TRIBUNAL REGIONAL ELEITORAL DE SANTA CATARINA

SECRETARIA DE CONTROLE INTERNO E AUDITORIA

AUDITORIAS INTEGRADAS DA JUSTIÇA ELEITORAL

RELATÓRIO DE AUDITORIA

PROCESSO DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Florianópolis/SC, agosto de 2022.

PREÂMBULO

Processo: PAE n. 17.745/2022 - Auditoria no Processo de Gestão de Segurança da Informação.

Atos originários: Plano de Auditoria Integrada de Longo Prazo 2022-2025 do TSE[1] e Plano Anual de Auditoria 2022 do TRE-SC[2].

Objetivo: Avaliar o processo de Gestão de Segurança da Informação, utilizando como critério principal o *framework CIS Controls*[3].

Período abrangido pela auditoria: Anos de 2021 a 2022.

Período de realização da auditoria: Planejamento: de 18 de maio a 29 de junho de 2022; Execução: de 30 de junho a 10 de agosto de 2022; Relatório: de 11 a 17 de agosto de 2022.

Unidade Auditada: Secretaria de Tecnologia da Informação (STI).

Ato de designação da equipe de auditoria: Termo de Designação (p. 3 dos autos).

[1] Disponível em: <https://www.tse.jus.br/transparencia-e-prestacao-de-contas/auditorias/arquivos/tse-palp-2022-2025-portaria-tse-no-761-2021>.

[2] Aprovado em 2.12.2021, com alterações posteriores aprovadas em 19.5.2022. Disponível em: <https://www.tre-sc.jus.br/transparencia-e-prestacao-de-contas/controle-interno/scia_arquivos/planos_atividades/TRE-SC-paa-2022-alterado>.

[3] *Center for Internet Security*. Controles CIS, Versão 8 (traduzido para o português). Disponível em <http://www.cisecurity.org/controls/v8>.

RESUMO

O presente trabalho é continuidade do projeto nominado “Auditorias Integradas da Justiça Eleitoral”, que teve início em 2017, tendo os Tribunais Regionais Eleitorais trabalhado conjuntamente, sob a coordenação central do Tribunal Superior Eleitoral (TSE), por sua Secretaria de Auditoria, avaliando temas críticos de forma padronizada e sistêmica, com o fito de aperfeiçoar a sua gestão e a própria sistemática de controle.

Para a Auditoria Integrada da Justiça Eleitoral 2022, o tema escolhido foi o processo de Gestão de Segurança da Informação, utilizando como critério principal o *framework CIS Controls*, versão 8.

Para tanto, foram seguidos o cronograma, a metodologia, os critérios, os papéis de trabalho padronizados, assim como demais procedimentos estabelecidos por aquela Corte Superior Eleitoral.

Considerando a metodologia de Auditoria Baseada em Riscos (ABR), foram levantados os principais riscos inerentes ao objeto da auditoria. A partir dos riscos identificados, foram definidos pelo TSE os testes de auditoria, a fim de verificar a existência e a efetividade dos controles associados àqueles riscos.

Após a execução dos testes, apresentação do Relatório Preliminar de Achados e respectiva resposta da Unidade Auditada, foram elaboradas as conclusões apontadas neste relatório, tendo restado 7 achados com propostas de encaminhamento, caracterizados conforme as normas técnicas aplicáveis ao processo de auditoria.

LISTA DE SIGLAS

ABR	Auditoria Baseada em Risco
CIS	*Center for Internet Security*
CNJ	Conselho Nacional de Justiça
CSC	Coordenadoria de Soluções Corporativas
CSIT	Coordenadoria de Suporte e Infraestrutura Tecnológica
DG	Direção Geral do TRE-SC
MFA	Múltiplo Fator de Autenticação
OTRS	Plataforma do Sistema de Gestão de Serviços do TRE-SC
PAE	Processo Administrativo Eletrônico
P	Presidência do TRE-SC
PSI	Política de Segurança da Informação
SAAGAAA	Seção de Acompanhamento e Avaliação da Gestão e Auditoria – Área Administrativa
SAU	Secretaria de Auditoria
SCIA	Secretaria de Controle Interno e Auditoria
STI	Secretaria de Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
TRE-SC	Tribunal Regional Eleitoral de Santa Catarina
TSE	Tribunal Superior Eleitoral

SUMÁRIO

I. INTRODUÇÃO

Em cumprimento à Resolução TSE nº 23.500/2016, que dispõe sobre as diretrizes acerca das Auditorias Integradas a serem efetuadas no âmbito da Justiça Eleitoral, assim como ao o Plano de Auditoria Integrada de Longo Prazo 2022-2025 do TSE, foi inserida no Plano Anual de Auditoria 2022 do TRE-SC a realização de exames de auditoria no processo de Gestão de Segurança da Informação, utilizando como critério principal o *framework CIS Controls*, versão 8, especificamente com relação aos Controles 5 – Gestão de Contas, 6 – Gestão do Controle de Acesso e 15 – Gestão de Provedor de Serviços, objetivando avaliar, em suma, a existência e a qualidade dos controles internos instituídos.

Inicialmente, a atividade estava prevista para iniciar em março de 2022. Entretanto, conforme consta nos Ofícios-Circulares GAB-SPR/GAB-PRES nº 234/2022 e SAU nº 277/2022 (pp. 89-104 do PAE n. 40.097/2021), o TSE necessitou alterar o cronograma da auditoria para o período de maio a agosto deste ano e, consequentemente, o Plano Anual de Auditoria 2022 do TRE-SC também foi retificado.

Com vistas à determinação dos objetivos e do escopo desta auditoria, tendo por base o Plano de Trabalho encaminhado pelo TSE, foi elaborado o Comunicado de Auditoria (pp. 04-06), onde constam ainda o cronograma e a requisição inicial de documentos e informações.

Em 19.5.2022, foi realizada a reunião de abertura da auditoria, quando o referido Comunicado de Auditoria foi apresentado à unidade auditada, tendo sido descrito o planejamento dos trabalhos, esclarecidas dúvidas acerca do objeto, extensão e critérios relacionados aos exames que seriam efetuados, assim como definido o interlocutor entre a Unidade Auditada e esta Unidade Técnica.

Encerrando a etapa de planejamento, foi elaborado o Programa de Auditoria em 4.7.2022 (pp. 56-62), conforme modelo disponibilizado pelo TSE, contendo os objetivos, o escopo, o período, a equipe e a metodologia da auditoria, além da Matriz de Planejamento dos Testes no seu anexo.

O Relatório Preliminar de Auditoria, com os achados resultantes dos testes aplicados, foi apresentado à unidade auditada em 3.8.2022, possibilitando aos gestores manifestação acerca do exposto, o que foi realizado tempestivamente, conforme documento de pp. 122-125.

A seguir, em tópicos específicos, os aspectos mais relevantes da auditoria em comento serão melhor explicitados.

II. VISÃO GERAL DO OBJETO AUDITADO

O objeto auditado consiste na Gestão de Segurança da Informação, especificamente com relação à gestão de provedores de serviços de TIC, gestão de contas e gestão do controle de acesso.

Consoante estabelecido no Regulamento Interno da Estrutura Orgânica do TRE-SC[4], atua como responsável nos processos relativos ao objeto desta auditoria a Secretaria de Tecnologia da Informação, em especial a Coordenadoria de Soluções Corporativas (CSC) e a Coordenadoria de Suporte e Infraestrutura Tecnológica (CSIT), respectivamente com as seguintes atribuições:

> Art. 127. À Coordenadoria de Soluções Corporativas compete:
> [...] II - administrar o portfólio de demandas por soluções tecnológicas, considerando as diretrizes de priorização definidas pela Administração;
> [...] VI - coordenar o planejamento e ações de governança de Tecnologia da Informação;
>
> [...]
>
> Art. 136. À Coordenadoria de Suporte e Infraestrutura Tecnológica compete:
> [...] IV - supervisionar a prestação de suporte técnico aos usuários de TI da rede de computadores da Justiça Eleitoral catarinense;
> [...] VI - supervisionar as atividades referentes à administração das políticas de segurança da informação da rede corporativa da Justiça Eleitoral catarinense;

Ademais, por meio da Portaria P n. 318/2017, foi instituída a Comissão de Segurança da Informação, assim como foram nomeados o Gestor da Comissão e Gestor da Segurança da Informação (Portaria DG n. 295/2017 e Portaria DG n. 26/2019).

[4] Resolução TRE-SC n. 7.930/2015: Aprova o Regulamento Interno da Estrutura Orgânica do TRE-SC. Disponível em: <http://apps.tre-sc.jus.br/site/legislacao/resolucoes/TRE-SC/2015/res-TRE-SC-7930-2015-regulamento-interno/index.html>.

O TRE-SC segue o que preconiza a Resolução TSE n. 23.644/2021, a qual dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral, não possuindo normas internas específicas relacionadas ao tema.

Os procedimentos executados relativos ao objeto não se encontram formalizados em manuais ou rotinas. O mapeamento do processo e a análise de riscos, realizados em conjunto com a Unidade Auditada, evidenciaram a existência de controles distribuídos ao longo das inúmeras atividades, em grande maioria manuais e de conformidade.

Quanto à **gestão de provedores de serviços de TIC**, são seguidas as normativas internas e orientações gerais sobre Governança de Contratações no TRE-SC[5]. Portanto, não existem critérios padronizados relacionados à segurança da informação, tanto no planejamento das contratações como na gestão dos contratos, sendo estabelecidos critérios específicos conforme a natureza de cada contratação.

Cabe ressaltar que, na reunião inicial com o provedor de serviços, as diretrizes que estarão em vigor no transcorrer da execução do contrato são repassadas de forma verbal, não havendo a prática de seu registro formal. Além disso, tampouco existe a obrigatoriedade contratual de assinatura de Termos de Confidencialidade e Sigilo por parte das empresas contratadas e respectivas(os) colaboradoras(es).

Os processos de **gestão de contas** e **gestão do controle de acesso**, são concomitantes. Para a criação de contas e acessos padronizados ([redacted]), há a necessidade de encaminhar um formulário de Ingresso de Colaborador pelo sistema [redacted] ao qual somente os gestores de pessoas possuem acesso. Pelo mesmo sistema, são encaminhados os formulários de Alteração de Lotação e Informação de Desligamento.

---

[5] Conforme orientações na página sobre Governança de Contratações na intranet do TRE-SC (http://intranet.tre-sc.gov.br/governanca-e-gestao/governanca-de-contratacoes) e as normas internas:

- Portaria P n. 93/2017: Política de Aquisições do TRE-SC;
- Portaria P n. 94/2017: processo formal de trabalho das aquisições do TRE-SC;
- Portaria P n. 95/2022: regramento dos processos de contratações de serviços no TRE-SC;
- Portaria P n. 67/2020: processo formal de trabalho para a Gestão de Contratos no TRE-SC;
- Portaria P n. 136/2021: apuração e aplicação de penalidades decorrentes de descumprimento parcial ou total das regras estabelecidas em edital de licitação e em contratos administrativos.

[redacted]

Para a concessão de acessos a serviços específicos, é necessário encaminhar uma solicitação via Sistema da Central de Serviços (OTRS), sendo solicitada aprovação do superior imediato e, conforme o caso, do gestor do sistema respectivo.

As contas ativas e os privilégios não são monitorados e revistos de tempos em tempos, somente quando é recebido o formulário Breve encaminhado pelo gestor. As contas possuem política de manutenção periódica [redacted]

[redacted]

Registra-se, por fim, que não houve, até a presente data, a realização de auditorias anteriores no processo de Gestão de Segurança da informação com enfoque na gestão de provedores de serviços de TIC, de contas e do controle do acesso, realizados por esta Unidade Técnica de auditoria. Tampouco esse mesmo tema foi objeto de auditoria por outro órgão interno do TRE-SC ou por outro órgão, entidade ou instituição externa, seja de controle ou não.

III. OBJETIVO DA AUDITORIA

Em atenção à orientação da Secretaria de Auditoria (SAU) do TSE, a presente auditoria teve por objetivo avaliar o processo de Gestão de Segurança da Informação, utilizando como critério principal o *framework CIS Controls*, 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;

[7] Informe na intranet do TRE-SC sobre "Medidas de Segurança da Informação". Disponível em: <http://intranet.tre-sc.gov.br/busca/noticias-e-informes/medidas-de-seguranca-da-informacao>.

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.

IV. ESCOPO E AMOSTRAS

Conforme definido pelo TSE, o *framework* utilizado como critério para a avaliação foi o *CIS Controls*, versão 8, tendo o controle 15 - Gestão de Provedores de Serviços - como principal. 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.

Para tanto, na Matriz de Planejamento dos Testes do Programa de Auditoria (pp. 59-62), ficou estabelecido que as amostras seriam delimitadas conforme a seguir:

a) capacitações em segurança da informação, a partir de 1.1.2021, das(os) servidoras(es) da área de TIC indicadas(os) em equipes de planejamento de contratações;

b) servidoras(es) e colaboradoras(es) de TIC desligadas(os) a partir de 1.1.2021;

c) contratações de bens/serviços de TIC vigentes;

d) provedores de serviços de TIC e respectivas(os) colaboradoras(es) com contratos vigentes;

e) unidades da STI que atuam diretamente com prestadores de serviços.

V. CRITÉRIOS

Os critérios utilizados como parâmetros para fundamentar as avaliações apresentadas neste trabalho foram os preceitos normativos e os documentos referenciais internacionalmente reconhecidos sobre a matéria, conforme segue:

1. Center for Internet Security. Controles CIS, versão 8 (traduzido para o português)[8].

2. Resolução CNJ n. 396, de 7 de junho de 2021: Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ)[9].

3. Resolução TSE n. 23.644, de 1º de julho de 2021: Dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral[10].

4. TRE-SC - Portaria P n. 318, de 20 de novembro de 2017: Institui a Comissão de Segurança da Informação no âmbito do TRE-SC[11].

5. TRE-SC - Portaria DG n. 491, de 11 de novembro de 2013: Limites técnicos associados à segurança da informação em meio digital[12].

6. TRE-SC - Portaria DG n. 213, de 21 de agosto de 2019: Institui os processos de gerenciamento de TI[13].

7. TRE-SC - Ordem de Serviço DG n. 3, de 11 de novembro de 2013: Procedimentos técnicos associados à segurança da informação em meio digital[14].

VI. METODOLOGIA

Os trabalhos de auditoria foram fundamentados na metodologia adotada pelo TSE, o qual encaminhou o modelo de Plano de Trabalho de Auditoria que foi observado por todos os Tribunais Regionais Eleitorais.

O desenvolvimento dos trabalhos observou os termos do procedimento fixado pela Resolução CNJ n. 309/2020, assim como pela Portaria P n. 120/2014. Tiveram

[8] Disponível em: <http://www.cisecurity.org/controls/v8>.

[9] Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3975>.

[10] Disponível em: <https://www.tse.jus.br/legislacao/compilada/res/2021/resolucao-no-23-644-de-1o-de-julho-de-2021>.

[11] Disponível em: <https://www.tre-sc.jus.br/legislacao/compilada/portaria-p/2017/portaria-p-n-318-de-20-de-novembro-de-2017>.

[12] Disponível em: <http://apps.tre-sc.jus.br/site/legislacao/normas-administrativas/portaria-dg/2013/portaria-dg-n-4912013/index.html>.

[13] Disponível em: <https://www.tre-sc.jus.br/legislacao/compilada/portaria-dg/2019/portaria-dg-n-213-de-21-de-agosto-de-2019>.

[14] Disponível em: <http://apps.tre-sc.jus.br/site/legislacao/normas-administrativas/ordem-de-servico-dg/2013/ordem-de-servico-dg-n-32013/index.html>.

ainda por base o Manual de Procedimentos de Auditoria, elaborado pelo TSE (2016), que estabeleceu a metodologia para a execução dos trabalhos de Auditoria Baseada em Riscos, definindo práticas e procedimentos a serem adotados para o desenvolvimento das atividades.

Na Auditoria Baseada em Risco (ABR), são aplicadas técnicas direcionadas ao processo de trabalho auditado e à mitigação dos riscos relacionados à consecução das atividades pertinentes.

Essa metodologia permite ao auditor testar os controles mais importantes, ou focar nas áreas estratégicas, otimizando os recursos humanos e materiais disponíveis, com vistas a que o resultado do trabalho venha a agregar valor e melhorar as atividades da organização. Abaixo segue quadro demonstrativo que, em suma, apresenta o sequenciamento das atividades de auditoria desenvolvidas sob a orientação da metodologia da ABR:

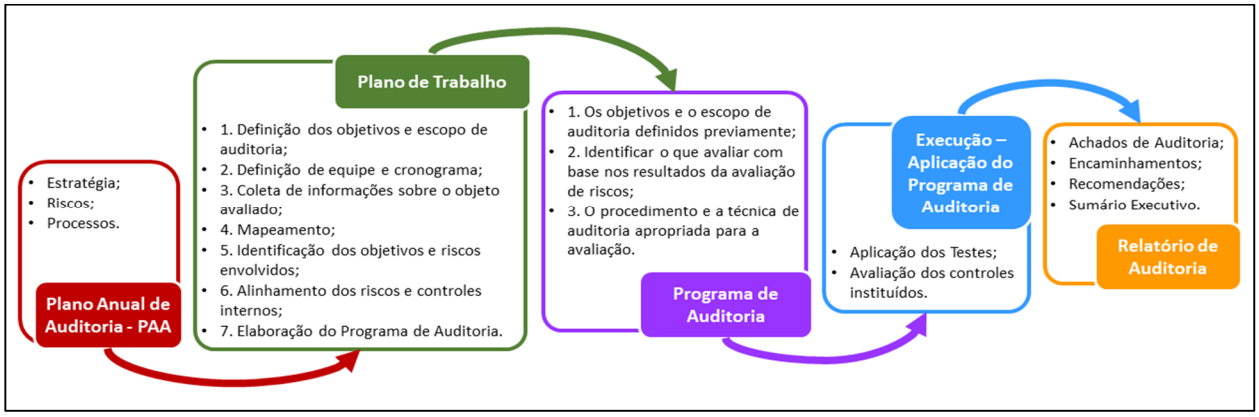

Figura 1 – Processo da Auditoria Baseada em Riscos

Na **etapa de planejamento** dos trabalhos, foi realizado o levantamento detalhado das atividades do processo auditado por meio de questionário encaminhado à Unidade Auditada (pp. 19-21), de informações coletadas com servidoras(es) que executam as atividades correlatas, assim como do estudo da documentação e normas pertinentes.

Considerando a inexistência de processos formais de trabalho, de fluxogramas gráficos e da análise de riscos específica, foram elaborados o Mapeamento dos Processos e a Matriz de Riscos e Controles (pp. 22-54), a partir das informações

previamente coletadas, assim como em conjunto com a Unidade Auditada e com a sua devida validação.

Em seguimento, foram encaminhados à SAU/TSE os documentos acima descritos, além da Matriz de Testes, como também o fizeram os demais Tribunais Regionais. A partir das informações disponibilizadas, aquela Unidade de Auditoria encaminhou o Programa de Auditoria padronizado com a respectiva Matriz de Planejamento dos Testes contendo os procedimentos mínimos a serem aplicados e os parâmetros para avaliar o processo (pp. 55-62).

A **fase de execução** dos testes teve como objetivo a coleta de evidências por meio dos procedimentos definidos no Programa de Auditoria padronizado, que dão suporte aos achados de auditoria. Neste momento, foram elaborados e preenchidos papeis de trabalho relativos aos itens previstos na Matriz de Planejamento dos Testes, executados nas amostras previamente definidas (pp. 78-111).

Após a conclusão da execução dos testes, foi elaborado o Relatório Preliminar de Auditoria com as informações e evidências obtidas, no qual constou a situação encontrada, os critérios, as evidências e a potencialidade dos achados, tendo sido o documento levado à análise da Unidade Auditada para conhecimento e manifestação quanto à pertinência das situações identificadas, assim como das respectivas prescrições (pp. 112-121).

Após, houve a manifestação da Unidade Auditada quanto ao Relatório Preliminar, o que foi realizado de forma consistente e tempestiva. Tais apontamentos foram consignados no presente relatório, o qual contém os achados e as prescrições de maior relevância, além da conclusão da equipe de auditoria sobre o processo avaliado.

O presente Relatório de Auditoria será encaminhado às unidades interessadas do TRE-SC, para ciência e adoção das providências pertinentes, assim como à Secretaria de Auditoria do TSE, para a consolidação dos principais achados.

VII. ACHADOS DE AUDITORIA

Os achados representam o resultado dos testes de auditoria aplicados e das informações coletadas nas entrevistas, análises documentais, correlação de informações, vistorias e conciliações guardando relação com o planejamento desta auditoria.

De acordo com a Matriz de Planejamento dos Testes, do Relatório Preliminar de Achados e da manifestação da Unidade Auditada, foram identificados achados que podem comprometer, em maior ou menor grau, o alcance dos objetivos do processo.

Isso posto, a seguir apresentam-se os achados de auditoria de maior relevância identificados, cada qual com a situação encontrada, as evidências, os critérios, as possíveis causas, as consequências do achado, a manifestação da Unidade Auditada, a conclusão da Equipe de Auditoria e, conforme o caso, a proposta de encaminhamento.

ACHADO A2 – INEXISTÊNCIA DE TERMOS DE CONFIDENCIALIDADE E SIGILO NAS CONTRATAÇÕES DE SERVIÇOS DE TIC

SITUAÇÃO ENCONTRADA: Nos processos das contratações de serviços de TIC vigentes, não foram encontrados Termos de Confidencialidade e Sigilo assinados, tampouco existe a respectiva previsão no planejamento da contratação.

EVIDÊNCIAS:

- Processos de contratação de serviços de TIC vigentes: PAE n. 18.080/2021; PAE n. 64.329/2018; PAE N. 13.347/2018; PAE n. 13297/2018; PAE n. 21334/2021; PAE n. 19549/2019; PAE n. 9.539/2022.

CRITÉRIOS:

- Controle CIS 15.4 - Garantir requisitos de segurança nos contratos.
- Resolução CNJ n. 396/2021, art. 23, IX.
- Resolução TSE n. 23.644/2021, art. 16.
- TRE-SC – Ordem de Serviço DG n. 3/2013, Art. 12.

POSSÍVEIS CAUSAS:

- Ausência de requisitos de Segurança da Informação nas contratações de TIC.
- Controles internos deficitários relativos ao cumprimento dos requisitos de Segurança da Informação constantes nas contratações de TIC.

CONSEQUÊNCIAS DO ACHADO:

- Impossibilidade de exigir a assinatura de Termos de Confidencialidade e Sigilo nas contratações de TIC.
- Não cumprimento dos requisitos de Segurança da Informação por parte da contratada e colaboradoras(es), com risco de divulgação de informações sensíveis de modo indevido.

MANIFESTAÇÃO DA UNIDADE AUDITADA (*in verbis*):

Em atenção ao achado A2, A4, A5, A6 informamos que foi elaborado plano de ação detalhado a seguir para sanar as situações encontradas. Em função do acúmulo de atividades relativas ao período eleitoral, as atividades serão iniciadas em novembro, logo após a data prevista para o segundo turno. Também vale ressaltar que, em função da inexistência de unidade exclusiva para segurança da informação, a Seção de Administração de Redes e de Servidores será indicada como unidade responsável provisoriamente que a unidade responsável pela segurança da informação seja criada.

Atividades	Cronograma		Responsável
	Início	Término	
Elaborar modelo de termos de confidencialidade e sigilo nas contratações de serviços de TIC	Novembro/ 2022	Março/ 2023	Seção de Administração de Redes e de Servidores
Definir aspectos a serem abordados na reunião inicial com provedores de serviços de TIC	Janeiro/ 2023	Março/ 2023	Seção de Administração de Redes e de Servidores
Formalizar a obrigatoriedade do uso do termo de confidencialidade e da apresentação dos critérios de segurança na reunião inicial com provedores de serviço de TIC.	Abril/2023	Abril/2023	Secretaria de Tecnologia da Informação
Levantar escopo e critérios de segurança para a contratação dos provedores de serviço de TIC	Maio/2023	Agosto/ 2023	Seção de Administração de Redes e de Servidores
Elaborar checklist modelo para atestar conformidade do objeto ou serviço durante a execução contratual	Agosto/ 2023	Outubro/ 2023	Seção de Administração de Redes e de Servidores
Formalizar os critérios de segurança para os provedores de serviço de TIC no processo de contratação e execução contratual	Novembro/ 2023	Novembro/ 2023	Secretaria de Tecnologia da Informação

CONCLUSÃO DA EQUIPE DE AUDITORIA:

Verificou-se que o plano de ação apresentado pela Unidade Auditada, com execução prevista para o período de novembro/2022 a novembro/2023, abrange as prescrições contidas nos Achados A2, A4, A5 e A6, respectivamente sobre inexistência de:

- termos de confidencialidade e sigilo nas contratações de serviços de TIC;
- registros acerca da reunião inicial com provedores de serviço de TIC;
- critérios de segurança da informação para a gestão de provedores de serviço de TIC na execução dos contratos; e
- requisitos de segurança da informação para avaliar o objeto ou serviço prestado durante a execução contratual.

De acordo com as informações prestadas e dada a relevância do tema, conclui-se pela necessidade de acompanhamento do procedimento por parte desta Unidade Técnica.

PROPOSTA DE ENCAMINHAMENTO:

Acompanhamento do plano de ação proposto pela Unidade Auditada, verificando a efetivação de todas as todas as etapas previstas, no prazo no prazo de novembro/2022 a novembro/2023.

ACHADO A3 – SERVIDORAS(ES) E COLABORADORAS(ES) DESLIGADAS(OS) COM PERFIS ATIVOS NA BASE DO SISTEMA CONTROLE DE CONTAS

SITUAÇÃO ENCONTRADA: Na amostra de servidoras(es) e colaboradoras(es) desligadas(os) a partir de 1.1.2021, foram encontrados perfis ainda ativos na base do sistema de controle de contas.

EVIDÊNCIAS:

- Amostra de servidoras(es) e colaboradoras(es) desligadas(os) a partir de 1.1.2021 (pp. 108-109).
- Consultas realizadas no sistema de controle de contas, por intermédio do link [redacted] conforme consta na relação de pp. 114-115.

CRITÉRIOS:

- Controle CIS 5.3 - Desabilitar contas inativas.

- Controle CIS 6.2 - Estabelecer um Processo de Revogação de Acesso.
- Resolução CNJ 396/2021, art. 29.
- Resolução TSE 23.644/2021, art. 9º, II, b.

POSSÍVEIS CAUSAS:

- Ausência de verificação periódica dos perfis ativos de servidoras(es) e colaboradoras(es) que deveriam estar desabilitadas(os).
- Orientação deficitária aos gestores de pessoas a respeito do procedimento em caso de desligamento de servidoras(es) e colaboradoras(es).

CONSEQUÊNCIAS DO ACHADO:

- Risco de acesso a informações de modo indevido tendo em vista a manutenção do acesso de pessoas já desligadas do TRE-SC a sistemas que contêm dados sensíveis.

MANIFESTAÇÃO DA UNIDADE AUDITADA (*in verbis*):

> Sobre o achado A3 informamos que o desligamento de usuários é realizado pela Central de Serviços de TI, assim que são recebidas as devidas comunicações via o formulário "Informação de desligamento - TRE" do sistema [redacted].
>
> Neste sentido, foi aberto o chamado #00099932 na Central de Serviços de TI para inativação dos usuários identificados pela auditoria, sendo que todos aqueles relacionados tiveram suas contas inativadas, com exceção dos usuários José Roberto Ventura (terceirizado) e Zurita Maria Pacheco Ruckl (operadora de Totalização), pois foram recentemente (re)contratados.
>
> Ainda sobre este achado, foi enviado o memorando 042/2022 à SGP reforçando a necessidade do devido preenchimento do referido formulário sempre que um colaborador é desligado, bem como foi publicado informe na intranet reforçando a importância do registro da solicitação, conforme imagem a seguir:
>
> [Imagem do informe na intranet, conforme link abaixo]
>
> http://intranet.tre-sc.gov.br/principal/informes/2022/8/desativacao-de-usuariosorientacoes

CONCLUSÃO DA EQUIPE DE AUDITORIA:

Em que pese restar confirmado o desligamento das contas acima descritas, verificou-se que não foi apontada nenhuma ação de mitigação do risco de existir contas ativas de pessoas que já não fazem parte do quadro (seja próprio ou terceirizado) do TRE-SC, como a verificação periódica de todos os casos pendentes.

De acordo com as informações prestadas, conclui-se pela necessidade de fortalecimento dos controles internos relativos à desativação de contas e perfis de servidoras(es) e colaboradoras(es) que já não atuam mais neste Tribunal.

PROPOSTA DE ENCAMINHAMENTO:

Orientação à Unidade Auditada para robustecer os controles internos relativos à desativação de contas de servidoras(es) e colaboradoras(es) que não atuam mais no TRE-SC, verificando periodicamente as pessoas que foram desligadas do Tribunal e desabilitando perfis que porventura ainda estiverem ativos indevidamente.

ACHADO A4 – INEXISTÊNCIA DE REGISTROS ACERCA DA REUNIÃO INICIAL COM PROVEDORES DE SERVIÇO DE TIC

SITUAÇÃO ENCONTRADA: Nos processos das contratações de serviços de TIC vigentes, verificou-se não haver registro formal de reunião inicial do contrato, tampouco quaisquer outros documentos nos quais são explanados os requisitos de Segurança da Informação para a execução contratual.

EVIDÊNCIAS:

- Processos de contratação de serviços de TIC vigentes: PAE n. 18.080/2021; PAE n. 64.329/2018; PAE N. 13.347/2018; PAE n. 13297/2018; PAE n. 21334/2021; PAE n. 19549/2019; PAE n. 9.539/2022.

CRITÉRIOS:

- Controle CIS 15.2 - Estabelecer e manter uma política de gestão de provedores de serviços
- Resolução CNJ 396/2021, art. 28, IV.
- Resolução TSE 23.644/2021, art. 27.

POSSÍVEIS CAUSAS:

- Ausência de procedimentos padronizados relativos à gestão de contratos de TIC.
- Controles internos deficitários relativos ao cumprimento de procedimentos padronizados relativos à gestão de contratos de TIC.

CONSEQUÊNCIAS DO ACHADO:

- Ausência de formalização da apresentação dos critérios da Segurança da informação à contratada, aumentando o risco de desconhecimento dos respectivos requisitos.

MANIFESTAÇÃO DA UNIDADE AUDITADA: conforme consta no Achado A2.

CONCLUSÃO DA EQUIPE DE AUDITORIA: conforme consta no Achado A2.

PROPOSTA DE ENCAMINHAMENTO: conforme consta no Achado A2.

ACHADO A5 – INEXISTÊNCIA DE CRITÉRIOS DE SEGURANÇA DA INFORMAÇÃO PARA A GESTÃO DE PROVEDORES DE SERVIÇO DE TIC NA EXECUÇÃO DOS CONTRATOS

SITUAÇÃO ENCONTRADA: Nos processos das contratações de serviços de TIC vigentes, verificou-se não haver critérios de Segurança da Informação para a gestão da execução dos contratos, relativos a classificação, inventário, avaliação, monitoramento e descomissionamento dos respectivos provedores de serviço.

EVIDÊNCIAS:

- Conforme p. 74 dos autos, Unidade Auditada informou que não possui política de gestão de provedores, são realizadas ações ad hoc e não formalizadas.
- Processos de contratação de serviços de TIC vigentes: PAE n. 18.080/2021; PAE n. 64.329/2018; PAE n. 13.347/2018; PAE n. 13297/2018; PAE n. 21334/2021; PAE n. 19549/2019; PAE n. 9.539/2022.

CRITÉRIOS:

- Controle CIS 15.1 - Estabelecer e manter um inventário de provedores de serviços.
- Controle CIS 15.2 - Estabelecer e manter uma política de gestão de provedores de serviços.
- Controle CIS 15.3 - Classificar provedores de serviços.
- Controle CIS 15.5 - Avaliar provedores de serviços.
- Controle CIS 15.6 - Monitorar provedores de serviços.
- Controle CIS 15.7 - Descomissionar com segurança os provedores de serviços.
- Resolução CNJ 396/2021, art. 28, IV.
- Resolução TSE 23.644/2021, art. 27.

POSSÍVEIS CAUSAS:

- Ausência de procedimentos padronizados relativos à gestão de contratos de TIC.

- Controles internos deficitários relativos ao cumprimento de procedimentos padronizados relativos à gestão de contratos de TIC.

CONSEQUÊNCIAS DO ACHADO:

- Ausência de inventário de provedores de serviços, gerando descontrole sobre o seu monitoramento e descomissionamento.

MANIFESTAÇÃO DA UNIDADE AUDITADA: conforme consta no Achado A2.

CONCLUSÃO DA EQUIPE DE AUDITORIA: conforme consta no Achado A2.

PROPOSTA DE ENCAMINHAMENTO: conforme consta no Achado A2.

ACHADO A6 – INEXISTÊNCIA DE REQUISITOS DE SEGURANÇA DA INFORMAÇÃO PARA AVALIAR O OBJETO OU SERVIÇO PRESTADO DURANTE A EXECUÇÃO CONTRATUAL

SITUAÇÃO ENCONTRADA: Nos processos das contratações de serviços de TIC vigentes, verificou-se não haver requisitos de Segurança da Informação para avaliar o objeto ou serviço prestado durante a execução contratual, tais como *checklists* para atestação da conformidade do objeto ou da prestação durante a execução.

EVIDÊNCIAS:

- Conforme pp. 74-75 dos autos, Unidade Auditada informou que não utiliza checklist para atestar a conformidade relacionada à Segurança da Informação.
- Processos de contratação de serviços de TIC vigentes: PAE n. 18.080/2021; PAE n. 64.329/2018; PAE n. 13.347/2018; PAE n. 13297/2018; PAE n. 21334/2021; PAE n. 19549/2019; PAE n. 9.539/2022.

CRITÉRIOS:

- Controle CIS 15.5 – Avaliar provedores de serviços.
- Controle CIS 15.6 – Monitorar provedores de serviços.
- Resolução CNJ 396/2021, art. 28, IV.
- Resolução TSE 23.644/2021, art. 27.

POSSÍVEIS CAUSAS:

- Ausência de procedimentos padronizados relativos à gestão de contratos de TIC.
- Controles internos deficitários relativos ao cumprimento de procedimentos padronizados relativos à gestão de contratos de TIC.

CONSEQUÊNCIAS DO ACHADO:

- Avaliações equivocadas sobre a execução dos serviços de contratos de TIC.

MANIFESTAÇÃO DA UNIDADE AUDITADA: conforme consta no Achado A2.

CONCLUSÃO DA EQUIPE DE AUDITORIA: conforme consta no Achado A2.

PROPOSTA DE ENCAMINHAMENTO: conforme consta no Achado A2.

ACHADO A7 – INEXISTÊNCIA DE NORMATIVOS INTERNOS ESPECÍFICOS RELACIONADOS À SEGURANÇA DA INFORMAÇÃO

SITUAÇÃO ENCONTRADA: O TRE-SC segue o que preconiza a Resolução TSE n. 23.644/2021, a qual dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral. Entretanto, não possui normas internas específicas relacionadas à Segurança da Informação, previstas na normativa acima descrita, no seu no art. 9º, *in verbis*:

> Art. 9º A estrutura normativa referente à Segurança da Informação será estabelecida e organizada conforme definido a seguir:
>
> I - Nível Estratégico: Política de Segurança da Informação da Justiça Eleitoral, constituída por esta Resolução, a qual define as diretrizes fundamentais e os princípios basilares incorporados pela instituição à sua gestão, de acordo com a visão definida pelo Planejamento Estratégico dos órgãos da Justiça Eleitoral;
>
> **II - Nível Tático: Normas Complementares sobre Segurança da Informação, que contemplam obrigações a serem seguidas de acordo com as diretrizes estabelecidas nesta PSI, a serem editadas por todos os tribunais que compõem a Justiça Eleitoral, e devem abarcar, no mínimo, os seguintes temas:**
>
> a. Gestão de Ativos;
> **b. Controle de Acesso Físico e Lógico;**
> **c. Gestão de Riscos de Segurança da Informação;**
> d. Uso Aceitável de Recursos de TI;
> e. Geração e Restauração de Cópias de Segurança (backup);
> f. Plano de Continuidade de Serviços Essenciais de TI;
> g. Gestão de Incidentes de Segurança da Informação;
> h. Gestão de Vulnerabilidades e Padrões de Configuração Segura;
> i. Gestão e Monitoramento de Registros de Atividade (logs);
> j. Desenvolvimento Seguro de Sistemas;

> k. Uso de Recursos Criptográficos.
>
> **III - Nível Operacional: Procedimentos de Segurança da Informação que contemplam regras operacionais, roteiros técnicos, fluxos de processos, manuais com informações técnicas que instrumentalizam o disposto nas normas referenciadas no plano tático, de acordo com o disposto nas diretrizes e normas de segurança estabelecidas, permitindo sua utilização nas atividades do órgão.**
>
> [...] (grifo nosso)

EVIDÊNCIAS:

- Informações Preliminares prestadas pela Unidade Auditada, conforme pp. 19-20 dos autos.
- Pesquisa realizada na página de Governança e Gestão de Tecnologia da Informação e Comunicação (link: <http://intranet.tre-sc.gov.br/governanca-e-gestao/governanca-e-gestao-de-tecnologia-da-informacao-e-comunicacao>).

CRITÉRIOS:

- Resolução CNJ 396/2021, art. 28.
- Resolução TSE 23.644/2021, art. 9º.

POSSÍVEIS CAUSAS:

- Ausência ou impossibilidade de priorização da atividade de elaboração de normativos internos específicos relacionados à Segurança da Informação.

CONSEQUÊNCIAS DO ACHADO:

- Não observância do art. 9º da Resolução TSE 23.644/2021.
- Falta de padronização das ações relativas à Segurança da Informação no TRE-SC.

MANIFESTAÇÃO DA UNIDADE AUDITADA (*in verbis*):

> Em relação ao achado A7, informamos que este Tribunal não possui unidade exclusiva dedicada à segurança da informação e a execução de atividades relativas ao tema fica prejudicada, pois são executadas tangencialmente por outras unidades e acabam por concorrer com as atividades ordinárias, conforme demonstrado no PAE 33.181/2021. Em que pese esta sabida carência de estrutura, existem diversas normas sendo elaboradas e devem estar publicadas até o final de 2023. Dentre elas destacam-se:
> a. Gestão de Ativos
> b. Controle de Acesso Físico e Lógico
> h. Gerenciamento de Vulnerabilidades
> i. Gestão e Monitoramento de Registros de Atividades (logs)
>
> Ademais, existe um grupo nacional da Justiça Eleitoral trabalhando, de forma colaborativa, com os normativos relacionados à segurança da informação. O TRE-SC participa deste grupo e assim que outros normativos forem produzidos pelo referido grupo, poderão ser analisados e customizados à realidade deste

Regional para posterior publicação. A expectativa é que as demais normas sendo produzidas estejam publicadas até o final de 2023.

CONCLUSÃO DA EQUIPE DE AUDITORIA:

De acordo com as informações prestadas, conclui-se que a Unidade Auditada está ciente da necessidade de elaboração das respectivas normas e vem investindo esforços para a sua efetivação até o próximo exercício, sendo necessário o respectivo acompanhamento por parte desta Unidade Técnica.

PROPOSTA DE ENCAMINHAMENTO:

Acompanhamento da elaboração dos normativos relacionados à Segurança da Informação previstos na Resolução TSE n. 23.644/2021, art. 9º, II, em especial sobre "Controle de Acesso Físico e Lógico" e "Gestão de Riscos de Segurança da Informação", com previsão para o final do ano de 2023.

ACHADO A8 – SISTEMAS CRÍTICOS COM APENAS UMA FORMA DE AUTENTICAÇÃO

SITUAÇÃO ENCONTRADA: Foram identificados sistemas com acesso externo sem que houvesse uma camada de proteção adicional ao processo de entrada além da senha (MFA - autenticação multifator).

EVIDÊNCIAS:

[redacted]Sistemas: [redacted]

CRITÉRIOS:

- Controle CIS 6.3 - Exigir MFA para aplicações expostas externamente.
- Controle CIS 6.4 - Exigir MFA para acesso remoto à rede.
- Controle CIS 6.5 - Exigir MFA para acesso administrativo.
- Resolução CNJ 396/2021, art. 11, IX.
- Resolução TSE 23.644/2021, art. 9°, II, b.

POSSÍVEIS CAUSAS:

- Impossibilidade técnica de implementação de MFA em sistemas específicos.
- Ausência de contratação de solução de TIC para implementação de MFA.
- Ausência de identificação e controle dos sistemas considerados sensíveis.

CONSEQUÊNCIAS DO ACHADO:

- Ausência de proteção adicional em sistemas ou tipos de acessos considerados sensíveis, aumentando o risco de acesso indevido.

MANIFESTAÇÃO DA UNIDADE AUDITADA (*in verbis*):

> Em atenção ao achado A8, informamos que recentemente foi adquirida - resultado da contratação objeto do PAE 21.782/2022 - solução que permitirá ao TRE-SC adotar multifator (MFA) em sistemas ou tipos de acesso considerados sensíveis como, por exemplo, o Sistema [redacted] que deverá estar integrado até dezembro de 2022. O sistema [redacted] e a integração dele com o MFA será objeto de integração futura, pois a atual versão já está em uso e a mudança, neste momento, poderia trazer risco a [redacted]. Por fim, os sistemas Agendamento Eleitoral e e-Docs, quando acessados pela internet, são sistemas apenas de consulta, ou uso irrestrito, não sendo necessária a autenticação para utilizar referidos sistemas pela internet.

CONCLUSÃO DA EQUIPE DE AUDITORIA:

Verificou-se que a contratação de serviço de autenticação por múltiplos fatores, com suporte técnico, implantação e treinamento formal, prevista no PAE 21.782/2022, encontra-se no início, tendo sido designada a equipe de planejamento em 14.6.2022. Até o momento, não foram elaborados os Estudos Preliminares e tampouco o Projeto Básico/Termo de Referência.

Ademais, observou-se que não foram identificados outros sistemas considerados sensíveis além daqueles relacionados nas evidências acima, os quais tratam de amostra de auditoria e não representam todo o rol respectivo.

De acordo com as informações prestadas, conclui-se pela necessidade de acompanhamento por parte desta Unidade Técnica da contratação constante no PAE 21.782/2022, assim como de análise por parte da Unidade Auditada dos demais sistemas e formas de acesso que denotem a necessidade de autenticação por múltiplos fatores.

PROPOSTA DE ENCAMINHAMENTO:

Acompanhamento da efetivação da contratação de serviço de autenticação por múltiplos fatores, com suporte técnico, implantação e treinamento formal, por intermédio do PAE 21.782/2022.

Orientação à Unidade Auditada para identificar todos os sistemas e formas de acesso considerados sensíveis, como aqueles acessados pela internet ou contas com privilégios administrativos, assim como avaliar a necessidade e viabilidade técnica de implementação de múltiplo fator de autenticação para cada um deles.

VIII. CONCLUSÃO

Em face dos exames de auditoria ora realizados, tendo por finalidade avaliar a existência e a qualidade dos controles internos instituídos no processo de Gestão de Segurança da Informação, especificamente no que diz respeito à Gestão de Contas, Gestão do Controle de Acesso e Gestão de Provedor de Serviços de TIC, constatou-se o que segue:

1. A Unidade Auditada, aqui considerada a STI em sua completude, empenha esforços na gestão do processo de Gestão de Segurança da Informação, com enfoque na gestão de provedores de serviços de TIC, gestão de contas e do controle de acesso, haja vista a profunda participação das Coordenadorias de Soluções Corporativas (CSC) e de Suporte e Infraestrutura Tecnológica (CSIT), ressaltando a atribuição da CSIT em "supervisionar as atividades referentes à administração das políticas de segurança da informação da rede corporativa da Justiça Eleitoral catarinense", conforme consta na Resolução TRE-SC n. 7.930/2015, art. 136, VI. Entretanto, os processos não estão formalizados por meio de manuais ou portarias específicas, tendo seus controles internos instituídos em sua maioria de forma manual e focados mais na conformidade do que na aplicação de boas práticas de governança. A gestão de provedores de serviços de TIC carece de requisitos e padronizações referentes à Segurança da Informação. A gestão de contas e do controle de acesso possui controles internos dependentes de solicitações e informações dos gestores de pessoas, porém sem práticas estabelecidas de revisões periódicas no que diz respeito à desativação de perfis.

2. Da análise realizada, cumpre destacar como achados positivos:

- A iniciativa da Unidade Auditada em demandar a contratação de licenças de acesso à plataforma integrada de treinamento online, especializada em oferta de conteúdos de capacitação e conscientização em Segurança da Informação, no PAE 21.243/2022, a qual efetivou-se recentemente com a assinatura do Contrato 062/2022. Ademais, verificou-se que a Unidade Auditada demonstrou o envio de orientação a todas(os) as(os) servidoras(es) da STI acerca da necessidade de capacitação em segurança da informação para participar como integrante técnico nas contratações. De acordo com as informações prestadas (p. 122), conclui-se pelo atendimento ao prescrito no Achado A1 do Relatório Preliminar (p. 113), com a devida priorização de indicação de

integrantes técnicos para a Equipe de Planejamento da Contratação que possuam capacitação específica na área de Segurança da Informação, assim como disponibilização de treinamento por meio do contrato acima descrito.

- Conforme descrito no Achado A3, a Unidade Auditada prontamente desativou as contas de pessoas que já não possuem vínculo com o TRE-SC identificadas na amostra e apontadas no Relatório Preliminar (p. 114-115), com vistas a reduzir o risco de acessos indevidos.
- Conforme descrito no Achado A8, a Unidade Auditada, antes mesmo da conclusão deste trabalho de auditoria, iniciou o processo de contratação de serviço de autenticação por múltiplos fatores, com suporte técnico, implantação e treinamento formal, por intermédio do PAE 21.782/2022, com vistas a reduzir o risco de acessos indevidos a sistemas considerados sensíveis.

3. Verificaram-se algumas inconsistências que se refletem nos achados de auditoria consignados nesse relatório, em grande parte devido à inexistência de normativos internos sobre os processos de gestão, com a devida padronização de procedimentos e documentos, em especial na gestão de provedores de serviços de TIC. Ademais, na gestão de contas e do controle do acesso, verificou-se serem deficitários os controles internos para mitigação do risco da existência indevida de contas ativas, além de acesso a sistemas considerados sensíveis com uma única forma de autenticação.

4. Por fim, o presente trabalho de auditoria trouxe alguns benefícios imediatos à Unidade Auditada, podendo ser citado, em especial, o mapeamento dos processos de trabalho relacionados, resultando na elaboração das representações gráficas (fluxogramas) e respectiva análise de riscos, assim como da Matriz de Controles e Riscos, procedimentos estes realizados em conjunto com a STI, o que se transformou em uma oportunidade de aperfeiçoamento das concepções e práticas administrativas relativas ao tema.

IX. PROPOSTA DE ENCAMINHAMENTO

Diante do exposto, submete-se o presente relatório à consideração do Senhor Secretário de Controle Interno e Auditoria substituto, para encaminhamento ao Senhor Presidente do TRE-SC e à Secretaria de Auditoria do TSE, com vistas a ciência da Unidade Auditada, referente aos seguintes itens:

1. PELA ORIENTAÇÃO À UNIDADE AUDITADA PARA:

1.1. robustecer os controles internos relativos à desativação de contas de servidoras(es) e colaboradoras(es) que não atuam mais no TRE-SC, verificando periodicamente as pessoas que foram desligadas do Tribunal e desabilitando perfis que porventura ainda estiverem ativos indevidamente [Achado A3];

1.2. identificar todos os sistemas e formas de acesso considerados sensíveis, como aqueles acessados pela internet ou contas com privilégios administrativos, assim como avaliar a necessidade e viabilidade técnica de implementação de múltiplo fator de autenticação para cada um deles [Achado A8].

2. PELO ACOMPANHAMENTO, POR PARTE DESTA UNIDADE TÉCNICA:

2.1. do plano de ação proposto pela Unidade Auditada, verificando a efetivação de todas as todas as etapas previstas, no prazo de novembro/2022 a novembro/2023 [Achados A2, A4, A5 e A6];

2.2. da elaboração dos normativos relacionados à Segurança da Informação previstos na Resolução TSE n. 23.644/2021, art. 9º, II, em especial sobre “Controle de Acesso Físico e Lógico” e “Gestão de Riscos de Segurança da Informação”, com previsão para o final do ano de 2023 [Achado A7];

2.3. da efetivação da contratação de serviço de autenticação por múltiplos fatores, com suporte técnico, implantação e treinamento formal, por intermédio do PAE 21.782/2022 [Achado A8].

Por fim, em cumprimento aos termos da Resolução TSE n. 23.500/2016 e ao cronograma fixado pela SAU/TSE, o presente Relatório de Auditoria será encaminhado àquela Unidade de Auditoria como término dos trabalhos das Auditorias Integradas da Justiça Eleitoral de 2022.

Florianópolis, 16 de agosto de 2022.

Juliana Teixeira Ferreira Pinheiro
Analista Judiciária

Maurício Merkl
Analista Judiciário

José Farias Junior
Chefe da Seção de Acompanhamento, Avaliação de Gestão e Auditoria - Área Administrativa

De acordo.

Encaminhe-se o presente Relatório de Auditoria à Presidência deste Tribunal Regional Eleitoral de Santa Catarina e, em seguimento, à Secretaria de Controle Interno e Auditoria do Tribunal Superior Eleitoral.

Florianópolis, 16 de agosto de 2022.

Elton Carioni Carsten
Secretário de Controle Interno e Auditoria substituto