2022

RELATÓRIO DE AUDITORIA

AUDITORIA EM SEGURANÇA DA INFORMAÇÃO - 2022
0002029-23.2022.6.03.8000
PORTARIA-TSE Nº 761/2021
(PUBLICADA NO DJE 219 DE 26 DE NOVEMBRO DE 2021, PG.418)

SUMÁRIO

1. INTRODUÇÃO

O presente trabalho teve o objetivo de avaliar, no âmbito da Justiça Eleitoral do Amapá, o Processo de Gestão Segurança da Informação. Esta Auditoria foi prevista no Plano de Auditoria de Longo Prazo das Auditorias Integradas (PALP) 2022-2025, aprovado pela Portaria-TSE nº 761/2021.

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, que devem ser seguidos por todo agente público na execução de suas atribuições.

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 segurança da informação no âmbito da Justiça Eleitoral do Amapá.

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

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

A Auditoria Integrada da Justiça Eleitoral do ano de 2022 teve a finalidade de atuar em três pontos específicos da Segurança da Informação:

1. Gestão de Contas;
2. Gestão de Provedores e
3. Gestão de Controle de Acesso

Para tanto, foram selecionados como diretrizes os capítulos 5º, 6º e 15º do *CIS Controls V8*, um Framework de melhores práticas na matéria de gestão da segurança da informação.

3. ESTRATÉGIA METODOLÓGICA E LIMITAÇÕES

Esta auditoria se utilizou das seguintes técnicas:

- ✓ Análise Documental,
- ✓ Indagação,
- ✓ Inspeção e
- ✓ Verificação *in loco*.

4. POSSÍVEIS BENEFÍCIOS ESPERADOS

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

2. Prevenção de falhas na Segurança da Informação devido à falta ou deficiência de gestão de contas habilitadas nos sistemas internos.

3. Atualização ou criação de normativos internos em relação a matéria auditada.

4. Desenvolvimento de rotinas seguras de gestão de contas e de acesso aos sistemas críticos.

5. RESTRIÇÕES AOS TRABALHOS DE AUDITORIA

No levantamento dos sistemas críticos utilizados pelo Tribunal Regional Eleitoral do Amapá, foi identificado que a Secretaria de Tecnologia da Informação não detinha o controle de vários deles, como exemplo: SEI, SGRH, PJE, ODIN e ELO. Portanto, os testes foram focados naqueles softwares cujos mecanismos de segurança poderiam ser aperfeiçoados pela gestão deste próprio Tribunal.

Destaca-se que o SGRH apresenta duas falhas de segurança em seu acesso, a saber: aceita-se a inserção de senhas fracas e não é protegido com Autenticação de Multifator (MVA).

6. RELATÓRIO DETALHADO E PRINCIPAIS ACHADOS

Através do processo SEI de nº 0002029-23.2022.6.03.8000, Secretaria de Tecnologia da Informação foi requisitada a apresentar os documentos necessários para o início dos trabalhos de auditoria em 05/07/2022; ato contínuo, houve mais duas requisições de informações e um procedimento de teste *in loco*. A partir dos quais a Auditoria Interna do Tribunal Regional Eleitoral identificou os achados de auditoria que constam na lista abaixo:

1º Achado	Critérios	Causa	Efeito
Não há Política de gestão de provedores de serviço institucionalizada.	Medida de Segurança nº 15.2 do CIS v8	Ausência de estrutura organizacional que priorize a Segurança da Informação (art. 12º Resolução TRE/AP 570/2022)	Possíveis falhas na gestão de provedores.

2º Achado	Critérios	Causa	Efeito
Não há processo institucionalizado de verificação da execução contratual quanto aos aspectos de Segurança da Informação.	Medida de Segurança nº 15.6 do CIS v8	Ausência de estrutura organizacional que priorize a Segurança da Informação (art. 12º Resolução TRE/AP 570/2022)	Ausência de histórico dos prestadores de serviço que pode interferir em escolhas feitas em futuras contratações.

3º Achado	Critérios	Causa	Efeito
Não há processo institucionalizado de descredenciamento de servidores e colaboradores que são desligados do Tribunal.	Medida de Segurança nº 5.3 do CIS v8	Ausência de estrutura organizacional que priorize a Segurança da Informação (art. 12º Resolução TRE/AP 570/2022)	O usuário ativo do servidor que foi desligado do Tribunal pode ser utilizado para fins maliciosos.

4º Achado	Critérios	Causa	Efeito
O E-mail corporativo não utiliza MFA para acesso.	Medida de Segurança nº 6.5 do CIS v8	Falta de pessoal dedicado a Segurança da Informação e quadro reduzido de servidores da STI.	O E-mail institucional do TRE/AP possui serviços sensíveis a segurança da informação, como *OneDrive,* onde os arquivos institucionais são armazenados em nuvem. Somado a este risco, o E-mail também tem acesso pela internet. Logo, seria possível um acesso malicioso somente com a captura da senha de um usuário ativo.

5º Achado	Critérios	Causa	Efeito
Não há política de segurança institucionalizada para acesso ao *datacenter*	Boas práticas de gestão da segurança.	Ausência de estrutura organizacional que priorize a Segurança da Informação (art. 12º Resolução TRE/AP 570/2022)	Possível acesso indevido ao *DataCenter*.

7. CONCLUSÕES E RECOMENDAÇÕES

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

À STI/Alta Gestão:

I – Instituir Política Interna de Gestão de Provedores, inclusive incluindo no inventário de provedores de serviços uma ou mais características, como sensibilidade de dados, volume de dados, requisitos de disponibilidade, regulamentos aplicáveis, risco inerente e risco mitigado, conforme o item 15.3 do CIS v8. (**1º Achado**);

À STI:

II – Incluir, nos processos de acompanhamento dos contratos, um *cheklist* de verificação dos aspectos atinentes a Segurança da Informação (2º Achado);

III – Instituir mecanismo de controle de desligamento de servidores e colaboradores em geral dos quadros de pessoal do Tribunal, com vista à descredenciamento imediato de contas e acessos (**3º Achado**).

IV – Instituir mecanismo de multifator (MFA) para acesso ao E-mail corporativo pelos usuários. (**4º Achado**).

À Diretoria Geral:

V – Indicar os responsáveis pela informação sobre desligamento de servidores e colaboradores no processo citado no **item III** deste capítulo (**3º Achado**).

VI – Instituir estrutura desvinculada da STI com a finalidade de realizar a gestão estratégica da segurança da informação no âmbito do Tribunal Regional Eleitoral do Amapá, conforme o Art. 12 da Resolução TRE/AP n° 570/2022.

À STI e à Segurança Institucional:

VII – Elaborar política alinhada às melhores práticas de segurança da informação para acesso ao DataCenter deste Regional (**5º Achado**).

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, 17 de agosto de 2022.

Francisco Barros
Coordenador da Auditoria Interna
Supervisor da Auditoria

Moisés Silva Campos
Chefe da SAUD I
Coordenador da Auditoria

Anderson Martins Mirabile
Chefe da SAUD II
Coordenador da Auditoria