, notadamente em se tratando de área com elevados investimentos e consideráveis risco, além da dependência das ferramentas de TIC cada vez mais intensa nesta instituição.

Por oportuno, incluíram-se três breves descritivos no campo de informações, atinentes a fatos observados que, embora não constituam achados de auditoria, com a amplitude típica a eles atribuída, revelam deficiências formais com potencial desdobramento operacional, como, o desalinhamento de nomenclatura e atribuições de compartimentos deste órgão em atos e regulamento geral e a deficiência de estrutura do NGTIC.

Responsáveis pela elaboração:	
Adrienne Ramos Garcia Coordenadora de Serviço da SCGAP	**Anísio de Sousa Meneses Filho** Analista Judiciário – Esp. Eng. Civil
Data: 11/3/2019	

Responsáveis pela Coordenação:	**Aprovação e revisão:**
Adrienne Ramos Garcia Coordenadora de Serviço da SCGAP	**Ana Paula Borges de Araújo Zaupa** Secretária de Controle Interno
Data: 11/3/2019	**Data:**11/3/2019