TRIBUNAL REGIONAL ELEITORAL DA PARAÍBA
Avenida Princesa Isabel, 201 - Bairro Centro - CEP 58020-911 - João Pessoa - PB

Relatório

RELATÓRIO FINAL DE AUDITORIA

SUMÁRIO EXECUTIVO

(Auditoria Integrada da Justiça Eleitoral: Processo de Gestão de Segurança da Informação).

1. APRESENTAÇÃO:

Este sumário executivo representa um resumo do Relatório de Auditoria dirigido aos gestores como forma de demonstrar sinteticamente os resultados do trabalho realizado pela equipe, sendo este composto apenas do objetivo, escopo e critério dos trabalhos, descrição do achado e conclusão, por questão de sigilo de informações consideradas sensíveis contidas na versão integral do relatório. Entretanto, salientamos que este sumário serve apenas como guia, por isso, não substitui o relatório completo, cuja leitura é recomendada, especialmente, pelos executores.

2. Objetivo

O avanço do protagonismo e o crescimento do valor da informação para o sucesso e bom funcionamento das organizações vem, nos anos recentes, promovendo o tema Segurança da Informação a um aspecto crítico, estratégico, para a boa prestação de serviço e a satisfação do público-alvo.

Relevante citar trechos do plano de trabalho da auditoria, também no sentido de demonstrar a importância do tema:

> "O objeto auditado, a cada dia, torna-se central na gestão das organizações, pois engloba a adoção de estratégias que devem se dar de modo organizado e planejado, com o propósito de proteger um ativo de importância singular: a informação. Nesse contexto, a cibersegurança é transversal, requerendo a implementação de diretrizes, políticas, práticas e protocolos, assim como a aderência a aspectos legais e a revisão de procedimentos técnicos.
>
> Diante desse cenário de riscos e ameaças, a Justiça Eleitoral é um dos principais alvos de ataques cibernéticos, em especial devido a sua crítica missão de liderar e organizar as etapas do processo eleitoral brasileiro, representando instrumento essencial da democracia. Considerando a proximidade das eleições de 2022, que apresenta um provável cenário político bastante polarizado, além de declarações polêmicas que

buscam ferir a imagem da Justiça Eleitoral, a temática da Segurança Cibernética no TSE se tornou ainda mais relevante".

No âmbito da Administração Pública, o protagonismo da Segurança da Informação se verifica, por exemplo, no Levantamento de Governança do TCU - Ciclo 2021, que aborda explicitamente esse tema nas questões referente às práticas "4240 - Gerir risco da Tecnologia da informação" (Questões 4241 e 4242), "4250 - Definir políticas de responsabilidades para a gestão da segurança da informação" (Questões 4251 a 4253) e "4260 - Estabelecer processos e atividades para a gestão da segurança da informação" (Questões 4261 a 4266).

Mais especificamente, ainda trazendo à seara do Poder Judiciário, o Levantamento de governança, gestão e infraestrutura de TIC do Poder Judiciário ano 2020, aborda o tema Segurança da informação 27 vezes, com destaque explícito à auditoria na questão do tema "Em relação a auditoria interna", ao indagar se "*a área de Auditoria Interna do órgão realiza, periodicamente, auditoria quanto a eficácia dos controles da Governança e da Gestão de TIC, inclusive nos aspectos relativos aos riscos afetos à segurança da informação, aos serviços judiciais e aos demais ativos de TIC críticos do órgão*".

No âmbito do TRE/PB, a gestão de processos em Segurança da Informação é objeto de atuação do Comitê de Governança de Segurança da Informação, Comitê Gestor de Segurança da Informação, Assessoria de Segurança da Informação (recém criada) e de alguns setores da Secretaria de Tecnologia da Informação e Comunicação (STIC), tais como: Coordenadoria de Apoio à Governança, Gestão de TIC e Segurança Cibernética, Seção de Apoio à Governança e Gestão de TIC e Seção de Segurança Cibernética; assim como da Equipe de Tratamento e Resposta de Incidentes de Segurança da Informação, os quais demandam e acompanham ações funcionais do Tribunal com o intuito de prover o melhor controle de riscos e ameaças relativos a exposição, acesso indevido e destruição de informações.

Pois bem. Após o conhecimento inicial do objeto auditado e, considerando as estruturas das unidades de auditorias, o fluxo de trabalho e o volume de trabalho das unidades clientes da auditoria, definiu-se o seguinte objetivo desta auditoria: avaliar o processo de Gestão de Segurança da Informação, utilizando como critério principal o framework CIS Controls (*The Center for Internet Security*), versão 8, nos seguintes pontos:

a. A existência e a qualidade dos controles internos instituídos no processo de gerenciamento de provedores de serviço e seus respectivos contratos, no tocante à segurança da informação, de modo que seja verificado o tratamento dos riscos que impactem o alcance dos objetivos;
b. A existência e a qualidade dos controles internos instituídos no processo de gestão de identidade e de controle de acessos aos ativos da organização, de modo que seja verificado o tratamento dos riscos que impactem o alcance dos objetivos;
c. Avaliar o alcance dos objetivos do processo quanto aos aspectos da eficiência, eficácia, economicidade e legalidade.

3. Critério de Auditoria

Neste trabalho foram utilizados como critério de auditoria, basicamente, as seguintes normas, modelo e Instrução Normativa:

1. *The Center for Internet Security* (CIS Controls) versão 8;
2. ITIL V4
3. Instrução Normativa SGM/ME 01.

4. Escopo

O escopo de auditoria, concebido pela Grupo de Trabalho de Auditoria, ficou assim definido:

> "Como retratado no Plano de Trabalho desta auditoria integrada, o framework utilizado como critério para a avaliação foi o The Center for Internet Security (CIS Controls) versão 8, tendo o controle 15 - Gestão de Provedores de Serviços - como principal. Segundo o CIS, o controle em questão incentiva o desenvolvimento de processo para avaliar os provedores de serviços que mantêm dados sensíveis, ou que são responsáveis por plataformas ou processos de TI críticos de uma organização, para garantir que esses provedores estejam protegendo as plataformas e os dados de forma adequada.
>
> Incidentalmente, os controles 5 e 6, que tratam, respectivamente, da Gestão de Contas e da Gestão do controle de Acesso, também são objeto de avaliação, pois possuem inter-relação direta com o controle 15. A gestão dos provedores de serviço envolve o gerenciamento da autorização de credenciais, bem como a utilização de processos e ferramentas para criar, atribuir, gerenciar e revogar credenciais de acesso e privilégios para contas de usuários, administradores e serviços em ativos e softwares corporativos, melhorando, assim, a segurança tecnológica da instituição".

5. Descrição dos achados

A1 DESCRIÇÃO DO ACHADO
Oportunidade de aprimoramento no processo de Gestão de Acessos à infraestrutura de TICs.

A2 DESCRIÇÃO DO ACHADO
Oportunidade de aprimoramento no processo de Gestão de Acessos à infraestrutura de TICs.

A3 DESCRIÇÃO DO ACHADO
Oportunidade de aprimoramento no processo de Gestão de Provedores de Serviços.

A4 DESCRIÇÃO DO ACHADO
Oportunidade de aprimoramento no processo de contratação e fiscalização de contratos de Soluções de TICs que exijam requisitos de Segurança da Informação.

4. CONCLUSÃO

A Auditoria Integrada no Processo de Gestão de Segurança da Informação, cujo resultados são apresentados neste relatório, ofereceu um esforço de observação e busca de aprimoramento em processos sensíveis a guarda, privacidade, integridade e acesso do conjunto de informações físicas e, sobretudo, digitais, custodiadas nas rotinas de trabalho executadas no âmbito do TRE-PB.

Evidências relativas a contratação de Solução de TIC´s, Gestão de Contas, Gestão de Acesso e Gestão de Provedores de Serviços foram analisadas sob a luz de referências consagradas na literatura e boas práticas para estas áreas no Brasil e no mundo.

O panorama geral encontrado atesta um inegável grau de maturidade de gestão nos processos observados, evidenciado por um volume considerável de práticas institucionalizadas, devidamente documentadas, apoiadas por regramentos internos e externos, assim como ferramental tecnológico dando suporte de automação e escalabilidade para os controles atuantes em riscos afetos a Segurança da Informação.

Foi verificado que há certo controle de acesso físico mediante registro da visita de prestador externo na recepção, com aprovação e/ou acompanhamento por servidor responsável (teste realizado com constatação positiva, de modo que não constou em qualquer achado).

No entanto, foram identificadas oportunidades de aprimoramento no decorrer da Auditoria, as quais são oferecidas como meio para melhorar os controles existentes, introduzir/iniciar algumas boas práticas, assim como potencializar a geração de registros e evidências que virão a prover melhores subsídios tanto para decisões de gestão, como para avaliação e respostas a eventuais incidentes de Segurança da Informação.

A exemplo da Auditoria anterior, mais ampla, realizada em 2019 sobre tema afeto (0007347-56.2019.6.15.8000), que se encontra em fase de monitoramento, a sinergia entre diferentes unidades e níveis de governança volta a ser um componente fundamental para o sucesso no cumprimento das recomendações sumarizadas a seguir. Tal cumprimento consiste em desdobramento fundamental para a obtenção dos benefícios perseguidos pela equipe de auditores e pela Secretaria de Auditoria Interna (SEAUDI) no exercício de seu mister.

É o sumário executivo do relatório.

JOSÉ AUGUSTO DE OLIVEIRA NETO
CHEFE DA SEÇÃO DE AUDITORIA - ÁREA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Documento assinado eletronicamente por JOSÉ AUGUSTO DE OLIVEIRA NETO em 19/08/2022, às 17:42, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-pb.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1341205** e o código CRC **A18CEEC3**.