RELATÓRIO DE AUDITORIA SOBRE A GESTÃO DE SEGURANÇA DA INFORMAÇÃO EXECUTADA PELA ÁREA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - TIC.

JULHO
2018

RELATÓRIO DE AUDITORIA N.8/2018- CCI

1. INTRODUÇÃO:

Em cumprimento ao disposto na Resolução CNJ n. 171/2013, bem como ao estabelecido no subitem 17 do item II do Anexo do Plano Anual de Ações de Controle para o exercício de 2018, aprovado pelo Ato n. 104/GP/TRT19ª, de 21 de novembro de 2017, apresentam-se os resultados da Auditoria Interna sobre a Gestão de Segurança da Informação e Comunicação, realizados pelo Tribunal Regional do Trabalho da 19ª Região, no período entre 5 fevereiro de 2018 e 20 de abril de 2018.

2. OBJETIVO:

O presente Relatório tem como finalidade demonstrar o resultado da Auditoria Interna sobre a Gestão de Segurança da Informação e Comunicação do TRT19ª Região, a qual foi realizada mediante a observância do cumprimento das normas vigentes, considerando a necessidade da implementação de uma política de segurança da informação e comunicação no âmbito deste Regional com o intuito atender as diretrizes da Resolução CNJ n. 211/2015.

3. ESCOPO:

Conforme a Matriz de Planejamento elaborada pela equipe de auditoria, foram evidenciadas sete questões de auditorias, a seguir descritas:

Q1. Existe uma Política de Segurança da Informação (SI) formalmente aprovada e em vigor?

Q2. Existe um Comitê de Segurança da Informação formalmente instituído que atua de acordo com os requisitos estabelecidos na legislação pertinente?

Q3. Foi definido formalmente um processo de Gestão de Riscos de Segurança da Informação e Comunicação - GRSIC quanto à análise de riscos de TI?

Q4. Há um Plano de Continuidade de Serviços Essenciais de TI, com intuito de assegurar que a organização possua mecanismos sistematizados de retorno à normalidade em casos de incidentes?

Q5. Estão formalmente instituídos os processos de gestão da segurança da TI neste Regional?

Q6**.** O Processo de Gestão de Ativos de TIC está sendo implementado de acordo com as diretrizes internas?

Q7. O Centro de Processamento de Dados (CPD) ou *Data Center* deste Tribunal Regional do Trabalho da 19ª preenche os requisitos exigidos na legislação pertinente que rege a Segurança das Informações?

4. TÉCNICAS DE AUDITORIA:

As investigações foram feitas mediante a aplicação das seguintes técnicas de auditoria:

4.1. Entrevista: Formulação de perguntas escritas, no formato de Requisições de Documentos e Informação - RDI, para a unidade administrativa auditada, para obtenção de dados e informações.

4.2. Exame dos Registros: Verificação se os dados e informações relacionados à gestão das segurança da informação, nos campos "Contas Públicas" e "Portal da Transparência", foram registrados adequadamente no sítio eletrônico deste Regional, nos termos da legislação vigente.

4.3. Inspeção física: Realização de exame in loco no dia 01/03/2018 nos seguintes lugares:

* 1º andar do Anexo II deste Regional, onde está localizado os Setores de Infraestrutura e Banco de Dados, além do Centro de Processamento de Dados (CPD) ou *Data Center;*

* pavimento Térreo do Edifício Sede Pontes de Miranda (onde está localizada a Sala Segura).

4.4. Correlação das Informações Obtidas: Correlação das informações obtidas na Requisição de Informação (RDI) com aquelas apuradas durante a inspeção física no ambiente do *Data Center* e na Sala Segura.

5. PARÂMETROS NORMATIVOS E JURISPRUDENCIAIS:

- Princípio da Continuidade dos Serviços Públicos;
- Lei n. 7.783/89 (processamento de dados ligados a serviços essenciais);
- Lei n. 8.078/90 (fornecimento de serviços essenciais);
- Instrução Normativa GSI/PR 1/2008;
- Norma Complementar 3/IN01/DSIC/GSIPR (DIRETRIZES DA POLÍTICA DE SIC);
- Norma Complementar n. 04/IN01/DSIC/GSIPR – Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC;
- Norma Complementar 6/IN01/DSIC/GSIP - Gestão de Continuidade de Negócios em Segurança da Informação e Comunicações;
- Norma Complementar n. 10/IN01/DSIC/GSIPR – Inventário e Mapeamento de Ativos de Informação nos Aspectos Relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal;
- ABNT NBR ISO 27002:2013 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para controles de segurança da informação;
- ABNT NBR ISO 27005:2011 – Tecnologia da Informação – Técnicas de Segurança – Gestão de riscos de segurança da informação;
- ABNT NBR 15999 (Gestão de Continuidade de Negócios);
- ABNT NBR 15247;
- COBIT 5, item APO12 - Manage Risk;
- COBIT 5, item DSS04 (Manage Continuity);
- COBIT 5, item DSS01.05 - Manage facilities;
- Acórdão TCU n. 71/2007 – Plenário;
- Acórdão TCU n. 1.233/2012 – Plenário;
- Acórdão CSJT-A-1453-83.2015.5.90.0000;
- Resolução CNJ n. 211/2015;
- Resolução Administrativa TRT 19ª TP n.12/2008;
- ATO TRT19ª GP n. 66/2017.

6. DOS ACHADOS DE AUDITORIA E DAS RECOMENDAÇÕES:

Seguindo as diretrizes prescritas pela Resolução CNJ n. 171/2013, foram encontrados, os ACHADOS DE AUDITORIA, que são atos ou fatos em desconformidade com a legislação aplicada ao caso, dignos de serem reportados pelos auditores.

Visando otimizar as atividades administrativas, objeto da presente auditoria interna, encaminhamos o Relatório Preliminar para as unidades auditadas - Diretoria Geral (DG) e Secretaria de Tecnologia e das Comunicações (SETIC) -, através dos Mem. n. 17/2018/C.C.I., respectivamente, protocolado no PROAD sob n. 1.427/2018. As unidades auditadas se manifestaram e apresentaram plano de ação no referido processo.

Para cada um desses Achados são identificados os pontos abaixo:

- **SITUAÇÃO ENCONTRADA:** Situação existente, identificada e documentada durante a fase de execução do trabalho.
- **CRITÉRIO:** Legislação, jurisprudência, princípios ou, ainda, padrões e boas práticas que a equipe compara com a situação encontrada. Reflete como deveria ser a gestão.
- **EVIDÊNCIA:** Informações obtidas durante a execução dos trabalhos no intuito de documentar os achados e de respaldar as opiniões e conclusões da equipe, podendo ser classificadas como físicas, testemunhais, documentais e analíticas.
- **CAUSA:** O que, possivelmente, motivou a ocorrência do achado.
- **EFEITOS / RISCOS:** Consequências ou possíveis consequências do achado, que possam dificultar o alcance dos objetivos.
- **RECOMENDAÇÕES:** Providências indicadas pela Unidade de Controle Interno com o intuito de aperfeiçoar os controles internos da unidade auditada, com vistas a corrigir falhas detectadas, cuja gravidade possa repercutir em eventos futuros e evitar a sua repetição, demandando da Administração pronta ação ou correção.

ACHADO DE AUDITORIA	**A.1**
DESCRIÇÃO DO ACHADO:	**Falhas na divulgação da Política de Segurança da Informação e Comunicação (SIC).**

SITUAÇÃO ENCONTRADA:

Conforme pesquisa no Boletim Interno deste Tribunal, bem como através da resposta concedida pela unidade auditada à RDI CCI n. 01/2018, constatou-se, à época, que não houve atualização da RA TP n.12/2008, no que concerne à Política de Segurança da Informação e Comunicações (SIC) deste Tribunal, para atender às diretrizes da Resolução n. 211/2015 do Conselho Nacional de Justiça e para cumprir as determinações do Conselho Superior da Justiça do Trabalho proferidas no Acórdão CSJT-A-1453-83.2015.5.90.0000.

Nesse aspecto, cumpre observar que o art. 9º da Resolução n. 211/2015 do CNJ preceitua que:

> *"Cada órgão deverá elaborar e aplicar política, gestão e processo de segurança da informação a serem desenvolvidos em todos os níveis da instituição, por meio de um Comitê Gestor de Segurança da Informação, e em harmonia com as diretrizes nacionais preconizadas pelo Conselho Nacional de Justiça"*

Por sua vez, viando concretizar a diretriz acima transcrita, o Conselho Superior da Justiça do Trabalho, ao realizar auditoria da área de Tecnologia da Informação, determinou no Acórdão CSJT-A-1453-83.2015.5.90.0000 ao TRT da 19ª Região:

> *" 8. Aperfeiçoe seu sistema de gestão de segurança da informação, o qual deve incluir (achado 2.18):*
> *8.1. Em até 90 dias, a contar da ciência desta deliberação, revisão da Política de Segurança da Informação, contemplando as referências legais e normativas que basearam sua elaboração, as diretrizes gerais sobre, no mínimo, os temas enumerados na Norma Complementar 3/IN01/DISC/GSIPR e os previstos na própria política de segurança da informação do Tribunal e a definição da periodicidade de sua revisão;*
> *8.2. Em até 90 dias, a contar da ciência desta deliberação, processo de gestão de riscos, que contenha, pelo menos: lista de riscos; avaliação dos riscos identificados por meio da probabilidade e impacto; priorização dos riscos para tratamento; e metodologia para a gestão dos riscos;*
> *8.3. Em até 180 dias, a contar da ciência desta deliberação, plano de continuidade de TI para os principais serviços, contendo, no mínimo: a definição dos papéis e responsáveis, condições para ativação, procedimentos a serem adotados e detalhes de comunicação;*
> *8.4. Em até 180 dias, a contar da ciência desta deliberação, processo de monitoramento e tratamento de incidentes de segurança da informação, principalmente no que diz respeito à observação da política de segurança da informação instituída pelo Tribunal. 9. Implante, em até 90 dias, a contar da ciência desta deliberação, unidade dedicada à gestão de segurança da informação no âmbito do Tribunal (achado 2.20)"*

Diante do Relatório Preliminar apresentado por esta Coordenadoria de Controle Interno na presente auditoria, a SETIC providenciou houve a atualização da Política de Segurança da Informação e Comunicação junta a Presidência deste Tribunal, através do Ato

TRT19ª GP n. 45/2018. Todavia, observa-se que não houve a promoção de ações de conscientização, educação e treinamento em Segurança da Informação para os servidores deste Tribunal, o que se mostra imprescindível para assegurar a efetividade da política instituída pelo referido Plano no âmbito deste Tribunal.

CRITÉRIO:	- Instrução Normativa GSI/PR 1/2008, art. 5º, VII; - Norma Complementar 3/IN01/DSIC/GSIPR (DIRETRIZES DA POLÍTICA DE SIC); - NBR-ISO/IEC 27.002 - Itens 5.1 e 5.1.2 (Revisão da Política); - Resolução CNJ n. 211/2015; - Acórdão CSJT-A-1453-83.2015.5.90.0000.
EVIDÊNCIA:	- RA TP n.12/2008 disponível no Boletim Interno deste Tribunal; - Resposta à RDI CCI n. 01/2018 pela unidade auditada; - ATO TRT19ª GP n. 45/2018 disponível no Boletim Interno deste Tribunal.
CAUSA:	- Falhas no processo de gestão de segurança da informação.
EFEITOS/RISCOS:	- Risco de comprometer a melhoria da infraestrutura e governança de Tecnologia da Informação e Comunicação deste Tribunal por falta de efetividade da Política instituída. - Risco nos procedimentos de segurança da informação e consequente impacto nos processos de negócio do TRT19.
ENCAMINHAMENTO / RECOMENDAÇÕES:	Recomenda-se, diante da recente aprovação da nova Política de Segurança da Informação e Comunicação, ocorrida em 21 de maio de 2018, através do Ato TRT19ª GP n. 45/2018, que o Tribunal promova ações de conscientização, educação e treinamento em Segurança da Informação para os servidores deste Tribunal, visando sua efetividade.

ACHADO DE AUDITORIA	**A.2**
DESCRIÇÃO DO ACHADO:	**Falhas na composição e atuação do Comitê Gestor de TI.**

SITUAÇÃO ENCONTRADA:

O ATO n. 169/GP/TRT 19ª, de 22 de dezembro de 2016, ao estabelecer a composição do Comitê de Segurança da Informação, não indica quem exercerá a função de Gestor do Comitê, o que está em desacordo com o requisito contido no art. 7º da Instrução Normativa GSI/PR n. 1/2008 (documento em anexo), o qual dispõe:

> *"Ao Gestor de Segurança da Informação e Comunicações, de que trata o inciso IV do art. 5º, no âmbito de suas atribuições, incumbe:*
> *I - promover cultura de segurança da informação e comunicações;*
> *II - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;*
> *III - propor recursos necessários às ações de segurança da informação e comunicações;*
> *IV - coordenar o Comitê de Segurança da Informação e Comunicações e a equipe de tratamento e resposta a incidentes em redes computacionais;*
> *V - realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;*
> *VI - manter contato direto com o DSIC para o trato de assuntos relativos à segurança da informação e comunicações;*
> *VII - propor normas relativas à segurança da informação e comunicações.*

Em resposta à RDI CCI n. 01/2018, a unidade auditada informou que o Presidente do Comitê não exerce as funções de Gestor. Naquela oportunidade, acrescentou ainda que, na última auditoria realizada, o CSJT recomendou a criação de um Escritório de Segurança da Informação com atribuições semelhantes, porém o atual quadro da SETIC está muito reduzido, impossibilitando o cumprimento da recomendação.

Em relação às ações do referido Comitê, a unidade auditada informou que a atuação tem ocorrido com foco na garantia da infraestrutura de TIC adequada ao funcionamento dos Sistemas de TIC, porém não apresentou nenhum documento que pudesse comprovar a referida atuação.

CRITÉRIO:	- Instrução Normativa GSI/PR n. 1/2008, art. 5º, IV e art. 7º; - Norma Complementar 3/IN01/DSIC/GSIPR, item 5.3.7.3 (DIRETRIZES DA POLÍTICA DE SIC); - NBR-ISO/IEC 27.002, Item 6.1.2; - Resolução CNJ n. 211/2015, art. 9º.
EVIDÊNCIA:	- Resposta à RDI CCI n. 01/2018 pela unidade auditada
CAUSA:	- Falhas na governança de TI.

EFEITOS/RISCOS:	- Riscos de desalinhamento dos investimentos de Tecnologia da Informação com os objetivos do órgão; - Risco de o TRT não alcançar as metas definidas em seu PETIC.
ENCAMINHAMENTO / RECOMENDAÇÕES:	- Recomenda-se que o Presidente deste Regional designe o Gestor do Comitê de Segurança da Informação, na forma estabelecida na Instrução Normativa GSI/PR n. 1/2008, art. 5º, IV; -Recomenda-se ao Comitê de Segurança da Informação que apresente, periodicamente, documentos que comprovem a sua efetiva atuação, com o intuito de garantir a implementação das ações de segurança da informação.

ACHADO DE AUDITORIA	**A.3**
DESCRIÇÃO DO ACHADO:	**Inexistência de um processo formal de Gestão de Riscos de Segurança da Informação e Comunicação (GRSIC), com a análise dos riscos de TI.**
SITUAÇÃO ENCONTRADA:	
Verificou-se a inexistência de processo de formal de Gestão de Riscos de Segurança da Informação e Comunicação **(GRSIC)** no âmbito deste Tribunal. Em resposta à RDI CCI n. 01/2018, a unidade auditada informou que não há metodologia para a gestão dos riscos, com indicação de critérios de avaliação e de aceitação, formalmente implantada. Informou, ainda, que a referida metodologia encontra-se em elaboração considerando a agenda da política institucional estabelecida para gestão de riscos. Salienta-se que a Política de Gestão de Riscos e de Controles Internos deste Regional foi estabelecida através da Resolução Administrativa TRT19 TP n. 104/2016, a qual, em seu art. 9º, previu um prazo de 2 (dois) anos para que os gestores implantassem a Gestão de Risco nas suas unidades. Tal prazo somente irá expirar em outubro de 2018.	
CRITÉRIO:	- COBIT 5, item APO12 - Manage Risk; - Instrução Normativa GSI/PR 1/2008, art. 5º, VII; - Norma Complementar 4/IN01/DSIC/GSIPR, itens 6.1.1 e 6.1.12 (GESTÃO DOS RISCOS DE SIC - GRSIC); - NBR-ISO/IEC 27.002, item 4; - Resolução CNJ n. 211/2015, art. 12º, inciso II.
EVIDÊNCIA:	- Resposta à RDI CCI n. 01/2018 pela unidade auditada
CAUSA:	- Falhas na governança de TI.
EFEITOS/RISCOS:	- Risco nos procedimentos de segurança da informação e consequente impacto nos processos de negócio do TRT; - Indisponibilidade de serviços críticos de TI prejudicando as atividades estratégicas do TRT.
ENCAMINHAMENTO / RECOMENDAÇÕES:	Recomenda-se à Secretaria de Tecnologia da Informação e Comunicações do TRT da 19ª Região que cumpra as etapas necessárias para a implantação do processo formal de Gestão de Riscos de Segurança da Informação e Comunicação (GRSIC), mediante a análise dos riscos de TI.

ACHADO DE AUDITORIA	**A.4**
DESCRIÇÃO DO ACHADO:	**Ausência de Plano de Continuidade de serviços essenciais de TIC.**
SITUAÇÃO ENCONTRADA:	
Verificou-se a inexistência de Plano de Continuidade de serviços essenciais de TIC para os processos de negócio mais críticos do Tribunal. Em resposta à RDI CCI n. 01/2018, a unidade auditada informou que não há um Plano de Continuidade formalmente instituído, com o intuito de assegurar o retorno à normalidade, em casos de incidentes. O gestor da SETIC justifica que não há um número suficiente de servidores especializados na unidade de TIC para elaborar e implementar o referido Plano. Informa. todavia, que já comunicou à Presidência deste Regional a necessidade de lotação de mais servidores naquela Secretaria.	
CRITÉRIO:	- Princípio da Continuidade dos Serviços Públicos; - Art. 10, inciso IX, Lei n. 7.783/89 (processamento de dados ligados a serviços essenciais); - Art. 22 da Lei n. 8.078/90 (fornecimento de serviços essenciais); - Acórdão n. 71/2007-TCU-Plenário, item 9.2.14; - COBIT 5, item DSS04 (Manage Continuity); - COBIT 5, itens DSS 4.03, 4.04, 4.05 e 4.06; - Instrução Normativa GSI/PR 1/2008, art. 5º, VII; - Norma Complementar 6/IN01/DSIC/GSIP; - Resolução CNJ n. 211/2015, art. 10º, §2º; art. 12º, inciso II.
EVIDÊNCIA:	- Resposta à RDI CCI n. 01/2018 pela unidade auditada
CAUSA:	- Falhas na governança de TI; - Falhas no processo de gestão de segurança da informação.
EFEITOS/RISCOS:	Indisponibilidade de serviços críticos de TI prejudicando as atividades estratégicas do TRT.
ENCAMINHAMENTO / RECOMENDAÇÕES:	Recomenda-se à Secretaria de Tecnologia da Informação e Comunicações do TRT da 19ª Região que elabore Plano de Continuidade de TI para os principais serviços, que deverá dispor sobre: a definição dos papéis e responsáveis, as condições para ativação, os procedimentos a serem adotados e os regramentos de comunicação.

ACHADO DE AUDITORIA	**A.5**
DESCRIÇÃO DO ACHADO:	**Inexistência de processos de gestão da segurança da informação da TI.**

SITUAÇÃO ENCONTRADA:

Verificou-se a inexistência de processos formalmente instituídos de gestão da segurança da informação que englobassem:

a) classificação e tratamento de informações, com controles que garantam a proteção adequada ao grau de confidencialidade e integridade de cada classe da informação;

b) riscos;

c) vulnerabilidades técnicas de TI;

d) monitoramento do uso dos recursos de TI; e

e) incidentes de segurança da informação.

Em resposta à RDI CCI n. 01/2018, a unidade auditada informou que não há processos formalmente instituídos de gestão da segurança da informação, em razão do número insuficiente de servidores especializados na SETIC.

CRITÉRIO:	- Norma Complementar 3/IN01/DSIC/GSIPR (DIRETRIZES DA POLÍTICA DE SIC); - NBR-ISO/IEC 27.002, item 5; - NBR-ISO/IEC 27.005, item 8; - Acórdão do TCU n. 1.233/2012 - Plenário; - Resolução CNJ n. 211/2015.
EVIDÊNCIA:	- Resposta à RDI CCI n. 01/2018 pela unidade auditada.
CAUSA:	- Incipiência da cultura organizacional no que diz respeito ao tema Segurança da Informação; - Falhas no processo de gestão de segurança da informação.
EFEITOS/RISCOS:	Indisponibilidade de serviços críticos de TI prejudicando as atividades estratégicas do TRT;
ENCAMINHAMENTO / RECOMENDAÇÕES:	Recomenda-se à Secretaria de Tecnologia da Informação e Comunicações do TRT da 19ª Região que providencie a formalização dos principais processos na gestão da segurança da informação, os quais devem assegurar a confidencialidade e integralidade das informações, além do monitoramento do uso dos recursos de TI e dos incidentes de segurança da informação.

ACHADO DE AUDITORIA	**A.6**
DESCRIÇÃO DO ACHADO:	**Inexistência de um Inventário de Ativos de TIC.**

SITUAÇÃO ENCONTRADA:

Verificou-se que neste Tribunal não há Inventário de Ativos de TIC contendo, no mínimo:

a) a descrição do ativo;

b) configurações de *hardware*;

c) versões de *software*;

d) localização e,

e) quando pertinente, sua criticidade ou relevância (considerando os serviços e sistemas que ele suporta);

f) gestão das licenças de *softwares* nas quantidades e versões efetivamente instaladas; (onde estão localizadas).

Em resposta a RDI CCI n. 01/2018, a unidade auditada informou que não realizou o Inventário de Ativos, em razão do número insuficiente de servidores especializados na SETIC.

Quanto ao monitoramento dos ativos, o Sr. Secretário informou que está em fase de implantação, porém não mencionou nem comprovou o estágio em que se encontra.

CRITÉRIO:	- Instrução Normativa GSI/PR 1/2008, art. 5º, VII; - Norma Complementar 4/IN01/DSIC/ GSIPR, item 6.2.1 (GESTÃO DOS RISCOS DE SIC - GRSIC); - Norma Complementar 10/IN01/DSIC/ GSIPR; - NBR ISO/IEC 27.002, item 7.1 Responsabilidade pelos ativos; - ATO TRT19 GP n. 66/2017.
EVIDÊNCIA:	Resposta à RDI CCI n. 01/2018 pela unidade auditada.
CAUSA:	Falhas no processo de gestão de segurança da informação.
EFEITOS/RISCOS:	- Risco no processo de tomada de decisão acerca de novos investimentos; - - Risco da indisponibilidade de serviços críticos de TI, em razão da ausência de algum ativo de TI específico, prejudicando as atividades estratégicas do TRT; - Comprometimento da segurança dos ativos de TI, sem tratamento adequado e tempestivo.

ENCAMINHAMENTO / RECOMENDAÇÕES:	Recomenda-se à Secretaria de Tecnologia da Informação e Comunicações do TRT da 19ª Região que providencie: a) o Inventário de Ativos de TIC contendo: a descrição do ativo; configurações de hardware; versões de *software*; localização e, quando pertinente, sua criticidade ou relevância (considerando os serviços e sistemas que ele suporta); gestão das licenças de softwares nas quantidades e versões efetivamente instaladas; b) a implantação do monitoramento dos Ativos de TIC.

ACHADO DE AUDITORIA	**A.7**
DESCRIÇÃO DO ACHADO:	**Ausência de publicação no Portal do Tribunal do desenho do processo de Gestão de Configuração de Ativos de TIC.**

SITUAÇÃO ENCONTRADA:

Conforme pesquisa no Boletim Interno deste Tribunal, bem como através da resposta da RDI CCI n. 01/2018 enviada pela unidade auditada, constatou-se que não houve publicação no Portal do Tribunal do desenho do processo de Gestão de Configuração e Ativos de TIC.

Em sua resposta, a unidade auditada justificou que não efetuou a referida publicação, em razão da insuficiência de servidores especializados na SETIC.

Vale ressaltar que as diretrizes para subsidiar o processo de Gestão de Ativos foram elaboradas pela SETIC e formalmente regulamentadas através do Ato TRT 19ª GP n. 66/2017.

CRITÉRIO:	- Norma Complementar 4/IN01/DSIC/ GSIPR, item 6.2.1 (GESTÃO DOS RISCOS DE SIC - GRSIC); - Norma Complementar 10/IN01/DSIC/ GSIPR; - NBR ISO/IEC 27.002, item 7.1 Responsabilidade pelos ativos; - ATO TRT19 GP n. 66/2017.
EVIDÊNCIA:	- Boletim Interno deste TRT19; - Resposta à RDI CCI n. 01/2018 pela unidade auditada.
CAUSA:	Falhas no processo de gestão de Configuração e Ativos de TIC.
EFEITOS/RISCOS:	- Riscos no processo de tomada de decisão acerca de novos investimentos; - Comprometimento da segurança dos ativos de TI por se apresentar sem tratamento adequado e tempestivo;
ENCAMINHAMENTO / RECOMENDAÇÕES:	Recomenda-se à Secretaria de Tecnologia da Informação e Comunicações do TRT da 19ª Região que efetive a Política de Gestão de Ativos, formalmente aprovada em todos os seus aspectos, inclusive no tocante a publicação no Portal do Tribunal do desenho do processo de Gestão de Configuração de Ativos de TIC.

ACHADO DE AUDITORIA	**A.8**
DESCRIÇÃO DO ACHADO:	**Ausência da lista de atributos atualizada de todos os Ativos de TI, de forma a refletir a realidade e as necessidades específicas da SETIC e do Tribunal.**
SITUAÇÃO ENCONTRADA:	
Através da RDI n. 01/2018, foi questionou-se se há da lista de atributos atualizada de todos os Ativos de TI, que discrimine a realidade e as necessidades específicas da unidade auditada e do Tribunal. Em resposta, a unidade auditada informou que não mantém a lista de atributos atualizada em razão do quadro insuficiente de servidores.	
CRITÉRIO:	- Instrução Normativa GSI/PR 1/2008, art. 5º, VII; - Norma Complementar 4/IN01/DSIC/ GSIPR, item 6.2.1 (GESTÃO DOS RISCOS DE SIC - GRSIC); - Norma Complementar 10/IN01/DSIC/ GSIPR; - NBR ISO/IEC 27.002, item 7.1 Responsabilidade pelos ativos; - ATO TRT19 GP n. 66/2017, item 4.1.7 do anexo único.
EVIDÊNCIA:	Resposta à RDI CCI n. 01/2018 pela unidade auditada.
CAUSA:	Falhas no processo de gestão de Configuração e Ativos de TIC.
EFEITOS/RISCOS:	- Indisponibilidade de serviços críticos de TI, prejudicando as atividades estratégicas do TRT; - Riscos de insatisfação dos usuários em relação aos serviços prestados pela área de TI.
ENCAMINHAMENTO / RECOMENDAÇÕES:	Recomenda-se à Secretaria de Tecnologia da Informação e Comunicações do TRT da 19ª Região que efetive a Política de Gestão de Ativos, formalmente aprovada em todos os seus aspectos, inclusive no tocante ao fornecimento de uma lista de atributos atualizada de todos os Ativos de TI, de forma a refletir a realidade e as necessidades específicas da SETIC e do Tribunal.

ACHADO DE AUDITORIA	**A.9**
DESCRIÇÃO DO ACHADO:	**Vulnerabilidades no mecanismo de proteção a falhas no fornecimento de energia ao ambiente do Centro de Processamento de dados (CPD) ou *Data Center* deste Regional.**

SITUAÇÃO ENCONTRADA:

Trata-se da análise dos procedimentos e planos adotados e executados pelo Tribunal Regional do Trabalho da 19ª Região, no tocante a segurança do Centro de Processamento de dados (CPD) ou *Data Center*. deste Regional.

Foi realizada uma Inspeção Física no 1º andar do Anexo II deste Regional onde está localizado os Setores de Infraestrutura e Banco de Dados, além do Centro de Processamento de Dados (CPD) ou *Data Center.*

Verificou-se que o ambiente do *Data Center* atende aos requisitos de acesso, monitoramento, distribuição de infraestrutura elétrica e lógica estabelecidos na legislação pertinente.

Para atender à necessidade de alimentação elétrica dos equipamentos e do ambiente é necessário realizar um cálculo dimensionando da utilização de dispositivos como: lâmpadas, cabo de energia, conectores, dijuntores e o quadro elétrico. Este cálculo deve levar em consideração também a expansão de alguns equipamentos.

A energia deve ser adequada, estabilizada e monitorada para que, em caso de queda ou falha no fornecimento, o sistema de redundância seja automaticamente acionado, com o intuito de gerenciar esse risco de falha de energia. O ambiente do *Data Center* deste Regional conta com dois *nobreaks* para estabilizar e alimentar o *Data Center,* até que o gerador de energia assuma seu papel de restabelecer a energia.

Por último, cumpre destacar que a região onde se localiza o Tribunal sofre constantemente com sucessivas falhas no fornecimento de energia (durante a inspeção física, que durou cerca de uma hora, houve três falhas) e que o gerador utilizado não atende somente ao *Data Center*, e sim a todo o Edifício do Anexo II.

Pelo exposto, conclui-se que a situação acima narrada representa uma vulnerabilidade quanto à segurança das informações contidas no Centro de Processamento de dados (CPD) ou *Data Center* deste Regional.

CRITÉRIO:	- COBIT 5, item DSS01.05 - Manage facilities; - ABNT NBR ISO/IEC 27002:2005; - ABNT NBR 15999 (Gestão de Continuidade de Negócios); - ABNT NBR 15247; - Instrução Normativa GSI/PR 1/2008, art. 5º, VII; - Subitem 6.2.2, alínea "b" da Norma Complementar n. 4/IN01/DSIC/GSIPR; - Resolução CNJ n. 211/2015, art. 24, inciso VII.
EVIDÊNCIA:	Informações coletadas no dia 01.3.2018 durante a Inspeção Física realizada no ambiente onde está localizado o Centro de Processamento de dados (CPD) ou *Data Center* deste Regional.

CAUSA:	Ausência de um gerador destinado, exclusivamente, para atender às necessidades quanto às falhas de fornecimento de energia elétrica no *Data Center.*
EFEITOS/RISCOS:	-Potencial risco de sobrecarga no único gerador existente, permitindo a interrupção do fornecimento de energia e, com isso, possibilitando afetar a integralidade dos dados processados pelo *Data Center* deste Regional; - Riscos na Gestão da Segurança da Informação.
ENCAMINHAMENTO / RECOMENDAÇÕES:	Recomenda-se à SETIC a instalação de um gerador que dê suporte, exclusivamente, ao ambiente do Centro de Processamento de Dados (CPD) ou *Data Center* deste Regional.

ACHADO DE AUDITORIA	**A.10**
DESCRIÇÃO DO ACHADO:	**Falhas quanto aos requisitos mínimos para a estrutura do ambiente *backup* (Sala Segura)**

SITUAÇÃO ENCONTRADA:

Trata-se da análise dos procedimentos e planos executados pelo Tribunal Regional do Trabalho da 19ª Região, no tocante à segurança das informações processadas no ambiente de *backup* (Sala Segura) deste Regional.

Em Inspeção Física, realizada em 01.03.2018, no pavimento Térreo do Edifício Sede Pontes de Miranda (onde está localizada a Sala Segura), verificou-se que o local atende, em parte, aos requisitos de acesso, monitoramento, distribuição de infraestrutura elétrica e lógica, estabelecidos na legislação pertinente.

Foram detectadas as seguintes impropriedades:

a) O acesso físico ao ambiente de backup (Sala Segura) não é registrado, nem controlado. Todavia, a "Sala Segura" é monitorada por duas câmeras de segurança;

b) Durante a Inspeção Física, verificamos a presença de materiais sem funcionamento depositados na Sala Segura, tais como: *nobreaks* em desuso, mesa, cadeira, caixas de fios. Ressaltamos, ainda, a existência de materiais inflamáveis em um ambiente que não conta com um sistema de proteção contra incêndios.

c) Não há sistema de controle de temperatura;

d) Não há sistema de detecção de fumaça;

e) Segundo o servidor Hermes Gustavo de Aquino, Chefe do Setor de Infraestrutura da SETIC, não são realizados com regularidade testes de funcionalidades. Porém, quando ocorre a interrupção parcial dos serviços executados no *Data Center,* os equipamentos da Sala Segura processam os dados, em uma qualidade inferior (o que é normal), porém não há descontinuidade do serviço.

CRITÉRIO:	- COBIT 5, item DSS01.05 - Manage facilities; - Instrução Normativa GSI/PR 1/2008, art. 5º, VII; - Subitem 6.2.2, alínea "b" da Norma Complementar n. 4/IN01/DSIC/GSIPR; - Resolução CNJ n. 211/2015, art. 24, inciso VIII.
EVIDÊNCIA:	Informações coletadas no dia 01.3.2018 durante a Inspeção Física realizada no ambiente onde está localizado a Sala Segura deste Regional.
CAUSA:	Ausência de procedimentos de controles internos, por parte da Administração, quanto aos requisitos exigidos na legislação pertinente, no tocante a preservação e condições de processamento da Sala Segura deste Regional.
EFEITOS/RISCOS:	- Riscos na Gestão da Segurança da Informação; - Indisponibilidade de serviços críticos de TI, prejudicando as atividades estratégicas do TRT.

ENCAMINHAMENTO / RECOMENDAÇÕES:	Recomenda-se à SETIC: a) a implantação de um controle de acesso à Sala Segura; b) que sejam acondicionados em outro local os materiais que possam afetar a segurança do ambiente, notadamente os inflamáveis; c) instalação de detector de fumaça e de controle de temperatura; d) a realização de testes de funcionalidade com mínima periodicidade, observados os requisitos de segurança.

7. CONSIDERAÇÕES EM FACE DA RESPOSTA DA UNIDADE AUDITADA

Inicialmente, esclarece-se que as auditorias desenvolvidas por esta Coordenadoria de Controle Interno seguem o rito processual estabelecido no Anexo II do Ato GP/TRT19ª n. 74/ 2014, o qual prevê a etapa do envio do Relatório Preliminar de Auditoria às unidades auditadas para manifestações, esclarecimentos, elucidações de erros, elaboração de um plano de ação, dentre outras possibilidades. Somente após a avaliação das respostas encaminhadas pelas unidades auditadas à Coordenadoria de Controle Interno, foi elaborado o presente Relatório Final de Auditoria.

As unidades Auditadas, Diretoria Geral Administrativo-Financeira e a Secretaria de Tecnologia da Informação de Comunicação, após tomarem conhecimento dos levantamentos inseridos no Relatório Preliminar, encaminharam a esta Coordenadoria o Documento n. 11 do PROAD n. 1.427/2018, contendo considerações acerca de cada um dos 10 (dez) Achados de Auditoria apontados no mencionado Relatório. Observa-se que o Documento apresentado pela contempla um Plano de Ação (anexo a este Relatório) com as medidas visando o cumprimento das recomendações firmadas.

Não obstante os esclarecimentos apresentados pela SETIC, verifica-se a necessidade da manutenção dos Achados supracitados, a fim de que haja aprimoramento da gestão administrativa no que diz respeito à Política de Gestão de Segurança da Informação no âmbito deste Tribunal.

8 - RECOMENDAÇÕES

8. 1. Recomenda-se, diante da recente aprovação da nova Política de Segurança da Informação e Comunicação, ocorrida em 21 de maio de 2018, através do Ato TRT19ª GP n. 45/2018, que o Tribunal promova ações de conscientização, educação e treinamento em Segurança da Informação para os servidores deste Tribunal, visando sua efetividade.

8.2. Recomenda-se que o Presidente deste Regional designe o Gestor do Comitê de Segurança da Informação, na forma estabelecida na Instrução Normativa GSI/PR n. 1/2008, art. 5º, IV;

8.3. Recomenda-se ao Comitê de Segurança da Informação que apresente, periodicamente, documentos que comprovem a sua efetiva atuação, com o intuito de garantir a implementação das ações de segurança da informação.

8.4. Recomenda-se à Secretaria de Tecnologia da Informação e Comunicações do TRT da 19ª Região que cumpra as etapas necessárias para a implantação do processo formal de Gestão de Riscos de Segurança da Informação e Comunicação (GRSIC), mediante a análise dos riscos de TI.

8.5. Recomenda-se à Secretaria de Tecnologia da Informação e Comunicações do TRT da 19ª Região que elabore Plano de Continuidade de TI para os principais serviços, que deverá dispor sobre: a definição dos papéis e responsáveis, as condições para ativação, os procedimentos a serem adotados e os regramentos de comunicação.

8.6. Recomenda-se à Secretaria de Tecnologia da Informação e Comunicações do TRT da 19ª Região que providencie a formalização dos principais processos na gestão da segurança da informação, os quais devem assegurar a confidencialidade e integralidade das informações, além do monitoramento do uso dos recursos de TI e dos incidentes de segurança da informação.

8.7. Recomenda-se à Secretaria de Tecnologia da Informação e Comunicações do TRT da 19ª Região que providencie:

a) o Inventário de Ativos de TIC contendo: a descrição do ativo; configurações de hardware; versões de software; localização e, quando pertinente, sua criticidade ou relevância (considerando os serviços e sistemas que ele suporta); gestão das licenças de softwares nas quantidades e versões efetivamente instaladas;

b) a implantação do monitoramento dos Ativos de TIC.

8.8. Recomenda-se à Secretaria de Tecnologia da Informação e Comunicações do TRT da 19ª Região que efetive a Política de Gestão de Ativos, formalmente aprovada em todos os seus aspectos, inclusive no tocante a publicação no Portal do Tribunal do desenho do processo de Gestão de Configuração de Ativos de TIC.

8.9. Recomenda-se à Secretaria de Tecnologia da Informação e Comunicações do TRT da 19ª Região que efetive a Política de Gestão de Ativos, formalmente aprovada em todos os seus aspectos, inclusive no tocante ao fornecimento de uma lista de atributos atualizada de todos os Ativos de TI, de forma a refletir a realidade e as necessidades específicas da SETIC e do Tribunal.

8.10. Recomenda-se à SETIC a instalação de um gerador que dê suporte, exclusivamente, ao ambiente do Centro de Processamento de Dados (CPD) ou Data Center deste Regional.

8.11. Recomenda-se à SETIC: a) a implantação de um controle de acesso à Sala Segura;

b) que sejam acondicionados em outro local os materiais que possam afetar a segurança do ambiente, notadamente os inflamáveis;

c) instalação de detector de fumaça e de controle de temperatura;

d) a realização de testes de funcionalidade com mínima periodicidade, observados os requisitos de segurança.

9 – CONCLUSÃO

A presente auditoria visou avaliar o conjunto de diretrizes, estruturas organizacionais, processos e mecanismos de controle que visam garantir que as decisões e as ações relativas à Gestão de Segurança da Informação executadas pela área de TIC deste Regional, a fim de que estejam alinhadas às necessidades da organização, contribuindo para o alcance das suas metas.

Dessa forma, as recomendações emanadas por esta Coordenadoria de Controle Interno têm, precipuamente, por objetivo assegurar o cumprimento das normas vigentes e a adoção de boas práticas na área da Segurança da Informação, mediante a observância dos princípios básicos da autenticidade, disponibilidade, integridade e confidencialidade.

Maceió, 16 de julho de 2018.

Eliana de Carvalho Souza
Líder da Equipe de Auditoria

Flávia Caroline Fonseca Amorim
Membro da Equipe de Auditoria

Rafaela de Freitas Santos
Supervisora de Equipe de Auditoria

10. PROPOSTA DE ENCAMINHAMENTO:

Ante o exposto, considerando o papel da auditoria interna preconizado no art. 74 da Constituição Federal, e com o intuito de auxiliar a Administração deste Regional no controle, eficiência e legalidade da gestão, submete-se o presente Relatório ao Exmo. Desembargador Presidente do Tribunal Regional do Trabalho da 19ª Região, a fim de que possa deliberar acerca dos resultados da presente Auditoria, realizada em face da gestão de Segurança da Informação executada pela área de Tecnologia da Informação e Comunicação, no âmbito do Tribunal.

Maceió, 25 de julho de 2017.

RAFAELA DE FREITAS SANTOS
Coordenadora do Controle Interno