JUSTIÇA DO TRABALHO
Tribunal Regional do Trabalho da 7ª Região (CE)
Secretaria de Controle Interno

RELATÓRIO DE AUDITORIA TRT7.SCI.GABIN Nº 11/2019

I. IDENTIFICAÇÃO	
Número do Processo	PROAD 5497/2019
Nº da Ordem de Serviço	TRT7.SCI.GABIN Nº 11/2019
Unidade Responsável pela Auditoria	Gabinete da Secretaria de Controle Interno
Unidade Auditada	TRT7 (órgãos relacionados a sua Política de Segurança da Informação e Comunicações (POSIC)
Tipo de Auditoria	Especial
Objeto da Auditoria	Avaliação da efetiva atuação do Comitê Gestor de Segurança da Informação (CGSI), em conformidade com a Resolução TRT7 278/2017

1. Introdução:

1.1. O presente Relatório apresenta os resultados da ação de controle de auditoria realizada no período de 12/8/2019 a 10/9/2019, na Sede do TRT 7ª Região, em cumprimento ao contido na Ordem de Serviço SCI.GABIN nº 11/2019, com o objetivo de contribuir para a melhoria da gestão e da governança de TIC, bem como atender a recomendação ao TRT7, promovida pela CCAUD/CSJT e referida no Despacho do Conselheiro-Relator de 25/10/2018, emitido no Processo MON-0001752-55.2018.5.90.0000:

> "4.2. recomendar ao TRT da 7ª Região que acompanhe, por meio de sua Unidade de Controle Interno: (...)
> 4.2.4. a efetiva atuação do CSGI, visando garantir o cumprimento da Resolução n.º 278/2017."

1.2. A avaliação se deu sobre a competência do CGSI e sua atuação, assim como sua interação com os demais órgãos que compõem a estrutura da Segurança da Informação do TRT7.

1.3. Os trabalhos foram conduzidos em estrita observância às normas de auditoria dispostas no Manual de Atividades do Controle Interno do TRT da 7ª Região e às aplicáveis ao Serviço Público Federal, tendo sido utilizadas as técnicas de análise documental e indagação escrita, não tendo sido imposta qualquer restrição a sua realização.

2. Escopo:

2.1. Os exames foram dirigidos às atas de reunião do Comitê Gestor de Segurança da Informação ocorridas entre outubro de 2018 e agosto de 2019 aos processos, assim como a documentos e às informações disponibilizadas pela Secretaria-Geral da Presidência, pelo Núcleo de Apoio à Gestão de Tecnologia da Informação e Comunicação e Segurança da Informação e pela própria Secretaria de

Tecnologia de Informação e Comunicação relacionadas ao objeto, e contemplaram os seguintes assuntos/ aspectos:

- Deliberações e reuniões do comitê (art. 12, *caput*, Res. 278/2017);
- Reuniões conjuntas com a Comissão de Segurança Institucional (art. 13, *caput*, Res. 278/2017);
- Interação entre os demais órgãos que compõem a estrutura Segurança da Informação no TRT7 e o CGSI (art. 8º, Res. 278/2017); e
- Competência do CGSI (normas correlatas).

3. Resultados dos Exames:

3.1. Os exames realizados resultaram na identificação das constatações listadas no título "Constatações" neste Relatório de Auditoria, juntamente com as respectivas recomendações corretivas e prazos estabelecidos para a adoção de providências.

3.2. No Quadro "Informação" é indicado registro para o qual a manifestação do auditado foi suficiente para descaracterizar necessidade de recomendações.

II. INFORMAÇÃO

II.1 Assunto/ Ponto de Controle: ATUAÇÃO DO CGSI - Deliberações e reuniões do Comitê de Gestão da Segurança da Informação

Informação nº 1 - Atuação efetiva do CGSI

Fato:

O Comitê Gestor de Segurança da Informação (CGSI) do TRT7 foi instituído pela Resolução TRT7 278/2017[1] e constituído mediante a Portaria TRT7.PRESI 366/2018 .

Em resposta a RDI, a SETIC informou a realização das seguintes reuniões do CGSI: nos dias 26/10/2018, 20/2/2019 e 27/8/2019, juntando as atas correspondentes (docs. 23, 25 e 26).

Manifestação do Auditado:

SETIC:

Em resposta à Questão 1 da RDI SCI.GABIN 1/2019, a Secretaria de Tecnologia da Informação e Comunicação informou que foram realizadas três reuniões, nos dias 26/10/2018, 20/02/2019 e 27/08/2019, e que o Comitê Gestor de Segurança da Informação está atuando na avaliação do processo de gestão de riscos de TIC, conforme se evidencia em e-mail apresentado.

Análise da Equipe:

As evidências coletadas atestam a efetiva atuação do CGSI.

III. CONSTATAÇÕES DE AUDITORIA

III.1 Assunto/ Ponto de Controle: ATUAÇÃO DO CGSI - Reuniões conjuntas com a Comissão de Segurança Institucional

[1] Que instituiu a Política de Segurança da Informação e Comunicações (POSIC), distinguindo-a da Política de Segurança Institucional e alterando a Resolução TRT7 313/2010.

Constatação nº 1 - Não realização de reuniões conjuntas com a Comissão de Segurança Institucional

Fato:

Em resposta a Requisição de Documentos e Informações, a SETIC informou a realização das seguintes reuniões do CGSI: nos dias 26/10/2018, 20/2/2019 e 27/8/2019, juntando as atas correspondentes (docs. 23, 25 e 26), mas nenhuma delas denota a realização de encontro conjunto com a Comissão de Segurança Institucional.

O Art. 13 da Res. TRT7 278/2017 dispõe que o CGSI se reunirá ordinariamente com a Comissão de Segurança Institucional, pelo menos duas vezes por ano, e de forma extraordinária, quando necessário.

Manifestação do Auditado:

SETIC:

Conforme resposta à Questão 2 da Requisição de Documentos e Informações SCI.GABIN 1/2019, foi proposta alteração do teor do artigo 13 à Presidência, nos termos dispostos no Proad 5807/2019:

> "Art. 13. O CGSI se reunirá ordinariamente pelo menos duas vezes por ano, e de forma extraordinária, quando se fizer necessário.
> § 1º As deliberações do CGSI serão consignados em ata e, quando implicar em acréscimo de despesas e/ou alteração no planejamento tático ou operacional de qualquer unidade administrativa ou judiciária, deverão ser encaminhadas à Presidência para aprovação."

Secretaria-Geral da Presidência: "embora essas reuniões não tenham ocorrido nos anos anteriores, há a pretensão de realizarmos essas reuniões ainda este ano."

Análise da Equipe:

O *caput* do artigo 13, em sua redação atual, refere reuniões ordinárias do CGSI com a Comissão de Segurança Institucional; o § 1º do mesmo artigo, por sua vez, dispõe que as deliberações do CGSI serão consignadas em ata e encaminhadas à Comissão de Segurança Institucional para aprovação.

No exercício de sua discricionariedade, pode a Administração alterar o normativo ao qual não tem sido dado cumprimento, se entender seu teor descabido.

Registre-se, entretanto, analisando o teor proposto, que substituir, na norma, uma instância interna de apoio à governança (Comissão Permanente) pela Presidência, integrante da Alta Administração, contribui para a centralização, em desprestígio à estrutura de governança definida pela Resolução TRT7 158/2018 (v. inciso IV de seu art. 16).

Mais coerente com a estrutura em tela seria a substituição por outro órgão também de apoio à governança, como o Comitê de Governança de Tecnologia da Informação e Comunicação, em consonância com a proposta de alteração do Ato TRT7.PRESI 148/2016, objeto do Proad 5981/2019.

Recomendação:

1. Avaliar a conveniência em, caso decida alterar o teor do artigo 13 da Resolução TRT7 278/2017, fazê-lo sem suprimir a submissão de determinadas deliberações do CGSI por órgão que constitua instância interna de apoio à governança, atentando ainda para alinhar

as propostas de alteração da Resolução e do Ato TRT7.PRESI 148/2016, objeto do Proad 5981/2019 .
Prazo: 90 dias.

III.2 Assunto/ Ponto de Controle: ATUAÇÃO DO CGSI - Interação entre o CGSI e demais órgãos que compõem a estrutura de Segurança da Informação no TRT7
Constatação nº 2 - Não encaminhamento das deliberações do CGSI à Comissão de Segurança Institucional
Fato: As deliberações constantes das atas das reuniões realizadas pelo Comitê Gestor de Segurança da Informação não foram encaminhadas à Comissão de Segurança Institucional, para aprovação, conforme disposto no § 1º do artigo 13 da Resolução TRT7 278/2017.
Manifestação do Auditado: **SETIC:** "Apesar das deliberações (atas) não terem sido formalmente encaminhadas ao Comissão de Segurança Institucional, vemos que, smj, tal encaminhamento não se fazia necessário, pois as ações, até o momento, são meramente operacionais, dando concretude ao planejamento de ações já presentes no PETI e no PDTIC (Gestão de Riscos, por exemplo) e não implicam em qualquer despesas adicional. - De qualquer forma, objetivando o aprimoramento do processo de trabalho e de conformidade, o Coordenador do CGSI sugeriu à Presidência a alteração do Art. 13 (PROAD 5807/2019)" **Secretaria-Geral da Presidência:** "nada a acrescentar, senão a manifestação do interesse em fazer cumprir a determinação."
Análise da Equipe: Aqui remete-se à análise da Constatação 1.
Recomendação: Para a presente constatação, é satisfatória a Recomendação 1.
Prazo: 90 dias.
Constatação nº 3 - Ausência de designação de gestor de segurança da informação interno
Fato: O Art. 15 do Decreto nº 9.637/2018, que instituiu a Política Nacional de Segurança da Informação, dispôs sobre a governança da segurança da informação e outras matérias, estabelece, em seus incisos I a X, diversas obrigações para os órgãos e entidades da Administração Pública Federal, no que concerne à matéria, dentre elas: "III - designar um gestor de segurança da informação interno, indicado pela alta administração do órgão ou da entidade;" Em pesquisa nos atos e portarias administrativos, não se constatou a designação de servidor para a posição em tela.
Manifestação do Auditado: **NGTIC/SETIC:** "Essa atribuição está consignada no Parágrafo único do Art. 10 da Política de Segurança da

Informação do TRT7 (Resolução n. 278/2017), reproduzido abaixo:

> "Art. 10. O ESI deve ser vinculado diretamente à Secretaria de Tecnologia da Informação, com estrutura organizacional e de pessoal compatíveis com o grau de responsabilidade e demanda.
>
> **Parágrafo único. Caberá ao Coordenador do ESI o papel de Gestor de Segurança da Informação e Comunicações.**" (grifo nosso)

http://www.trt7.jus.br/files/institucional/governanca_ti/seguranca_de_ti/RESOL_278-2017.pdf

Cabe destacar que o Escritório de Segurança da Informação, e naturalmente suas atribuições, foi incorporado ao 'Núcleo de Apoio à Gestão de TIC e Segurança da Informação' (Resolução 83/2018)."

Secretaria-Geral da Presidência: "nada a acrescentar em relação à manifestação da SETIC."

Análise da Equipe:

A designação para a função referida no inciso III do Art. 15 do Decreto nº 9.637/2018 não pode ser considerada válida se decorrente de disposição implícita ou objeto de dedução.

A rigor, da forma como consta nos normativos (art. 42 do Regulamento Geral, Resoluções TRT7 287/2017 e 83/2018), não há Gestor de Segurança da Informação designado, convindo a atualização da Resolução TRT7 278/2017.

Recomendação:

2. Avaliar a conveniência de atualizar a Resolução TRT7 278/2017, ante as alterações posteriores de estrutura da SETIC, deixando inequívoco a quem compete o encargo de Gestor de Segurança da Informação, sem prejuízo da designação pessoal em instrumento a parte (portaria, p.ex.).

Prazo: 120 dias.

III.3 Assunto/ Ponto de Controle: ATUAÇÃO DO CGSI - Competência do CGSI (normas correlatas)

Constatação nº 4 - Responsabilidades da Alta Administração - Governança da Segurança da Informação - desatualização dos normativos correspondentes

Fato:

O Art. 17 do Decreto nº 9.637/2018, que instituiu a Política Nacional de Segurança da Informação e dispôs sobre a governança da segurança da informação e outras matérias, estabelece:

> "Art. 17. Compete à alta administração dos órgãos e das entidades da administração pública federal a governança da segurança da informação, e especialmente:
>
> I - promover a simplificação administrativa, a modernização da gestão pública e a integração dos serviços públicos, especialmente aqueles prestados por meio eletrônico, com vistas à segurança da informação;
>
> II - monitorar o desempenho e avaliar a concepção, a implementação e os resultados da sua política de segurança da informação e das normas internas de segurança da informação;
>
> III - incorporar padrões elevados de conduta para a garantia da segurança da informação e orientar o comportamento dos agentes públicos, em consonância com as funções e as atribuições de seus órgãos e de suas entidades;
>
> IV - planejar a execução de programas, de projetos e de processos relativos à segurança da informação;
>
> V - estabelecer diretrizes para o processo de gestão de riscos de segurança da informação;

VI - observar as normas que estabelecem requisitos e procedimentos para a segurança da informação publicadas pelo Gabinete de Segurança Institucional da Presidência da República;
VII - implementar controles internos fundamentados na gestão de riscos da segurança da informação;
VIII - instituir um sistema de gestão de segurança da informação;
IX - implantar mecanismo de comunicação imediata sobre a existência de vulnerabilidades ou incidentes de segurança que impactem ou possam impactar os serviços prestados ou contratados pelos órgãos da administração pública federal; e
X - observar as normas e os procedimentos específicos aplicáveis, implementar e manter mecanismos, instâncias e práticas de governança da segurança da informação em consonância com os princípios e as diretrizes estabelecidos neste Decreto e na legislação.

§ 1º O planejamento e a execução de programas, de projetos e de processos relativos à segurança da informação de que trata o inciso IV do caput serão orientados para:
I - a utilização de recursos criptográficos adequados aos graus de sigilo exigidos no tratamento das informações e as restrições de acesso estabelecidas para o compartilhamento das informações, observada a legislação;
II - o aumento da resiliência dos ativos de tecnologia da informação e comunicação e dos serviços definidos como estratégicos pelo Governo federal;
III - a contínua cooperação entre as equipes de resposta e de tratamento de incidentes de segurança na administração pública federal direta, autárquica e fundacional e o Centro de Tratamento de Incidentes de Redes do Governo do Gabinete de Segurança Institucional da Presidência da República; e
IV - a priorização da interoperabilidade de tecnologias, processos, informações e dados, com a promoção:
a) da integração e do compartilhamento dos ativos de informação do Governo federal ou daqueles sob sua custódia;
b) da uniformização e da redução da fragmentação das bases de informação de interesse do Governo federal e da sociedade;
c) da integração e do compartilhamento das redes de telecomunicações da administração pública federal direta, autárquica e fundacional; e
d) da padronização da comunicação entre sistemas.

§ 2º O sistema de gestão de segurança da informação de que trata o inciso VIII do caput identificará as necessidades da organização quanto aos requisitos de segurança da informação e implementará o processo de gestão de riscos de segurança da informação." (grifamos)

A Resolução TRT7 158/2018, que instituiu a Política de Governança no âmbito do Tribunal Regional do Trabalho da 7ª Região, dispôs, § 2º do Art. 22:

"§ 2º A condução da Governança de TIC se dará, em primeira instância, pelo Comitê de Governança de Tecnologia da Informação e Comunicação (CGTIC)."

O Ato TRT7.PRESI 148/2016, que instituiu o Comitê de Governança de Tecnologia da Informação e Comunicação do Tribunal Regional do Trabalho da 7ª Região, por sua vez, estabeleceu a competência do CGTIC em seu Art. 2º:

omissis

Manifestação da Unidade Auditada:

NGTIC/SETIC:

"Foi proposto à Presidência a atualização do Ato n. 148/2016, por meio do PROAD 5981/2019. Além de outras mudanças, sugerimos a inclusão da seguinte competência ao CGTIC:

'VIII - Apreciar as ações sobre a gestão da segurança da informação no âmbito da 7ª Região, nas deliberações do Comitê Gestor de Segurança da Informação que importem em alocação de recursos de TIC de qualquer natureza, inclusão de novos

projetos ou serviços no portfólio de TIC ou necessidade de mudanças em priorizações de projetos;'

Cabe destacar que a Gestão da Segurança da Informação é de competência do CGSI, conforme definido no Art. 12 da Resolução n. 278/2017:

'Art. 12. Compete ao Comitê Gestor de Segurança da Informação (CGSI) deliberar sobre as ações voltadas a gestão da segurança da Informação no âmbito do TRT da 7ª Região, segundo os objetivos, os princípios e as diretrizes estabelecidos nesta Resolução e em normas complementares.'

Porém, smj, a proposta de inclusão da necessidade do Comitê de Governança de TIC deliberar sobre as ações de segurança da informação, nos casos em que se fizer necessário alocação de recursos e/ou alterações de prioridades, busca harmonizar essas competências posto que concorrem nos mesmos recursos (humanos e financeiros)."

Secretaria-Geral da Presidência: "nada a acrescentar em relação à manifestação da SETIC."

Análise da Equipe:

O Art. 17 do Decreto nº 9.637/2018 elenca competências da Alta Administração, as quais, smj, podem ser exercidas diretamente ou por meio de uma de suas instâncias internas de governança, como é o caso do Comitê de Governança de TIC.

A alteração proposta se afigura satisfatória, em seu teor.

É importante, entretanto, que Administração avalie a conveniência em se normatizar endossando a essência de competências relevantes indicadas no Decreto nº 9.637/2018, como por exemplo o encargo delineado em seu inciso II, de *monitorar o desempenho e avaliar a concepção, a implementação e os resultados da sua política de segurança da informação e das normas internas de segurança da informação*, seja diretamente à Alta Administração, seja a instância interna de governança.

Recomendações:

3. Atualizar o Ato TRT7.PRESI 148/2016, no que concerne à competência do Comitê de Governança de Tecnologia da Informação e Comunicação.
4. Avaliar a conveniência e oportunidade de normatizar sobre competências relevantes indicadas no art. 17 do Decreto nº 9.637/2018, seja diretamente à Alta Administração, seja a instância interna de governança.

Prazo: 90 dias

IV. CONCLUSÃO

Concluídos os trabalhos de auditoria, na extensão definida no escopo, seguem relacionadas as constatações apuradas:

Constatação nº 1 - Não realização de reuniões conjuntas com a Comissão de Segurança Institucional

Constatação nº 2 - Não encaminhamento das deliberações do CGSI à Comissão de Segurança Institucional

Constatação nº 3 - Ausência de designação de gestor de segurança da informação interno

Constatação nº 4 - Responsabilidades da Alta da Administração - Governança da Segurança da Informação - desatualização dos normativos correspondentes.
Para saneamento das impropriedades, formularam-se as seguintes **recomendações**:

1. Avaliar a conveniência em, caso decida alterar o teor do artigo 13 da Resolução TRT7 278/2017, fazê-lo sem suprimir a submissão de determinadas deliberações do CGSI por órgão que constitua instância interna de apoio à governança, atentando ainda para alinhar as propostas de alteração da Resolução e do Ato TRT7.PRESI 148/2016, objeto do Proad 5981/2019. (Prazo de 90 dias)
2. Avaliar a conveniência de atualizar a Resolução TRT7 278/2017, ante as alterações posteriores de estrutura da SETIC, deixando inequívoco a quem compete o encargo de Gestor de Segurança da Informação, sem prejuízo da designação pessoal em instrumento a parte (portaria, p.ex.). (Prazo de 120 dias)
3. Atualizar o Ato TRT7.PRESI 148/2016, no que concerne à competência do Comitê de Governança de Tecnologia da Informação e Comunicação. (Prazo de 90 dias)
4. Avaliar a conveniência e oportunidade de normatizar sobre competências relevantes indicadas no art. 17 do Decreto nº 9.637/2018, seja diretamente à Alta Administração, seja a instância interna de governança. (Prazo de 90 dias)

Conclui-se que a atuação do Comitê Gestor de Segurança da Informação (CGSI) deste Tribunal está em conformidade, em todos os aspectos relevantes, com as normas aplicáveis, ressalvados os tópicos apontados neste Relatório e a conveniência de atualização normativa.

Responsável pela Elaboração e Aprovação:
Ana Paula Borges de Araújo Zaupa
Secretária de Controle Interno

Data: 10/9/2019