2021

RELATÓRIO DE AUDITORIA

AUDITORIA EM SEGURANÇA DA INFORMAÇÃO - 2020
0002507-02.2020.6.03.8000
PORTARIA PRESIDÊNCIA Nº 273/2019 TRE-AP/PRES/CCI
(PUBLICADA NO DJE 214 DE 05 DE DEZEMBRO DE 2019)

SUMÁRIO

1. INTRODUÇÃO

O presente trabalho tem o objetivo de avaliar a conformidade do Processo de Segurança da Informação no âmbito do TRE-AP. Foi previsto no Plano Anual de Auditoria do ano de 2020, aprovado pela Portaria Presidência Nº 273/2019 TRE-AP/PRES/CCI/SEAUD. O objetivo esperado pela aplicação dos testes é avaliar a conformidade do Processo de Segurança da Informação no âmbito do TRE-AP.

Na presente análise, a atuação da equipe de auditoria foi pautada pelos princípios éticos presentes na NBC PG 100 - Aplicação Geral aos Profissionais da Contabilidade e o contido na NBC TI 01 – Da Auditoria Interna e na Resolução TRE-AP nº 482/2016.

Em âmbito global, a função da Auditoria está relacionada à verificação do cumprimento das obrigações, da execução dos programas de trabalho, da veracidade das informações geradas pela Contabilidade, bem como à prevenção de danos ou prejuízos ao Erário. São também preocupações da Auditoria, os controles de toda natureza mantidos pela Administração.

Segundo o IPPF[1]:

> *"A auditoria interna é uma atividade independente e objetiva de avaliação (assurance) e de consultoria, desenhada para adicionar valor e melhorar as operações de uma organização. Ela auxilia uma organização a realizar seus objetivos a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, controle e governança."*

Na concepção da *PricewaterhouseCoopers*, uma estrutura de auditoria interna forte e estratégica integra *compliance*, controles e um gerenciamento sofisticado de riscos à missão e visão da empresa e às expectativas dos *stakeholders*. Ela pode ajudá-lo a formular um novo paradigma de governança e riscos – antecipando problemas, aumentando a sua eficácia, eliminando duplicidades e identificando possíveis áreas de melhoria de desempenho.

Além disso, existe o dever funcional estampado na Constituição Federal, nas Leis nºs. 8.112/90 e 8.443/92, bem como os princípios da Administração Pública, quem devem ser seguidos por todo agente público na execução de suas atribuições.

[1] *Estrutura Internacional de Práticas Profissionais (IPPF) – Instituto dos Auditores Internos do Brasil.*

As análises realizadas obedeceram às normas legais e a correta aplicação dos procedimentos de Auditoria no Serviço Público Federal, com objetivo de emitir parecer sobre a regularidade da gestão de contratos de mão-de-obra terceirizada.

De acordo com o Regulamento da Secretaria, Resolução TRE-AP nº 406 de 16/05/2012, à Secretaria de Tecnologia da Informação compete:

Art. 53 [...]

I – orientar e supervisionar as unidades que lhe são subordinadas;

II – planejar e supervisionar as atividades relativas à área de gestão de tecnologia da informação, estabelecendo diretrizes, normas, critérios e programas adotados na execução dessas atividades;

III – subsidiar a elaboração dos relatórios de gestão e estatísticos;

IV – estabelecer as diretrizes a serem observadas quando da elaboração do planejamento das eleições, definindo as ações referentes à logística, treinamentos, sistemas eleitorais e orientações aos cartórios eleitorais;

V – subsidiar a elaboração das propostas orçamentárias do Tribunal, no que se refere às necessidades de contratação de serviços e de aquisição de material e equipamentos referentes às atividades informatizadas;

VI – pesquisar e propor a introdução de novas tecnologias, programas, normas e procedimentos para o aperfeiçoamento das atividades relativas à área de informática;

VII – apresentar projeto básico referente à contratação de serviços e aquisição de equipamentos, periféricos e acessórios de informática;

VIII – gerenciar as ações estratégicas a serem desenvolvidas.

2. ESCOPO/OBJETIVOS DA AUDITORIA/EXTENSÃO

Os trabalhos de auditoria buscaram avaliar a conformidade das operações internas com a Resolução TSE n° 23.501 e a Resolução do TRE-AP nº 510/2017, que dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral.

3. ESTRATÉGIA METODOLÓGICA E LIMITAÇÕES

Esta auditoria se utilizou das seguintes técnicas:

- ✓ Análise Documental e

✓ Verificação *in loco*.

4. POSSÍVEIS BENEFÍCIOS ESPERADOS

1. Aperfeiçoamento da Segurança de Informação no âmbito da Justiça Eleitoral do Amapá.

5. RELATÓRIO DETALHADO E PRINCIPAIS ACHADOS

Através da Matriz de Planejamento a Secretaria de Tecnologia da Informação foi requisitada a apresentar os documentos necessários para o início dos trabalhos de auditoria em 28/09/2020; a resposta do auditado foi enviada a Seção de Auditoria em 13/10/2020, tal manifestação gerou o Relatório Preliminar (SEI 0481413), o qual identificou possíveis achados e abriu prazo com a finalidade de manifestação do auditado. Esta última manifestação foi apresentada por meio do Despacho 786 (SEI 0501422).

Diante do testes e exames aplicados e das informações obtidas junto à Secretaria de Tecnologia da Informação, enumeramos os principais achados (o número das questões abaixo refere-se à Matriz de Planejamento):

Q2. Há indicação de responsável com atribuições claramente?

1º Achado	Critérios	Causa
Ausência de indicação de responsável com atribuições claramente definidas para cada ativo de informação e de processamento.	Art. 7º § único Resolução TSE nº 23.501/2016	Não observação do regramento interno

Efeito: Possíveis falhas de controle na gestão e na renovação dos contratos de permissão de utilização dos ativos.

Q4. A classificação da informação produzida ou custodiada pelo TRE-AP apresenta o grau de: confidencialidade, criticidade,	Critérios	Causa

disponibilidade, integridade e prazo de retenção?2º Achado		
A classificação das informações não possui uma ou todas as qualificadoras seguintes: confidencialidade, criticidade, disponibilidade, integridade e prazo de retenção.	Art. 11 Resolução TRE-AP nº 510/2017. Art. 9º Resolução TSE nº 23.501/2016.	Não atendimento do regramento da Justiça Eleitoral.

Efeito: Como não há classificação da informação, não existe um controle efetivo de quais e de que forma as informações devem ser protegidas.

Q5. Foi estabelecido e é revisado periodicamente, o processo de Gestão de Riscos de ativos de informação e de processamento do Tribunal, visando à identificação, avaliação e posterior tratamento e monitoramento dos riscos considerados críticos para a segurança da informação?

3º Achado	Critérios	Causa
Inexistência de um processo de gestão de riscos de ativos de informação aprovado.	Art. 15 Resolução TRE-AP nº 510/2017. Art. 13 Resolução TSE nº 23.501/2016.	Não atendimento do regramento da Justiça Eleitoral.

Efeito: O artigo 13 da Resolução 23.501/2016 dispõe que o Processo de Gestão de Riscos tem como finalidade identificar os riscos para posterior tratamento, logo, a inexistência do Processo impede ou pelo menos dificulta a identificação dos riscos que podem afetar a Organização.

Q6. Há plano de Continuidade de negócios testado e revisado periodicamente?

4º Achado	Critérios	Causa
Ausência de Plano de Continuidade de Negócios formalizado.	Art. 16 Resolução TRE-AP nº 510/2017. Art. 14 Resolução TSE nº 23.501/2016.	Não atendimento do regramento da Justiça Eleitoral.

Efeito: O referido Plano atua, conforme o art. 14 da Res. TSE 23.501/2016, no estabelecimento de procedimentos e definição de recursos com a finalidade do desenvolvimento de uma resiliência organizacional capaz de garantir o fluxo de

informações críticas em momento de crise e salvaguardar o interesse das partes interessadas, a reputação e a marca da organização, portanto, estes importantes objetivos são negligenciados gerando um possível descontrole das informações, o desatendimento do interesse das partes e a materialização de risco à reputação da Justiça Eleitoral.

6. CONCLUSÕES E RECOMENDAÇÕES

Diante dos resultados e das constatações desta Auditoria, sugerimos os seguintes procedimentos à administração:

I – Indicar, no sistema, em campo próprio, os responsáveis por cada ativo cadastrado (1º Achado);

II – Indicar servidor com conhecimento necessário do assunto para classificar as informações ou, na falta deste, contratar serviço de pessoa física ou jurídica especializada em classificação das informações na área de Tecnologia da Informação (2º Achado);

III – Providenciar a apresentação do Plano de Gestão de Riscos já escrito para aprovação e posterior implementação na rotina de trabalho das equipes de T.I.C (3º Achado).

IV – Priorizar o desenvolvimento do Plano de Continuidade dos Negócios para adequação e aperfeiçoamento do fluxo das informações (4º Achado).

Para fins de monitoramento, registra-se que a elaboração do **Processo de Tratamento e Resposta a Incidentes em Redes de Computadores**, cuja criação é determinada pelo Art. 15 da Resolução 23.501/2016, foi centralizada pelo TSE em conjunto com os demais regionais, logo as questões de auditoria *Q7* e *Q13* foi foram respondidas.

Sugerimos que as unidades competentes apresentem plano de ação com vistas ao monitoramento da implementação das recomendações.

É o relatório. À apreciação superior.

Macapá-AP, 02 de fevereiro de 2021.

Moisés Silva Campos
Chefe da Seção de Auditoria

Anderson Martins Mirabile
Assistente III