TRIBUNAL REGIONAL ELEITORAL DO PARÁ
SECRETARIA DE AUDITORIA
COORDENADORIA DE AUDITORIA

RELATÓRIO FINAL

AUDITORIA DO PROCESSO DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Agosto/2022

Preâmbulo

Processos SEI: 0005982-86.2022.6.14.8000 (abertura) /

0008530-84.2022.6.14.8000 (execução).

Ato originário: Plano Anual de Auditoria 2022.

Objetivo: Avaliar o processo de gestão da segurança da informação, conforme práticas e medidas de segurança (controles internos) recomendadas pelo framework CIS Controls V8.

Período abrangido pela auditoria: De maio a agosto de 2022.

Período de realização da auditoria: Planejamento [de 23/05 a 30/06/22]; **Execução** [de 01/07 a 05/08/22]; e **Relatório** [de 08/08 a 17/08/22].

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

Equipe de Auditoria: Marco Antônio Fagundes de Moraes (Auditor responsável - lotado na SECOI), Fabrício Manoel Santiago Cordeiro (Chefe da SEAP) e Hugo Hyago de Carvalho Mendonça (lotado na SEAP).

Coordenador de Auditoria: Evandro Moreira Ramos.

Secretário de Auditoria: Miguel Chicre Bitar de Moraes.

Resumo

As Auditorias Integradas da Justiça Eleitoral ganham importância na medida em que avaliam, de forma padronizada e sistêmica, temas críticos e comuns a todos os Tribunais Eleitorais. Neste sentido, a auditoria integrada 2022 abordou o tema relevante para órgãos e entidades da Administração Pública: o Processo de Gestão da Segurança da Informação da Justiça Eleitoral.

Esta auditoria tem como escopo os controles 5, 6 e 15 do *framework CIS Controls* V8, que se referem à gestão de contas de usuários, ao controle de acesso e à gestão de provedores de serviços. A metodologia utilizada foi a Auditoria Baseada em Riscos (ABR), conforme plano de trabalho fornecido pelo Tribunal Superior Eleitoral (TSE), durante a fase de planejamento. De forma geral, essa metodologia pode ser dividida em três fases principais: (1) Planejamento; (2) Execução; e (3) Encerramento (Relatórios).

Seguindo para a fase de execução, o TSE forneceu o programa de auditoria, contendo os testes voltados para a verificação da existência e efetividade dos controles associados aos riscos identificados. Os testes aplicados permitiram a avaliação do objeto auditado, segundo o critério definido, favorecendo a obtenção de conclusões com base nas evidências encontradas.

Como resultado da aplicação dos testes, foram evidenciados 09 (nove) achados de auditoria, caracterizados segundo as normas técnicas aplicáveis, conformidade com o critério adotado, situação encontrada, evidências, causas, consequências, comentários dos gestores, conclusões da equipe de auditoria, propostas de encaminhamentos e recomendações.

Portanto, é apresentado o relatório final da auditoria, contendo os principais resultados obtidos, a ser encaminhado ao TSE para compilação no Relatório Consolidado da Auditoria Integrada, que deverá apresentar os achados recorrentes e relevantes a toda Justiça Eleitoral (conforme disposto no art. 6º da Resolução TSE nº 23.500/2016).

SUMÁRIO

I. INTRODUÇÃO 5

II. VISÃO GERAL DO OBJETO AUDITADO 5

III. OBJETIVO DA AUDITORIA 6

IV. ESCOPO 6

V. CRITÉRIOS 7

VI. METODOLOGIA ABR 7

VII. ACHADOS DE AUDITORIA 8

VIII. ACHADOS POSITIVOS 13

IX. PROPOSTAS DE ENCAMINHAMENTOS E RECOMENDAÇÕES 14

X. CONCLUSÃO 16

ANEXO I - QUADRO SINTÉTICO DOS ACHADOS DE AUDITORIA 18

ANEXO II - QUADRO SINTÉTICO DAS RECOMENDAÇÕES 19

ANEXO III - QUADRO SINTÉTICO DOS ACHADOS POSITIVOS 20

I. INTRODUÇÃO

1. Com base na competência fixada no art. 11, §2º, da Lei nº 8.868/94, que confere ao TSE a prerrogativa de definir ações de controle em relação a objetivos gerais da Justiça Eleitoral, foi aprovada a Resolução TSE nº 23.500/2016, que estabeleceu o modelo de avaliação, denominado Auditoria Integrada.

2. O objeto definido pelo TSE para a Auditoria Integrada deste exercício foi o processo de Gestão da Segurança da Informação no âmbito da Justiça Eleitoral, com enfoque nos seguintes controles do *framework CIS Controls* V8 (critério da auditoria): Gestão de Provedores de Serviços; Gestão de Contas; e Controle de Acesso. Para tanto, conforme a metodologia adotada na auditoria integrada, foram utilizados procedimentos e papéis de trabalho padronizados, para levantamento, identificação e avaliação dos controles internos adotados.

3. Vale destacar que o Plano Anual de Auditoria – PAA 2022, aprovado pela Presidência desta Corte, define como uma de suas ações prioritárias, a realização desta auditoria integrada, em atenção ao cronograma estabelecido e as diretrizes fornecidas pelo TSE.

II. VISÃO GERAL DO OBJETO AUDITADO

4. O objeto auditado consiste no processo de Gestão da Segurança da Informação (GSI), que visa proteger o ativo mais importante, no caso, a informação, garantindo a manutenção dos seus principais atributos: Autenticidade, Confidencialidade, Integridade e Disponibilidade.

5. No atual cenário, imposto pela instalação da indústria 4.0, somado à transformação digital do Judiciário para garantir o acesso rápido aos serviços da Justiça, como preconizado pelo Programa Justiça 4.0, a segurança cibernética da informação tem recebido crescente atenção.

6. Para avaliação do objeto auditado, foram realizados os exames no âmbito das coordenadorias de infraestrutura (atual - gestão da segurança cibernética [CGSC]) e de sistemas (COSIS), vinculadas à Secretaria de Tecnologia da Informação (STI).

III. OBJETIVO DA AUDITORIA

7. Objetivo principal desta auditoria é verificar o nível de implementação dos processos de cibersegurança, adotadas pelo setor de tecnologia da informação (TI) dos regionais, com práticas e medidas de segurança (controles internos) recomendadas pelo *framework CIS Controls* V8. Destacam-se como objetivos específicos:

a. Verificar a existência e a qualidade dos controles internos instituídos no processo de gestão de provedores de serviço e seus contratos, observando quesitos da segurança da informação, bem como o tratamento dos riscos ao longo do provimento do serviço;

b. Verificar a existência e a qualidade dos controles internos instituídos no processo de gestão de contas de usuários e de controle de acesso aos ativos da organização, considerando os riscos inerentes às operações verificadas;

c. Verificar a existência e a qualidade dos controles internos relacionados à identificação, proteção, detecção, resposta e recuperação de incidentes de cibersegurança.

IV. ESCOPO

8. O TSE estabeleceu, como escopo desta auditoria integrada, conforme consta no plano de trabalho, três controles do *framework CIS Controls* V8 (CIS V8), quais sejam:

a. **Gestão de Provedores de Serviço (Controle 15)**: Avalia se os provedores de serviços (interno ou externos) estão protegendo as plataformas e os dados de forma adequada, bem como os quesitos observados durante o processo de gestão contratual.

b. **Gestão de Contas e da Gestão do Controle de Acesso (Controles 5 e 6)**: Envolvem o gerenciamento de credenciais de acesso e (concessão/revogação) de privilégios das contas dos usuários, administradores e prestadores de serviços para os recursos corporativos de TI.

V. CRITÉRIOS

9. O critério adotado foi o *framework CIS Controls* V8, que fornece um conjunto de 18 controles, envolvendo práticas e medidas de segurança para mitigar ataques cibernéticos contra sistemas e redes da organização. É válido destacar que as medidas de segurança, ferramentas e procedimentos fornecidos pelo CIS V8 podem auxiliar na estruturação de um programa consistente de segurança da informação em nível estratégico organizacional.

VI. METODOLOGIA ABR[1]

10. Os trabalhos foram orientados pela aplicação das técnicas da Auditoria Baseada em Risco - ABR (*Risk Assessment*), que permite ao auditor testar os controles mais relevantes, otimizando a utilização dos recursos disponíveis, seguindo três fases principais: (1) Planejamento (plano de trabalho e programa de auditoria); (2) Execução (aplicação dos testes); (3) Encerramento (relatório da auditoria). A Figura 1 apresenta as etapas e os principais produtos de trabalho da ABR (Auditoria Baseada em Riscos).

Figura1. Etapas e Principais Produtos de Trabalho da ABR (Auditoria Baseada em Riscos)

[1] Auditoria Baseada em Riscos (ABR) – abordagem que utiliza a avaliação de riscos para definição do escopo, natureza, época e extensão dos procedimentos adicionais de auditoria (Curso ABR - TCU/2018; Issai 100/46, 48 e 49) .

VII. ACHADOS DE AUDITORIA

11. Como resultado da aplicação dos testes, definidos no Programa de Auditoria, foram obtidos os achados de auditoria. Esses achados correspondem à comparação entre "o que é" (situação encontrada), com "o que deveria ser" (critério adotado). Os achados são descobertas feitas pelos auditores, como consequência da aplicação dos procedimentos e técnicas de auditoria previstos pela metodologia utilizada, no caso, a ABR.

12. Os achados são disponibilizados aos gestores, para comentários, esclarecimentos ou considerações acerca das situações encontradas. Os quadros a seguir apresentam os 09 (nove) achados obtidos nesta auditoria.

ACHADO A1 - AUSÊNCIA DE MECANISMOS DE MONITORAMENTO QUANTO À SEGURANÇA DA INFORMAÇÃO DURANTE A EXECUÇÃO CONTRATUAL, ESPECIALMENTE NO TRABALHO REMOTO

N° do Teste	Situação Encontrada
T4/T9	Através da RDIM (formalizada no processo SEI 0008530-84.2022.6.14.8000), a unidade auditada informou que não dispõe de solução para apoiar a fiscalização e monitoramento dos contratos observando quesitos da segurança da informação.

Critérios de Auditoria	Evidências
CIS V8 - Medidas de Segurança 15.6 - monitorar o provimento de serviços de acordo com a política de gestão de provedores do órgão.	Resposta da unidade auditada à RDIM expedida pela equipe de auditoria à STI/COINF[CGSC] (RDIM - SEI 0008530-84.2022.6.14.8000).

Causas	Consequências do Achado
Ausência de política de gestão de provedores, que permita o monitoramento adequado do provedor de serviços em conformidade com as diretrizes instituídas no órgão, com reavaliação periódica.	Prejuízo potencial na aplicação de sanção contratual, no caso de violação de requisitos de segurança da informação.

ACHADO A2 - AUSÊNCIA DE CRITÉRIOS INSTITUÍDOS QUANTO À SEGURANÇA DA INFORMAÇÃO PARA AVALIAR/ATESTAR O OBJETO OU SERVIÇO PRESTADO DURANTE A EXECUÇÃO CONTRATUAL	
N° do Teste	**Situação Encontrada**
T4/T9	Através da RDIM (formalizada no processo SEI 0008530-84.2022.6.14.8000), a unidade auditada informou que não dispõe de critérios instituídos para ateste de serviços durante a execução contratual, segundo requisitos da segurança da informação.

Critérios de Auditoria	Evidências
CIS V8 - Medidas de Segurança 15.5 - avaliação cosistente com a política de gestão de provedores de serviços do órgão.	Resposta da unidade auditada à RDIM expedida pela equipe de auditoria à STI/COINF[CGSC] (RDIM - SEI 0008530-84.2022.6.14.8000).

Causas	Consequências do Achado
Ausência de política de gestão de provedores que permita uma avaliação objetiva, podendo ser através de relatórios padronizados ou questionários personalizados, por exemplo.	Possibilidade do aceite de objeto/serviço sem garantia dos requisitos da segurança da informação.

ACHADO A3 - POSSIBILIDADE DO ACEITE DE OBJETO/SERVIÇO SEM GARANTIA DOS REQUISITOS DA SEGURANÇA DA INFORMAÇÃO	
N° do Teste	**Situação Encontrada**
T4/T9	Através da RDIM (formalizada no processo SEI 0008530-84.2022.6.14.8000), a unidade auditada informou que não possui processo de gestão de riscos (específico de segurança da informação) durante a execução contratual.

Critérios de Auditoria	Evidências
CIS V8 - Medidas de Segurança 15.6 - estabelecer e manter uma política de gerenciamento de provedores de serviços.	Resposta da unidade auditada à RDIM expedida pela equipe de auditoria à STI/COINF[CGSC] (RDIM - SEI 0008530-84.2022.6.14.8000).

Causas	Consequências do Achado
Ausência de processo de gestão de riscos, específicos para segurança da informação **(SI)**, durante a execução contratual.	Potencial materialização de riscos de segurança da informação durante a execução do contrato.

ACHADO A4 - AUSÊNCIA DE ASSINATURA NOS TERMOS DE COMPROMISSO E CIÊNCIA COM A DECLARAÇÃO DE CONFIDENCIALIDADE E SIGILO	
N° do Teste	**Situação Encontrada**
T4/T9	Através da RDIM (formalizada no processo SEI 0008530-84.2022.6.14.8000), a unidade auditada informou que os termos de compromisso e sigilo não possuem assinatura do representante legal da contratada.

Critérios de Auditoria	Evidências
CIS V8 - Medidas de Segurança 15.4 - certificar que os contratos com provedores de serviços incluam requisitos de segurança consistentes com a política de gestão de provedores de serviços.	Resposta da unidade auditada à RDIM expedida pela equipe de auditoria à STI/COINF[CGSC] (RDIM - SEI 0008530-84.2022.6.14.8000).

Causas	Consequências do Achado
Ausência de itens na gestão contratual, específicos para **SI**, que garantam a notificação e resposta a incidentes de segurança e/ou violação de dados, requisitos de criptografia e descarte de dados.	Prejuízo potencial na aplicação de sanção contratual, no caso de violação de requisitos de segurança.

ACHADO A5 - POSSIBILIDADE DE UTILIZAÇÃO DE SENHAS COM BAIXO NÍVEL DE COMPLEXIDADE POR PARTE DOS USUÁRIOS	
N° do Teste	**Situação Encontrada**
T6/T7 e T12	Através da RDIM (processo SEI 0008530-84.2022.6.14.8000), o auditado informou que ainda é possível o usuário cadastrar senhas com baixo nível de complexidade.

Critérios de Auditoria	Evidências
CIS V8 - Medida de Segurança 5.2 - utilizar senhas exclusivas para acesso aos ativos corporativos.	Resposta da unidade auditada à RDIM expedida pela equipe de auditoria à STI/COINF[CGSC] (RDIM - SEI 0008530-84.2022.6.14.8000).

Causas	Consequências do Achado
A utilização de senhas com nível maior de complexidade, ainda está em implementação de acordo com nova política de senhas a ser instituída no TRE-PA.	Potencial de quebra de senha e acesso não autorizado aos ativos de TI.

ACHADO A6 - AUSÊNCIA DE INVENTÁRIO DE PROVEDORES DE SERVIÇOS	
N° do Teste	**Situação Encontrada**
T8	Através da RDIM (formalizada no processo SEI 0008530-84.2022.6.14.8000), a unidade auditada informou que atualmente ainda não mantém um inventário com os provedores de serviço.

Critérios de Auditoria	Evidências
CIS V8 - Medida de Segurança 15.1 e 15.2 - o inventário deve listar todos os provedores de serviços, incluindo suas classificações (sensibilidade de dados, volume de dados, requisitos de disponibilidade, regulamentos aplicáveis e riscos).	Resposta da unidade auditada à RDIM expedida pela equipe de auditoria à STI/COINF[CGSC] (RDIM - SEI 0008530-84.2022.6.14.8000).

Causas	Consequências do Achado
Ausência de política de gestão de provedores de serviços, que formalize a manutenção de um inventário, com a devida revisão e atualização.	Prejuízo potencial do processo de tomada de decisão em relação aos prestadores de serviços, devido à ausência de informações consistentes e centralizadas.

ACHADO A7 - AUSÊNCIA DE NORMATIVOS/POLÍTICAS ESPECÍFICOS QUANTO À SEGURANÇA DA INFORMAÇÃO NA CONTRATAÇÃO OU PRESTAÇÃO DE SERVIÇOS	
N° do Teste	**Situação Encontrada**
T11	Através da RDIM (processo SEI 0008530-84.2022.6.14.8000), o auditado informou a ausência de políticas específicas nas contratações ou prestação de serviços de TI.

Critérios de Auditoria	Evidências
CIS V8 - Medidas de Segurança 15.2 e 15.4 - instiuição de políticas para gestão de provedores e inclusão de requisitos de segurança em contratos.	Resposta do auditado à RDIM expedida pela equipe de auditoria à STI/COINF[CGSC](RDIM - SEI 0008530-84.2022.6.14.8000).

Causas	Consequências do Achado
Atualmente a unidade auditada observa os critérios previstos nas normas: 1) IN SGD/ME nº 1/2019; 2) Resolução CNJ Nº 468/2022; 3) Portaria SGD/ME Nº 6.432/2021.	**[1]**Potencial violação desproposital de aspectos de segurança da informação por parte do provedor de serviços. **[2]**Impossibilidade de aplicação de sanção contratual.

ACHADO A8 - UTILIZAÇÃO, EM ESTÁGIO INICIAL, DE MECANISMOS DIVERSOS DE AUTENTICAÇÃO DO USUÁRIO	
N° do Teste	**Situação Encontrada**
T12	Através da RDIM (formalizada no processo SEI 0008530-84.2022.6.14.8000), a unidade auditada informou que a maioria dos sistemas críticos utilizam apenas uma forma de autenticação.

Critérios de Auditoria	Evidências
CIS V8 - Medidas de Segurança 6.3, 6.4 e 6.5 - utilização de MFA para acesso a aplicativos expostos externamente, acesso remoto à rede e acesso administrativo.	Resposta da unidade auditada à RDIM expedida pela equipe de auditoria à STI/COSIS(RDIM - SEI 0008530-84.2022.6.14.8000).

Causas	Consequências do Achado
Adoção de mecanismos com multifator de autenticação está em processo de padronização no provimento do acesso a serviços e soluções de TI.	Potencial acesso remoto indevido aos ativos de TI, através de técnicas de quebra de segurança de autenticação.

ACHADO A9 - AUSÊNCIA DE PROCEDIMENTO NORMATIZADO DE IDENTIFICAÇÃO E GESTÃO DO ACESSO DOS PRESTADORES DE SERVIÇOS	
N° do Teste	**Situação Encontrada**
T13	Através da RDIM (formalizada no processo SEI 0008530-84.2022.6.14.8000), a unidade auditada informou que controla o acesso dos prestadores de serviço, com a devida autorização, registros e acompanhamentos

Critérios de Auditoria	Evidências
CIS V8 - Medidas de Segurança 15.1, 15.6 e 15.7 - a gestão dos provedores de serviços deve envolver o acesso, monitoramento e descomissonamento, obedecendo-se os requisitos de segurança.	Resposta da unidade auditada à RDIM expedida pela equipe de auditoria à STI/COINF[CGSC] (RDIM - SEI 0008530-84.2022.6.14.8000).

Causas	Consequências do Achado
São adotados procedimentos para controle de acesso físico aos ativos de TI por parte dos prestadores de serviços, contudo tais procedimentos não estão normatizados.	[1]Potencial descontinuidade dos procedimentos de controle de acesso físico. [2]Acesso indevido aos recursos de TI.

VIII. ACHADOS POSITIVOS

13. Embora, em regra geral, o achado de auditoria seja caracterizado como um ato praticado em desconformidade com determinado padrão ou norma, também é possível identificar boas práticas de gestão durante os exames aplicados. Essas boas práticas podem ser denominadas de achados positivos, conforme apresentado nos quadros a seguir.

TESTE	ACHADOS POSITIVOS - GESTÃO DE PROVEDOR DE SERVIÇOS
T1	No PAC (plano anual de capacitação) da STI são incluídos treinamentos específicos em segurança da informação, que são direcionados aos servidores que geralmente integram a equipe técnica das contratações.
T2	Os documentos DOD, ETP, TR/PB possuem requisitos de segurança da informação (ex: termos de confidencialidade), incluídos em forma de anexo. Por exemplo, ANEXO I - TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO, CTO 77/2021 (Solução Integrada de Colaboração e Comunicação Corporativa, em Ambiente de Nuvem - 77/2021).
T4/T9	Apesar de ainda não se ter um processo de gestão de riscos (específico para segurança da informação - SI) para a execução contratual, são abordados aspectos de SI durante o planejamento da contratação e Seleção de Fornecedor, realizado nos Estudos Preliminares da Contratação.
T8	Apesar de não se ter instituído um inventário de prestadores de serviços, a STI define um contato corporativo para cada provedor de serviço. Adicionado ao controle da vigência contratual dos provedores de serviço, que é realizado pela Seção de Contratos - SECON/COLIC e acompanhado pela gestão da fiscalização de cada contrato.
T11	Apesar de não se ter instituído normativos/políticas específicos para a segurança da informação, a STI adota as seguintes normas: 1) Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019; 2) Resolução CNJ Nº 468/2022; e 3) Portaria SGD/ME Nº 6.432/2021.
T13	Apesar de não se ter um procedimento instituído para identificar os prestadores de serviço, a STI repassa (frequentemente) informações suficientes para a segurança institucional identificá-los precisamente.

TESTE	ACHADOS POSITIVOS - GESTÃO DE CONTAS E CONTROLE DE ACESSO
T6/T7 T12	A STI adota práticas seguras e consolidadas na gestão de contas, senhas e controle de acesso, que estão implementadas através da PSI-NC.001.001 e da PSI-NC.006.001. Envolvendo a periodicidade na revisão das contas/privilégios de acesso, bloqueio automático de contas sem acesso por um dado período de tempo, procedimento padrão para descomissionar com segurança os privilégios de usuários desligados/realocados. Além disso, são adotados controles para que as senhas sejam trocadas obrigatoriamente antes do primeiro login, e ainda que essas senhas expirem periodicamente.
T6/T7 T12	Apesar da STI está em fase inicial de utilização de MFA (autenticação multifator) nos sistemas desenvolvidos por sua equipe técnica, é válido mencionar que a COSIS tem envidado esforços na evolução dos mecanismos de autenticação, adotando ferramentas que são padrão de mercado, como por exemplo o *Keycloak*, que fornece autenticação a aplicativos e serviços de forma segura e unificada, permitindo a conexão com a base corporativa de usuários (AD - *Active Directory*), autenticação forte, gerenciamento de usuários, autorização refinada, dentre outros recursos.

IX. PROPOSTAS DE ENCAMINHAMENTOS E RECOMENDAÇÕES

14. Diante do exposto, submete-se o relatório final para ciência da Presidência, da Diretoria-Geral e da Secretaria da Tecnologia da Informação do TRE/PA, sobre os resultados obtidos nesta auditoria integrada.

15. Este relatório final será encaminhado ao TSE, para compilação dos resultados no Relatório Consolidado da Auditoria Integrada, que apresentará os achados recorrentes e relevantes a toda Justiça Eleitoral. O relatório consolidado deverá ser levado ao conhecimento da Alta Administração do TSE e dos TREs, conforme disposto no art. 6º da Resolução TSE nº 23.500/2016.

a) À Secretaria de Tecnologia da Informação (STI):

Descrição	Achados
Recomendação nº 1 (R1) - Estabeleça procedimento para normatização acerca de uma política de gestão de provedores de serviços. Essa política deve abordar a **classificação, inventário, avaliação, monitoramento e descomissionamento** de provedores de serviços. Além disso, a política instituída deve estabelecer também períodos de revisão e atualização periódica.	**A1, A2 e A6**
Recomendação nº 2 (R2) - Implemente um **inventário de prestadores de serviços**, que forneça um repositório de todos os provedores de serviços, com seu respectivo contato corporativo. Esse inventário, pode classificar os provedores através de características, tais como sensibilidade de dados, volume de dados, requisitos de disponibilidade, regulamentos aplicáveis. O inventário implementado deve ser revisto e atualizado periodicamente.	**A6**
Recomendação nº 3 (R3) - Inicie procedimentos para formalização de um processo de gestão contratual, que inclua **aspectos específicos de segurança da informação** (**SI**), abrangendo o planejamento, a execução de contratos (conclusão e rescisão - descomissionamento) e o gerenciamento de riscos. Além de itens que assegurem a notificação e resposta a incidentes de segurança e/ou violação de dados, requisitos de criptografia de dados e compromissos de descarte de dados (termos de compromissos/confidencialidade/sigilo).	**A2, A3, A4 e A7**
Recomendação nº 4 (R4) - Implemente mecanismos de configuração de senhas que assegurem a **utilização de senhas fortes** (letras, números e, se possível, caracteres especiais), por parte dos usuários. Como por exemplo, práticas recomendadas incluem, no mínimo, uma senha de 8 caracteres para contas que usam MFA (Autenticação Multifator) e uma senha de 14 caracteres para contas que não usam MFA.	**A5**
Recomendação nº 5 (R5) - Estabeleça políticas, padrões e guias que exijam a **implementação de recursos de MFA** (Autenticação Multifator) em sistemas expostos externamente, para acesso remoto à rede interna do TRE (ex: VPN). O que deve também ser observado, de forma combinada, com a Recomendação R4.	**A8**
Recomendação nº 6 (R6) - Normatize os procedimentos de **controle de acesso físico** aos setores institucionais, por parte dos prestadores de serviços de TI. Envolvendo também, mecanismos de monitoramento e revogação do acesso, obedecendo os requisitos de segurança da informação.	**A9**

X. CONCLUSÃO

16. Nesta auditoria integrada, foram avaliados controles referentes à gestão de provedores de serviço (interno e externo), gestão de contas e controle de acesso aos recursos corporativos de TI, segundo consta no *framework* CIS Controls V8, adotado como critério desta auditoria.

17. Para tanto, foram executados os procedimentos de testes e verificações, conforme programa de auditoria enviado pelo TSE, o que resultou na em 09 (nove) achados de auditoria. Estes achados devem ser considerados como oportunidades de melhoria, e consequente aumento no nível de maturidade da gestão de segurança da informação no TRE/PA.

18. As propostas de encaminhamentos e recomendações, apresentadas neste relatório, visam contribuir para o aumento do nível de segurança cibernética da informação no TRE/PA. Essas recomendações, juntamente com as iniciativas dos gestores de TI, direcionadas à adoção de padrões, práticas e modelos nos processos de trabalho, impulsionam a implementação de inovação e melhorias no objeto auditado.

19. Por fim, todos os produtos gerados, ao longo dos trabalhos, materializam o resultado desta auditoria integrada, que visa agregar valor aos produtos e serviços fornecidos pelo TRE/PA, contribuindo para a manutenção da imagem institucional da Justiça Eleitoral perante à sociedade.

Belém, 17 de Agosto de 2022.

Marco Antonio Fagundes de Moraes
Auditor Responsável - SECOI

Fabrício Manoel Santiago Cordeiro
Auditor - Chefe da SEAP

Hugo Hyago de Carvalho Mendonça
Auditor - SEAP

ANEXO I - QUADRO SINTÉTICO DOS ACHADOS DE AUDITORIA

Achados	Descrição
A1	Ausência de mecanismos de monitoramento quanto à segurança da informação durante a execução contratual, especialmente no trabalho remoto.
A2	Ausência de critérios instituídos quanto à segurança da informação para avaliar/atestar o objeto ou serviço prestado durante a execução contratual.
A3	Possibilidade do aceite de objeto/serviço sem garantia dos requisitos da segurança da informação.
A4	Ausência de assinatura nos termos de compromisso e ciência com a declaração de confidencialidade e sigilo
A5	Possibilidade de utilização de senhas com baixo nível de complexidade por parte dos usuários.
A6	Ausência de inventário de provedores de serviços.
A7	Ausência de normativos/políticas específicos quanto à segurança da informação na contratação ou prestação de serviços.
A8	Utilização, em estágio inicial, de mecanismos diversos de autenticação do usuário.
A9	Ausência de procedimento normatizado de identificação e gestão do acesso dos prestadores de serviços.

ANEXO II - QUADRO SINTÉTICO DAS RECOMENDAÇÕES

Nº da Recomendação	Descrição	Achados
R1	Trata da política de gestão de provedores de serviços.	**A1, A2 e A6**
R2	Trata do inventário de prestadores de serviços.	**A6**
R3	Trata do processo de gestão contratual com inclusão de aspectos específicos de segurança da informação (SI).	**A2, A3, A4 e A7**
R4	Trata da implementação de senhas fortes.	**A5**
R5	Trata da implementação de MFA (Autenticação Multifator).	**A8**
R6	Trata do controle de acesso físico aos setores institucionais, por parte dos prestadores de serviços de TI.	**A9**

ANEXO III - QUADRO SINTÉTICO DOS ACHADOS POSITIVOS

ID	ACHADOS POSITIVOS - GESTÃO DE PROVEDOR DE SERVIÇOS
1	O PAC (plano anual de capacitação) da STI inclui treinamentos específicos em segurança da informação (SI).
2	Os documentos DOD, ETP e TR/PB incluem requisitos de SI.
3	O planejamento da contratação e a seleção de fornecedores incluem requisitos de SI.
4	A STI define um contato corporativo para cada provedor de serviço.
5	A STI adota as seguintes normas nas contratações: 1) Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019; 2) Resolução CNJ Nº 468/2022; e 3) Portaria SGD/ME Nº 6.432/2021.
6	A STI repassa informações suficientes para a segurança institucional identificar os prestadores de serviços.