TRIBUNAL REGIONAL ELEITORAL DE MATO GROSSO DO SUL
R. Desembargador Leão Neto do Carmo, 23 - Bairro Parque dos Poderes - CEP 79037-100 - Campo Grande - MS

RELATÓRIO FINAL DE AUDITORIA

AUDITORIA INTEGRADA NO PROCESSO DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

PREÂMBULO

PROCESSO SEI: 0003545-29.2022.6.12.8000.

CLIENTE(S): Secretaria da Tecnologia da Informação – STI.

ATO ORIGINÁRIO: Plano Anual de Auditoria – PAA, referente ao exercício 2022 (ID *1125778*), aprovado pelo Pleno (ID 1129880), em 8 de dezembro de 2021, conforme processo SEI nº 0006715-43.2021.6.12.8000, bem como Plano de Auditoria de Longo Prazo das Auditorias Integradas – PALP, do Tribunal Superior Eleitoral – TSE, exercício 2022-2025, aprovado pela Portaria TSE nº 761/2021.

OBJETIVO: Avaliar o processo de Gestão de Segurança da Informação, com enfoque no processo de gerenciamento de provedores de serviço e seus respectivos contratos, e 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.

PERÍODO DE ANÁLISE: junho/2020 a junho/2022.

PERÍODO DE REALIZAÇÃO DA AUDITORIA: abril a agosto/2022.

EQUIPE: Alessandra Falcão Gutierres de Souza (supervisora da auditoria), Nivaldo Azevedo dos Santos (líder de equipe), Flávio Alexandre Martins Nichikuma e Manuela Baptista Velasquez Shoji (auditores).

ATO DE DESIGNAÇÃO: Portaria Presidência nº 169/2022 TRE/PRE/GABPRE (ID 1207134), publicada no DJEMS nº 85, de 09 de maio de 2022, página 2.

RESUMO

❶ Porque a auditoria foi realizada?

A AUDIN realizou a presente auditoria no Processo de Gestão de Segurança da Informação em cumprimento ao Plano Anual de Auditoria – Exercício 2022 e ao Plano de Auditoria de Longo Prazo das Auditorias Integradas (PALP TSE) 2022-2025, aprovado pela Portaria-TSE nº 761/2021 e conforme Resolução TSE nº 23.500/2016. O objetivo foi avaliar a existência e a qualidade dos controles internos instituídos no processo de Gestão de Provedores de Serviço, Gestão de Contas e Gestão de Controle de Acesso aos ativos de informação do TRE/MS. A metodologia adotada foi a ABR (Auditoria Baseada em Riscos) e, nas análises, foram aplicados, como critérios de auditoria, os controles 5, 6 e 15 do *framework* CIS *Controls* v.8 e normativos do CNJ, TSE e TRE/MS afetos especificamente à segurança cibernética. Os trabalhos de auditoria foram realizados no período de 26/04/2022 a 17/08/2022, de forma conjunta e concomitante pelas unidades de Auditoria do TSE e dos TREs, sob a coordenação, supervisão e orientação da Secretaria de Auditoria (SAU/TSE). O Relatório de Auditoria será encaminhado às unidades interessadas do TRE/MS, para ciência e adoção das providências pertinentes, bem como à Secretaria de Auditoria do TSE, para a consolidação dos principais achados e a elaboração do Relatório Consolidado da Auditoria Integrada.

❷ O que foi encontrado?

Como resultado da comparação entre a situação encontrada e os critérios estabelecidos, foram descobertos 9 (nove) achados, devidamente comprovados por evidências e documentados em papéis de trabalho. Entretanto, também se identificou que o

Tribunal executa de forma satisfatória diversas ações de segurança cibernética e, em grande parte, aplica controles adequados para proteção de seus ativos de informação. Ademais, constatou-se o comprometimento no cumprimento da Estratégia Nacional de Cibersegurança da Justiça Eleitoral (2021 a 2024) e na observância dos prazos nela estabelecidos. Ocorre que, não obstante a existência de expressivos avanços em SI já em execução ou em vias de implantação, há ainda grande margem para aperfeiçoamento das ações de cibersegurança no TRE/MS, quanto a provedores de serviços, contas de usuários e controle de acesso. Assim, dentro de um observatório amplo, a auditoria detectou o seguinte cenário: (I) inexistência de uma cultura de Segurança da Informação (SI) no âmbito do TRE/MS (unidades/agentes); (II) ausência de unidade específica, na STI, formalizada regimentalmente e especializada em SI, com competência voltada à implementação e fomento de medidas para proteger os ativos de informação do TRE/MS (Prazo: Até 2021 – ENCiber-TSE); (III) inexistência de Gestor de Segurança da Informação junto à PRE ou DG (Prazo: Até 2023 – ENCiber-TSE); (IV) inexistência de alinhamento de conhecimento quanto à SI; (V) Política de Segurança da Informação ainda incipiente; (VI) normativos internos incompletos ou desatualizados.

❸ O que foi proposto?

Com o propósito de agregar valor e melhorar os processos organizacionais de segurança cibernética, para cada achado foram feitas sugestões de recomendações com a finalidade de eliminar as causas, mitigar suas consequências ou até mesmo incorporar uma boa prática, dentre as quais destacamos: (1) proporcionar que todos os agentes públicos e colaboradores do TRE/MS sejam conscientizados, capacitados e treinados em segurança da informação; (2) implementar modelos de ETP/TR/PB/minuta contratual com elementos mínimos acerca da SI, de forma a padronizar os documentos de planejamento da contratação de TIC; (3) excluir do *Active Directory* (AD) as contas ativas de usuários que não possuem mais vínculo com o TRE/MS, estabelecer uma regra para exclusão ou desabilitação de contas com alongado tempo de inatividade e instituir, na unidade competente da STI (SGI), rotina para a efetiva realização de revisões periódicas nas contas de usuários do AD, preferencialmente de forma automatizada; (4) propor a atualização/adequação dos normativos internos reguladores de SI e fomentar a cultura de segurança da informação, de forma a promover a aplicação efetiva dos normativos correspondentes, tais como Resoluções CNJ 396/2021 e Resolução TSE nº 23.644/2021; (5) incluir nas licitações/contratações a obrigatoriedade de observância dos normativos relativos à SI; (6) realizar a classificação e o inventário de provedores de serviços e instituir a respectiva Política de Gestão; (7) implementar o Múltiplo Fator de Autenticação (MFA) nos acessos remotos à rede e nos sistemas críticos.

❹ Quais os benefícios esperados?

Com o cumprimento das sugestões de recomendações apontadas nesta auditoria, espera-se alcançar os seguintes benefícios: a) aperfeiçoamento da Governança (Adm./TIC), com o aprimoramento dos controles e a mitigação dos riscos de ataques cibernéticos; b) corpo técnico qualificado nas atividades de segurança da informação; c) ganho de qualidade e eficiência nos processos internos que envolvam segurança cibernética (Ex. licitações/contratos); d) cumprimento da EN Cibersegurança da JE (2021/2024) e; e) alinhamento com as boas práticas internacionais de combate a ataques cibernéticos.

LISTA DE SIGLAS

AD	Active Directory
AUDIN	Auditoria Interna
CIS	Center for Internet Security
CITIS	Coordenadoria de Infraestrutura de Tecnologia da Informação e Suporte
CNJ	Conselho Nacional de Justiça
CODESC	Coordenadoria de Desenvolvimento de Soluções Corporativas
DG	Diretoria-Geral
EN	Estratégia Nacional
GABPRE	Gabinete da Presidência
GTA	Grupo de Trabalho de Auditoria Integrada
JE	Justiça Eleitoral
MFA	Autenticação Multifator
NSI	Núcleo de Segurança Institucional
PAA	Plano Anual de Auditoria
PRE	Presidência
PSI	Política de Segurança da Informação
RDIM	Requisição Documentos, Informações e Manifestações
SAF	Secretaria de Administração e Finanças
SEAUT	Seção de Auditoria de Tecnologia da Informação
SEI	Sistema Eletrônico de Informações
SGD/ME	Secretaria de Governo Digital do Ministério da Economia
SI	Segurança da Informação
TCU	Tribunal de Contas da União
TIC	Tecnologia da Informação e Comunicação
TRE/MS	Tribunal Regional Eleitoral de Mato Grosso do Sul
TSE	Tribunal Superior Eleitoral

I – INTRODUÇÃO

A área de gestão de segurança da informação foi prevista para ser auditada no Plano de Auditoria de Longo Prazo das Auditorias Integradas – PALP, exercício 2022-2025, do TSE, aprovado pela Portaria TSE nº 761/2021, e no Plano Anual de Auditoria – PAA do TRE/MS (ID *1125778*), referente ao exercício 2022, aprovado pelo Pleno (ID 1129880), em 8 de dezembro de 2021, conforme processo SEI nº 0006715-43.2021.6.12.8000. Desse modo, é parte integrante do conjunto de auditorias realizadas simultaneamente em todos os Tribunais Eleitorais do país, na sistemática de auditoria integrada, em conformidade com a Resolução TSE nº 23.500/2016.

A coordenação das atividades da auditoria, em âmbito nacional, ficou a cargo da Coordenadoria de Auditoria de Governança e Gestão de Aquisições – COAUG/TSE, apoiada pela Seção de Auditoria de Tecnologia da Informação – SEAUT/TSE, sendo

instituído pela Portaria TSE nº 372/2022 o Grupo de Trabalho de Auditoria Integrada – GTA, para padronização dos procedimentos e papéis de trabalho, adequados ao objeto auditado.

Com vistas a subsidiar a determinação do escopo da auditoria, elaborou-se o Plano de Trabalho (ID 1235011), em modelo padrão do GTA/TSE, no qual foram definidos o objetivo, a técnica a ser aplicada, o objeto dos exames, os meios e o tempo demandado para a sua concretização.

Foram realizadas reuniões de abertura (ID 1211630), comunicações/entrevistas para mapeamento do processo (SEI nº 0003634-52.2022.6.12.8000) e elaboração das matrizes de riscos (SEI nº 0004715-36.2022.6.12.8000) e reunião de encerramento dos trabalhos (ID 1260528) entre a equipe de auditoria e os gestores responsáveis pelo processo auditado.

Na reunião de encerramento, foram apresentados os resultados das análises, as recomendações e orientações da equipe por meio da Matriz de Achados Propositivos (ID 1259103). Oportunizada a manifestação do cliente da auditoria (STI) e demais unidades impactadas (SAF), as respostas foram consideradas e incluídas neste Relatório Final.

II – VISÃO GERAL DO OBJETO AUDITADO

É notório que a preocupação com os controles de segurança da informação vem ganhando força no mercado e nas instituições públicas, considerando que "*a informação é um ativo essencial para os negócios de uma organização e, consequentemente, ela necessita ser adequadamente protegida*" (NBR ISO/IEC 27002:2005).

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.

De acordo com o relatório de segurança da Symantec constante na 24ª edição do *Internet Security Threat Report* (ISTR), de fevereiro/2019, o Brasil é o principal alvo de ataques cibernéticos na América Latina, sendo o 4º no ranking mundial. Mais recentemente, segundo um relatório da empresa especializada Netscout, o Brasil assumiu a segunda posição entre os maiores alvos de ataques cibernéticos no mundo, atrás apenas dos Estados Unidos.

No âmbito do Judiciário, tem sido comum presenciar eventos de ataques cibernéticos, vide os ataques ao Superior Tribunal de Justiça – STJ (novembro/2020), Supremo Tribunal Federal – STF (maio/2021), TJ-RS (novembro/2020 e abril/2021) e TRF-3 (janeiro/2021 e março/2022).

A Justiça Eleitoral, que possui a crítica missão de liderar e organizar as etapas do processo eleitoral brasileiro, representando instrumento essencial da democracia, é um dos principais alvos de ataques cibernéticos. Em vista disso, a temática da Segurança Cibernética no TSE se tornou ainda mais relevante, em especial com 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.

Nesse sentido, o TSE aprovou a Estratégia Nacional de Cibersegurança, com o objetivo de direcionar "diversas ações em segurança cibernética necessárias para o ganho de maturidade em capacidade de identificação, proteção, detecção, resposta e recuperação de incidentes de segurança relacionados com a presença das instituições referenciadas no ciberespaço". A iniciativa complementa os demais normativos recentes publicados no Poder Judiciário e no TSE, tal como a Portaria CNJ nº 162, de 10 de junho de 2021, que aprova Protocolos e Manuais criados pela Resolução CNJ nº 396/2021, bem como a Política de Segurança da Informação – PSI da JE, instituída pela Resolução TSE nº 23.644, de 1º de julho de 2021.

Tendo em vista a gama de possibilidades que englobam o tema segurança da informação, o GTA/TSE, adotando como critério os controles desenvolvidos pelo *Center for Internet Security* (CIS), o CIS *Controls* versão 8, escolheu que os exames de auditoria se debruçassem sobre 3 (três) processos: i) processo de gerenciamento de provedores de serviço e seus respectivos contratos, no tocante à segurança da informação (controle 15); ii) processo de gestão do controle de acessos (controle 6) e; i) processo de gestão de contas (controle 5).

A partir das respostas obtidas (ID 1217630) com a aplicação de questionário ao cliente da auditoria, de entrevistas e observação direta, será apresentada abaixo a visão geral da segurança da informação no âmbito do TRE/MS.

Nos termos da Resolução TRE/MS nº 749/2021, este Regional adotou o PSI do TSE. Além disso, em 2018, instituiu a Comissão de Segurança da Informação (Portaria Presidência nº 170/2018 TRE/PRE/DG/GABDG) e designou Gestores de Segurança da Informação (Portaria Presidência nº 178/2018 TRE/PRE/DG/GABDG); em 2019, instituiu o Sistema de Gestão de Segurança da Informação – SGSI, por intermédio da Portaria Presidência nº 195/2019 TRE/PRE/DG/GABDG, e criou uma Política de Gestão de Riscos de Segurança da Informação (Portaria Presidência nº 259/2019 TRE/PRE/ASJES), além de normatizar o processo de elaboração, monitoramento e revisão da Política de Segurança da Informação – PSI do TRE/MS (Portaria Presidência nº 262/2019 TRE/PRE/DG/AEDG) e instituiu a Política de Controle de Acesso Físico e Lógico relativamente à SI (Resolução TRE/MS n. 663/2019).

Contudo, o modelo atual de gestão da SI é baseado em comissões instituídas, o que remete à necessidade de readequação da estrutura de segurança da informação na Justiça Eleitoral, a fim de que a instituição conte com uma estrutura mínima para ações preventivas e reativas compatíveis com os riscos que se apresentam, nos termos da *Proposta de estrutura organizacional para a segurança da informação e cibersegurança no âmbito da Justiça Eleitoral* (ID 1079079). Desse modo, a STI solicitou a criação de uma unidade organizacional de caráter permanente para tratar dessas questões, conforme SEI nº 0006249-49.2021.6.12.8000, ainda em análise na Diretoria-Geral.

Verifica-se que na gestão de segurança da informação, a STI não aplica o conjunto de controles do CIS *Controls*, versão 8 ou versões anteriores, embora tenha informado que está em estudo a adoção do *framework* para fomentar a gestão de riscos de segurança.

Quanto aos Protocolos e Manuais aprovados pela Portaria CNJ nº 162/2021, ainda não foram implementados por esta Corte Eleitoral (ID 1091050).

III – OBJETIVO DA AUDITORIA

Este trabalho de auditoria tem 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;

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

A necessidade de se proteger dados é premente na sociedade moderna. Para os órgãos da Administração Pública, que se utilizam de inúmeros relacionamentos com colaboradores, empresas e prestadores de serviço para a consecução de suas atividades, a segurança da informação se torna fundamental.

Frente a isso, selecionou-se como objeto de avaliação para esta ação o controle 15 do CIS *Controls*, versão 8, denominado Gestão de Provedores de Serviço. Segundo o CIS, esse é um processo para avaliar os provedores de serviços que mantêm dados sensíveis, ou que são responsáveis por plataformas ou processos de tecnologia da informação críticos de uma organização para garantir que esses provedores estejam protegendo as plataformas e os dados de forma adequada.

Além do controle acima citado, a presente ação de auditoria também abarcou os controles 5 e 6, que tratam, respectivamente, da Gestão de Contas e da Gestão do Controle de Acesso. Esses temas, em vários casos, possuem interrelação direta com o primeiro, pois 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 para ativos e *softwares* corporativos, melhorando, assim, a segurança tecnológica da instituição.

As análises desenvolvidas compreenderam o período de junho/2020 a junho/2022.

V – CRITÉRIOS

Os critérios utilizados como parâmetros para fundamentar as avaliações apresentadas neste trabalho foram os seguintes:

a) Controles 5, 6 e 15 do CIS *Control* Versão 8, de maio 2021;

b) Lei nº 13.709/2018 (LGPD);

c) Resolução CNJ nº 396/2021 (Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário - ENSEC-PJ);

d) Portaria CNJ nº 162/2021 (Aprova Protocolos e manuais criados pela Res. CNJ 396/2021);

e) Resoluções do TSE nº 23.644/2021 e nº 23.650/21 (Dispõe sobre a Política de Segurança da Informação -PSI, no âmbito da Justiça Eleitoral);

f) IN nº 01/2019 SGD/ME;

g) Resoluções do TRE/MS nº 663/2019; nº 604/2021; nº 690/2021; nº 740/2021 e nº 749/2021 e;

h) Portarias da Presidência do TRE/MS, em matéria de segurança da informação, como Portarias nº 170/2018, nº 178/2018, nº 195/2019, nº 259/2019 (alterada pela Portaria nº 262/2019) e nº 262/2019.

VI – METODOLOGIA ABR[1]

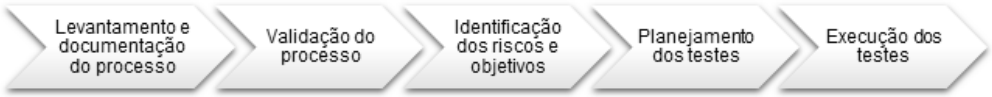
Os trabalhos de auditoria foram fundamentados na aplicação de técnicas de *Risk Assessment*, Auditoria Baseada em Risco (ABR), direcionados aos processos de trabalho e à mitigação dos riscos relacionados à consecução das atividades administrativas do TRE/MS.

Essa metodologia permite ao auditor testar os controles mais importantes, ou focar nas áreas estratégicas, otimizando os recursos humanos e materiais disponíveis:

VII - AVALIAÇÃO DOS CONTROLES INTERNOS

Conforme recomendam o Tribunal de Contas da União (TCU) e o Instituto dos Auditores Internos do Brasil (IIA Brasil), ao se planejar os trabalhos de auditoria em uma entidade ou atividade administrativa, deve-se avaliar a existência e a qualidade dos controles internos instituídos pelos gestores responsáveis.

As etapas da avaliação de controles internos são as seguintes:



A equipe de auditoria elaborou, em conjunto com os gestores das áreas responsáveis, o levantamento e a documentação do processo de trabalho da atividade auditada. Após o levantamento dos processos e a validação pelos gestores, foram identificados quais os objetivos de cada fase do processo, com seus riscos associados e os controles instituídos pelos gestores para administrar esses riscos, sendo encaminhado ao GTA/TSE 6 (seis) matrizes de testes, nas quais foram listados 29 (vinte e nove) testes, com 8 (oito) direcionados a riscos altos de segurança cibernética.

Em razão da dinâmica das auditorias integradas, a SEAUT/GTA padronizou 8 (oito) testes a serem realizados por todos os Regionais, conforme o Programa de Auditoria Padrão do TSE (ID 1239289). Ainda, ficou a cargo de cada Tribunal Eleitoral executar os seus próprios testes, com a cautela de evitar a repetição de testes. No caso do TRE/MS, dos 29 (vinte e nove) testes listados, 8 (oito) são direcionados a riscos altos de segurança cibernética e equivalentes aos testes determinados pela SEAUT/GTA. Desse modo, optou-se por trabalhar com a matriz de testes consolidada pelo TSE, aplicando todos os 8 (oito) testes nela previstos (5 coincidentes + 3 adicionais obrigatórios), acrescidos de mais 2 (dois) testes próprios de grande relevância para o resultado da auditoria, conforme o Programa de Auditoria da AUDIN/TRE/MS (ID 1238409).

VIII - RESULTADOS DOS EXAMES (ACHADOS DE AUDITORIA)

Os achados representam o resultado dos testes de auditoria aplicados e das informações coletadas nas reuniões de trabalho, guardando relação com o Programa de Auditoria (ID 1238409).

Das evidências coletadas, foram identificadas algumas situações/riscos que podem comprometer, em maior ou menor grau, os controles instituídos no processo auditado.

Foram detectados pontos positivos, como:

i) a existência de normativos de segurança da informação, cuja utilização, atualização e/ou aprimoramento precisa ser fomentado por esta Corte (Resolução TRE/MS nº 749/2021, que adota a Política de Segurança da Informação – PSI do TSE; Resolução TRE/MS nº 663/2019, que institui a Política de Controle de Acesso Físico e Lógico relativamente à SI; Portaria Presidência nº 259/2019 TRE/PRE/ASJES, que criou uma Política de Gestão de Riscos de Segurança da Informação);

ii) foi designada Comissão de Segurança da Informação, com as atribuições constantes do art. 23 da antiga Resolução nº 23.501/2016 do TSE, revogada pela Resolução nº 23.644/2021, art. 11, atual PSI da Justiça Eleitoral (Portaria Presidência nº 170/2018 TRE/PRE/DG/GABDG);

iii) foi solicitado termo de confidencialidade na contratação de Central de Serviço de Tecnologia da Informação;

iv) na contratação de Sistema de Testes Exaustivos de Urnas Eletrônicas – STE 2020 houve uma maior preocupação com SI, com previsão de regras específicas de SI, como os itens 5.4.4, e 5.11.7, do capítulo V, e item 14.1.10, do capítulo XIV, do Termo de Referência, embora sem formalização da confidencialidade por intermédio do respectivo termo.

Algumas situações, porém, apresentaram alguma distorção ou desconformidade passíveis de enquadramento como achados de auditoria.

A seguir, fundamentados no artigo 55 da Resolução CNJ nº 309/2020, apresentamos os achados de auditoria.

A1	CAPACITAÇÃO EM SEGURANÇA DA INFORMAÇÃO INSUFICIENTE

SITUAÇÃO ENCONTRADA: Analisadas as capacitações das unidades da STI (CITIS, NTI e CODESC), nos últimos 4 anos, verificou-se insuficiência de capacitação em Segurança da Informação. Com a tramitação da criação da unidade de Cibersegurança na STI, foram contratados diversos cursos em SI para este exercício (2022), entretanto, as capacitações não se estenderam a todos os servidores envolvidos diretamente com as contratações de provedores de serviço, assistência e suporte às demais unidades do TRE/MS. Em 2022, foram identificadas as seguintes capacitações: (i) Tratamento de Incidentes de Segurança; (ii) Fundamentos de Segurança da Informação; Tratamento de Incidentes de Segurança; (iii) Gestão de Riscos de Segurança da Informação e Privacidade. Os cursos foram distribuídos para servidores da STI (COCLE, CITIS e CODESC).

EVIDÊNCIAS: a) Sistema SEI - Capacitações; b) Sistema SGRH, módulo Capacitações; c) Planilha EXCEL extraída banco de dados SGRH, contendo capacitações de servidores no período de 2018-2022; d) SEI 0005421-53.2021.6.12.8000 e; e) SEI 0001645-11.2022.6.12.8000.

CRITÉRIOS: a) Controle 15 do CIS *Control* Versão 8, de maio/2021; b) Portaria CNJ nº 162/21, item 38, anexo I c/c item 2 - Programa Capacitação PCASC-PJ; c) Resoluções do TSE nº 23.650/21, art. 4, VII, e nº 23.644/21, art. 6, IV; d) IN 01/2019 SGD/ME, art. 16 e; e) Resolução CNJ nº 396/2021, art. 19, IV. c/c Art. 28, III.

POSSÍVEIS CAUSAS: a) Impossibilidade de priorização das medidas de SI em razão de outras demandas; b) Foco em outras áreas de TIC também relevantes; c) Pouco tempo de implantação da Política de Segurança da Informação no TRE/MS (Resolução nº 749, de 16/09/2021) e; d) Ausência de unidade técnica especializada em cibersegurança na estrutura da STI, para fomentar e acelerar a implantação de medidas de SI.

POSSÍVEIS CONSEQUÊNCIAS: a) Demora na efetivação das medidas de SI; b) Contratações de TIC que não atendam às necessidades do Tribunal em segurança da informação e; c) Desconformidade com normativos em segurança da informação (CNJ e TSE).

MANIFESTAÇÃO DO CLIENTE: A STI reconheceu a importância de ampliação das ações de capacitação em SI, todavia, destacou que a segurança da informação é responsabilidade de todos os servidores, magistrados, estagiários e terceirizados. Por essa razão, sugeriu que a proposta da AUDIN seja mais alongada e alcance todos os que atuam na Justiça Eleitoral de MS. A STI também destacou que o TRE-MS está adquirindo uma Plataforma de Capacitação e Sensibilização que poderá auxiliar no saneamento deste achado.

CONCLUSÃO DA EQUIPE DE AUDITORIA: A sugestão do cliente de auditoria merece acolhida e permitirá um ganho institucional maior, fazendo com que o conhecimento de SI seja alinhado entre os agentes e colaboradores e, ademais, atingirá toda a força de trabalho do TRE/MS, em todos os níveis de atuação (judicial e administrativo).

►RECOMENDAÇÕES (para STI e SGP):

1. Proporcionar que todos os agentes públicos e colaboradores do TRE/MS sejam conscientizados, capacitados e treinados em segurança da informação, de forma a promover o alinhamento do conhecimento em SI e a redução dos riscos na área de segurança cibernética;

2. Sem prejuízo das atividades eleitorais do pleito que se avizinha e de outras demandas igualmente relevantes, priorizar as ações de implantação da plataforma integrada de treinamento *on-line*, especializada na oferta de conteúdos de capacitação e conscientização em Segurança da Informação, cuja contratação já está em andamento (SEI 0004181-92.2022.6.12.8000).

Os recursos humanos do TRE/MS devem estar organizados, sensibilizados e dedicados às questões referentes à cibersegurança, exigências contidas no Eixo Estruturante 1: Pessoas e Unidades Organizacionais e no Eixo Estruturante 5: Sensibilização e Conscientização da Estratégia Nacional de Cibersegurança da Justiça Eleitoral 2021 a 2024.

A2	INEXISTÊNCIA DE CRITÉRIOS DE SI NO ETP/TR-PB/MINUTA DE CONTRATO E/OU AUSÊNCIA DE TERMOS DE CONFIDENCIALIDADE E SIGILO PREVISTOS

SITUAÇÃO ENCONTRADA: a) Nas contratações anteriores a julho/2020 não foram localizados critérios especificamente de SI nos documentos DOD/ETP/TR/PB, com exceção da contratação de Central de Serviços de TI, em que há o dever de sigilo das informações, mediante assinatura de Termo de Confidencialidade; b) Com a edição da Resolução nº 690/2020 (Código de Ética do TRE/MS), publicada em 03/07/2020, passou-se a exigir, nas minutas dos contratos e no Termo de Referência, a observância da confidencialidade ali prevista, inclusive pelos empregados da contratada, bem como a determinação de proteger informações confidenciais e privilegiadas, conforme regulamento próprio; contudo, sem exigir a formalização por meio de assinatura de um termo próprio de confidencialidade; c) Verificou-se, ainda que, além da observância do Código de Ética, na contratação de Sistema de Testes Exaustivos de Urnas Eletrônicas - STE 2020 houve uma maior preocupação com SI, com previsão de regras específicas nesta matéria, a saber: itens 5.4.4, e 5.11.7, do capítulo V, e item 14.1.10, do capítulo XIV do TR. Contudo, não houve a formalização da confidencialidade por intermédio do respectivo termo. Assim, verifica-se que a preocupação com cláusulas de SI depende do tipo de contratação de TIC; d) Quanto às sanções administrativas, são elaboradas pela Seção de Contratos/SEC/SAF e estão disciplinadas na minuta do contrato, sem referências específicas a casos de descumprimento de disposições relativas a SI; e) Das contratações a partir do segundo semestre de 2020, verifica-se a inclusão, nas minutas dos contratos, de cláusula determinando a observância da confidencialidade prevista no Código de Ética do TRE/MS, inclusive pelos empregados da contratada. Mas, não há menção de penalidade administrativa específica no caso de seu descumprimento e; f) A STI informou que está em fase de implementação nas novas contratações a solicitação de Termo de Compromisso, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes com ênfase em segurança da informação, firmados pelos prestadores de serviços, bem como respectivo Termo de Ciência da referida declaração, firmados pelos empregados da contratada diretamente envolvidos na contratação, ainda sem resultado prático.

EVIDÊNCIAS: a) Resposta da STI ao Questionário RDIM (ID 1248060) (questões 5 e 6), nos autos SEI 0005308-65.2022.6.12.8000; b) 0007090-78.2020.6.12.8000 (Rack Cofre): Documento de Oficialização de Demanda - DOD (ID 0900104), Estudos Preliminares - EP (ID 0906351), Termo de Referência - TR (ID 0956288) e Minuta do Contrato (ID 0956448); c) 0012417-72.2018.6.12.8000 e 0001862-54.2022.6.12.8000 (*Outsourcing* de impressão): DOD (ID 1063545), EP (ID 1065576), TR (ID 0654063) e Minuta do Contrato (ID 0654115); d) 0004285-55.2020.6.12.8000 (STE 2020): DOD (ID 0833927), EP (ID 0980099 e 0991457), TR (ID 1006399 – itens 5.4.4 e 5.11.7, do capítulo V, e item 14.1.10, do capítulo XIV) e; Minuta do Contrato (ID 1006405), cláusula 12.2 (dever de confidencialidade do Código de Ética do TRE/MS; e) 0004191-73.2021.6.12.8000 (Solução de *hardware* e *software* para VPN): DOD (ID 1063545), EP (ID 1065576), TR (ID 1107632 – item 6, do capítulo XI) e Minuta do Contrato (ID 1107633); f) 0007345-36.2020.6.12.8000 (Ferramenta de análise de *logs* (SIEM): DOD (ID 0906844), EP (ID 0915917), TR (ID 1108541 – item 1.8, 1.9, 1.10 e 1.11, do capítulo XI) e Minuta do Contrato (ID 1108542); g) 0003392-69.2017.6.12.8000 e 0002819-55.2022.6.12.8000 (Central de Serviço de TI): DOD (ID 0285035 e 1192625), EP (ID 0406952 e 1206476), TR (ID 0463519 – item 2, do capítulo XII), Termo de Confidencialidade de Informações (Anexo I – G – 0463762), Minuta do Contrato (ID 0463778) e Minuta da Prorrogação Contratual (ID 1222865); h) 0002904-75.2021.6.12.8000 (Solução para gestão do parque de UE integrada aos sistemas ASI e LOGUSWEB): DOD (ID 1031308), EP (ID 1089712), PB (ID 1091912 – itens 6 a 9, do capítulo XII) e Minuta do Contrato (ID 1118982 – item 12.2 da clausula décima segunda).

CRITÉRIOS: a) Controle 15.4 do CIS *Control* Versão 8; b) Lei nº 13.709/2018 (LGPD), art. 46; c) Resolução CNJ nº 396/2021, art. 28, IV; d) Resoluções do TSE nº 23.644/2021, arts. 7º, 8º, 24 e 27, e nº 23.650/2021, art. 1º, §§ 3º e 4º c/c art. 4º, VI; e) Resoluções do TRE/MS nº 690/2020 (Código de Ética do TRE/MS), art. 2º, VI c/c art. 4º, VII, e nº 749/2021 e; f) Art. 16, II, "i", da IN nº 01, de 04/04/2019, do Ministério da Economia.

POSSÍVEIS CAUSAS: a) Ausência ou falha na definição de uma política de gestão de segurança da informação; b) Percepção de que a política de gestão de segurança da informação é mera formalidade burocrática; c) Foco das práticas apenas nas informações sob gestão direta da organização, descuidando-se de informações armazenadas em nuvem ou sob custódia de terceiros; d) Licitações realizadas sem a padronização dos critérios de segurança da informação.

POSSÍVEIS CONSEQUÊNCIAS: a) Contratações que não atendam às necessidades do Tribunal em segurança da informação; b) Vazamento/furto de informações sigilosas; c) Danos à imagem da organização; d) Prejuízo ao erário.

MANIFESTAÇÃO DO CLIENTE: A STI manifestou de acordo, sem considerações ou ressalvas (ID 1261284). A SAF, através da CRM (ID 1264236), esclareceu que será analisada a possibilidade de inserção nas minutas de editais e contratuais dos seguintes dipositivos: Termo de Compromisso ou Acordo de Confidencialidade, Instrumento de Medição de Resultados com avaliação de critério de SI e sanções administrativas pelo descumprimento de requisitos de segurança da informação.

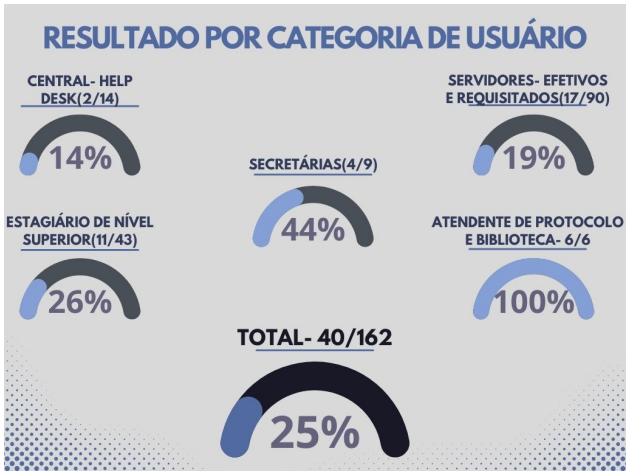
CONCLUSÃO DA EQUIPE DE AUDITORIA: Achado mantido.

►RECOMENDAÇÃO (para STI e SAF):

Implementar modelos de Estudos Técnicos Preliminares/Termo de Referência/Projeto Básico/Minuta Contratual com elementos mínimos acerca da SI, de forma a padronizar os documentos de planejamento da contratação de TIC (ex. termo de confidencialidade, previsão de glosas ou agravamento de sanções nos casos de violação de dados, notificação e resposta de incidente de segurança, medidas de segurança e privacidade dos dados coletados e armazenados pela contratada, etc.).

A3	EXISTÊNCIA DE SERVIDORES, REQUISITADOS, ESTAGIÁRIOS E COLABORADORES DESLIGADOS DO TRE/MS COM PERFIS ATIVOS NO SISTEMA DE GESTÃO E CONTROLE DE CONTAS (*ACTIVE DIRECTORY* - AD)

SITUAÇÃO ENCONTRADA: a) Após realizar o confronto da lista de usuários desligados do TRE/MS [servidores/requisitados (90), estagiários de nível superior (43) e colaboradores terceirizados (29)] com a de usuários ativos no *Active Directory* (AD), apurou-se a existência de contas ativas que deveriam ter sido canceladas e removidas do sistema, pois seus titulares não têm mais vínculo com o TRE/MS. Dos 162 (cento e sessenta e dois) desligamentos que ocorreram no período avaliado (junho/2020 a junho/2022), há 40 (quarenta) casos em que as contas estão atualmente ativas (25%), com usuário e senha ainda autenticados pelo AD. No caso das secretárias e atendentes de protocolo, em 100% dos casos (6 ocorrências) não houve o cancelamento do usuário; b) Ausência de comunicado formal de desligamento dos colaboradores, conforme relato da CITIS (ID 1250691); c) Inexistência de processo e/ou periodicidade de revisão das contas de usuários do AD, consoante relatou a CITIS (ID 1250691). A figura abaixo resume e ilustra os resultados apurados:



EVIDÊNCIAS: a) Planilha EXCEL com a listagem dos usuários ativos (ID 1250699); b) Planilha EXCEL de pessoas que perderam o vínculo com o Tribunal: (1) servidores/requisitados (ID 1249222), (2) Estagiários (ID 1248657), (3) colaboradores terceirizados (ID 1249341) e (4) colaboradores da central de serviços (ID 1250700); c) RDIM nº 04/2022 respondido pela CITIS (ID 1250691); d) RDIM nº 03/2022 respondido pela SAF (ID 1249341).

CRITÉRIOS: a) Controles 5.1 (inventário de contas), 5.3 (desabilitar contas inativas) e 5.5 (inventário de contas de serviços) do CIS *Controls* Versão 8 e; b) Resolução TRE/MS nº 663/2019, arts. 13 a 17.

POSSÍVEIS CAUSAS: a) Inexistência de monitoramento e revisões periódicas nas contas do AD; b) Ausência de comunicados, à STI, de desligamento de usuários pelas unidades competentes; c) Ausência de rotina de rastreamento das contas com alongado período de inatividade e; d) Inobservância do procedimento previsto no normativo de regência.

POSSÍVEIS CONSEQUÊNCIAS: a) Existência de contas válidas no AD mesmo após o rompimento do vínculo do usuário com o TRE/MS; b) Uso indevido das credenciais de usuários (login e senha); c) Ataques cibernéticos à rede interna do Tribunal e; d) Vazamento de informações e dados sigilosos.

MANIFESTAÇÃO DO CLIENTE: A STI manifestou de acordo, sem considerações ou ressalvas (ID 1261284). A SAF, através da CRM (ID 1264236), disse que será implementado mecanismos de controle que permita o monitoramento de terceirizados ativos e inativos.

CONCLUSÃO DA EQUIPE DE AUDITORIA: Achado mantido.

►RECOMENDAÇÕES:

a) Para a **STI**:

1. Excluir do AD as contas ativas de usuários que não possuem mais vínculo com o TRE/MS, identificadas pela AUDIN;

2. Elaborar minuta para atualização do normativo editado em 2019 (Res. TRE/MS n. 663), ampliando as normas sobre contas de usuários, de forma a separar a gestão do sistema de autenticação da gestão de aplicações, bem como disciplinar o procedimento específico de revisão, suspensão e cancelamento de contas de usuários;

3. Inserir, na minuta mencionada no item anterior, capítulo próprio com as regras de SI a serem observadas quanto aos provedores de serviços internos e externos, tendo por referência normas internacionais de controle como, por exemplo, CIS *Controls* v.8 e o ITIL v.4;

4. Estabelecer uma regra para exclusão ou desabilitação de contas com alongado tempo de inatividade (CIS V.8 MS n. 5.3);

5. Instituir, na unidade competente da STI (SGI), rotina para a efetiva realização de revisões periódicas nas contas de usuários do AD, preferencialmente de forma automatizada;

6. Obter das unidades interessadas maior adesão e participação no cumprimento do normativo, através de reuniões de alinhamento de conhecimento ou eventos similares de interação, para maior efetividade das normas de registro, alteração e cancelamento de usuários e acesso às aplicações;

7. Ajustar formalmente (ex. e-mail, termo de compromisso ou doc. similar) com a empresa responsável pelos serviços de suporte ao usuário (Central de Serviços) que comunique imediatamente ao fiscal do contrato o desligamento de colaboradores;

8. Promover ações de esclarecimento quanto a importância da gestão adequada das credenciais de usuários (login e senha), como medida de combate ao acesso não autorizado a ativos e dados do TRE/MS.

b) Para a **SAF**:

1. Ajustar formalmente (ex. e-mail, termo de compromisso ou doc. similar) com a empresa responsável pelos serviços terceirizados [atendente (protocolo e biblioteca) e secretárias] que comunique imediatamente ao fiscal do contrato a movimentação ou desligamento de colaboradores;

2. Informar imediatamente a STI a movimentação ou desligamento de colaboradores mencionados no item anterior, conforme determina o normativo interno de regência (Resolução nº 663/2019, art. 16).

c) Para a **SGP**:

Informar imediatamente a STI a movimentação ou desligamento de servidores (efetivos ou requisitados) e estagiários, conforme determina o normativo interno de regência (Resolução nº 663/2019, art. 16).

A4	AUSÊNCIA DE CLASSIFICAÇÃO DOS PROVEDORES DE SERVIÇO

SITUAÇÃO ENCONTRADA: Não há classificação dos provedores de serviço no TRE/MS, conforme informação da STI.

EVIDÊNCIAS: a) RDIM (ID 1246156) – SEI 0005159-69.2022.6.12.8000 e; b) Informação (ID 1217630) – SEI 0003545-29.2022.6.12.8000.

CRITÉRIOS: a) Controles 15.2 e 15.3 do CIS *Controls* Versão 8; b) Resolução TSE nº 23.644/2021, art. 9, "a" e "b"; c) Portaria CNJ 162/21, item 10.1 c/c item 34 - Da Detecção, letra "j".

POSSÍVEIS CAUSAS: a) Ausência ou falha na definição de uma política de gestão de segurança da informação; b) Percepção de que a política de gestão de segurança da informação é mera formalidade burocrática; c) Desconhecimento e/ou inobservância dos normativos em SI e; d) Insuficiência de capacitação em SI.

POSSÍVEIS CONSEQUÊNCIAS: a) Desconformidade com normativos em Segurança da Informação e; b) Monitoramento deficiente dos provedores de serviço.

MANIFESTAÇÃO DO CLIENTE: Manifestou de acordo, sem considerações ou ressalvas.

CONCLUSÃO DA EQUIPE DE AUDITORIA: Achado mantido.

►**RECOMENDAÇÃO (para STI):** Classificar os provedores de serviço em uso neste Regional, conforme estipulado na norma de controle.

A5	AUSÊNCIA DE POLÍTICA DE GESTÃO DE PROVEDORES DE SERVIÇOS

SITUAÇÃO ENCONTRADA: Em resposta ao RDIM, a STI/CITIS reportou que não há Política de Gestão de Provedores de Serviços no âmbito do TRE/MS.

EVIDÊNCIAS: a) RDIM (ID 1246156) – SEI 0005159-69.2022.6.12.8000 e; b) Informação (ID 1217630) – SEI 0003545-29.2022.6.12.8000.

CRITÉRIOS: a) Controle 15.2 do CIS *Controls* Versão 8; b) Resolução CNJ nº 396/2021, art. 19, I e II c/c art. 28 e; c) Portaria CNJ nº 162/2021, item 2.5.

POSSÍVEIS CAUSAS: a) Desconhecimento e/ou inobservância dos normativos em Segurança da Informação; b) Ausência ou falha na definição de uma política de gestão de segurança da informação; c) Percepção de que a política de gestão de segurança da informação é mera formalidade burocrática e; d) Insuficiência de capacitação em SI.

POSSÍVEIS CONSEQUÊNCIAS: a) Desconformidade com normativos em Segurança da Informação e; b) Monitoramento deficiente dos provedores de serviço.

MANIFESTAÇÃO DO CLIENTE: Manifestou de acordo, sem considerações ou ressalvas.

CONCLUSÃO DA EQUIPE DE AUDITORIA: Achado mantido.

►**RECOMENDAÇÃO (para STI):** Implementar Política de Gestão de Provedores de Serviço no âmbito do TRE/MS.

A6	AUSÊNCIA DE INVENTÁRIO DE PROVEDORES DE SERVIÇO DEVIDAMENTE FORMALIZADO

SITUAÇÃO ENCONTRADA: Em resposta ao RDIM, o cliente da auditoria reportou que não há inventário dos provedores de serviços no âmbito do TRE/MS.

EVIDÊNCIAS: a) RDIM (ID 1246156) – SEI 0005159-69.2022.6.12.8000 e; b) Informação (ID 1217630) – SEI 0003545-29.2022.6.12.8000.

CRITÉRIOS: a) Controle 15.1 do CIS *Controls* Versão 8; b) b) Resolução TSE nº 23.644/2021, art. 9º, II, "b".

POSSÍVEIS CAUSAS: a) Desconhecimento e/ou inobservância dos normativos em Segurança da Informação e; b) Ausência ou falha na definição de uma política de gestão de segurança da informação.

POSSÍVEIS CONSEQUÊNCIAS: a) Desconformidade com normativos em Segurança da Informação e; b) Monitoramento deficiente dos provedores de serviço.

MANIFESTAÇÃO DO CLIENTE: Manifestou de acordo, sem considerações ou ressalvas.

CONCLUSÃO DA EQUIPE DE AUDITORIA: Achado mantido.

►**RECOMENDAÇÃO (para STI):** Realizar a formalização de inventário dos provedores de serviço.

A7	APLICAÇÃO NÃO EFETIVA DOS NORMATIVOS DE SI

SITUAÇÃO ENCONTRADA: a) Considerando a Resolução TSE n.º 23.501/2016 (revogada pela Resolução nº 23.644/2021), que instituiu a Política de Segurança da Informação no âmbito da Justiça Eleitoral, o Tribunal instituiu a Comissão de Segurança da Informação e designou Gestores de Segurança da Informação; bem como instituiu o Sistema de Gestão de Segurança da Informação (SGSI) e criou uma Política de Gestão de Riscos de Segurança da Informação, além de normatizar o processo de elaboração, monitoramento e revisão da Política de Segurança da Informação – PSI do TRE/MS, contudo, a STI informou que tais normativos não são usados de maneira sistemática nas contratações de TIC; b) Percebe-se que há uma política de segurança da informação vigente, contudo, não é fomentada a cultura de planejamento/execução de contratações com enfoque em SI, com ações que visam avançar no processo de adequação às normas de SI, minimizando os riscos e; c) Nas contratações verificadas não há menção de normativos relacionados à SI.

EVIDÊNCIAS: a) Informação da STI por meio de resposta do Questionário RDIM (ID 1248060) (questão 7) nos autos SEI 0005308-65.2022.6.12.8000; b) Seguintes normas do TRE/MS: Portaria Presidência nº 170/2018 TRE/PRE/DG/GABDG, institui a Comissão de Segurança da Informação, Portaria Presidência nº 178/2018 TRE/PRE/DG/GABDG, designa os servidores para serem Gestor de Segurança da Informação no TRE/MS, Portaria Presidência nº 195/2019 TRE/PRE/DG/GABDG, institui o Processo do Sistema de Gestão de Segurança da Informação (SGSI), no âmbito do TRE/MS, Portaria Presidência nº 259/2019 TRE/PRE/ASJES, dispõe sobre a Política de Gestão de Riscos de Segurança da Informação (alterada pela Portaria Presidência nº 262/2019 TRE/PRE/DG/AEDG), Portaria Presidência nº 262/2019 TRE/PRE/DG/AEDG, institui os processos de elaboração, monitoramento e revisão da Política de Segurança da Informação – PSI do TRE/MS; c) 0007090-78.2020.6.12.8000 (Rack Cofre): DOD (ID 0900104) e Termo de Referência (ID 0956288) mencionam apenas que a contratação é para fins de atender o artigo 24 da Resolução CNJ nº 211/2015, visando a segurança; d) 0012417-72.2018.6.12.8000 (*Outsourcing* de impressão); e) 0004285-55.2020.6.12.8000 (STE 2020): Termo de Referência (ID 1006399) e Contrato nº 05/2021 só menciona o Código de Ética do TRE/MS; f) 0004191-73.2021.6.12.8000 (Solução de *hardware* e *software* para VPN): DOD (ID 1063545) indica que a própria contratação visa a segurança da informação, já o Termo de Referência (ID 1107632) e o Contrato nº 20/2021 (ID 1120675) só mencionam o Código de Ética do TRE/MS; g) 0007345-36.2020.6.12.8000 (Ferramenta de análise de *logs* (SIEM): DOD (ID 0906844) indica que a própria contratação visa a segurança da informação, já o Termo de Referência (ID 1108541) e o Contrato nº 24/2021 (ID 1130643) só mencionam o Código de Ética do TRE/MS; h) 0003392-69.2017.6.12.8000 e 0002819-55.2022.6.12.8000 (Central de Serviço de TI): Termo de Referência (ID 0463519) - prevê Termo de Confidencialidade de Informações e Contrato nº 53/2018 (ID 0502271); i) 0002904-75.2021.6.12.8000 (Solução para gestão do parque de UE integrada aos sistemas ASI e LOGUSWEB) e 0007145-92.2021.6.12.8000 (pagamento): PB (ID 1091912) e Contrato nº 22/2021 (ID 1129488) só mencionam o Código de Ética do TRE/MS.

CRITÉRIOS: a) Controle 15.2 do CIS *Controls* Versão 8; b) Lei nº 13.709/2018 (LGPD); c) Resolução CNJ nº 396/2021; d) Portaria CNJ nº 162/2021; e) Resoluções do TSE nº 23.644/2021 e nº 23.650/2021; f) Resoluções do TRE/MS nº 663/2019, nº 604/2021 (arts. 18 e ss), nº 749/2021 e nº 740/2021; g) Portaria Presidência nº 259/2019 TRE/PRE/ASJES, alterada pela Portaria Presidência nº 262/2019.

POSSÍVEIS CAUSAS: a) Ausência ou falha na definição de uma política de gestão de segurança da informação; b) Percepção de que a política de gestão de segurança da informação é mera formalidade burocrática e; c) Licitações realizadas sem modelos padronizados com os critérios de segurança da informação.

POSSÍVEIS CONSEQUÊNCIAS: a) Contratação que não atenda às necessidades do Tribunal em segurança da informação e; b) Danos à imagem da organização.

MANIFESTAÇÃO DO CLIENTE: A STI sugeriu que a recomendação para realização de ações para fomentar a cultura de segurança da informação no âmbito do TRE/MS fosse dirigida à Comissão de Segurança da Informação (CSI), pois trata-se de competência deste colegiado, conforme previsto expressamente na Resolução TSE n. 23.644/2021, art. 11, III. Também sugeriu a alteração do termo "proteção de dados" para "segurança da informação", pois a auditoria trata de segurança da informação (ID 1261284). A SAF, através da CRM (ID 1264236), informou que, no âmbito interno daquela Secretaria, haverá o alinhamento entre as unidades internas para dar efetivo cumprimento aos normativos de SI.

CONCLUSÃO DA EQUIPE DE AUDITORIA: A sugestão do cliente de auditoria merece acolhida, para adequação à regra de competência fixada na Resolução TSE n. 23.644/2021, art. 11, III. A segunda alteração sugerida foi igualmente realizada, com a substituição das expressões.

►**RECOMENDAÇÕES:**

a) Para a **Comissão de Segurança da Informação (CSI)**:

1. Propor a atualização/adequação da Portaria Presidência nº 170/2018 TRE/PRE/DG/GABDG, que institui a Comissão de Segurança da Informação, aos termos da Resolução TSE nº 23.644/2021(PSI), tendo em vista a revogação da Resolução TSE n.º 23.501/2016 (antigo PSI) que embasava a referida Portaria;

2. Fomentar a cultura de segurança da informação, com ações que visam avançar no processo de adequação às normas de SI, mormente as Resoluções CNJ 396/2021 e Resolução TSE nº 23.644/2021, visando definir e implementar estratégia para atuar preventivamente nas frentes de segurança da informação e privacidade de dados, minimizando os riscos em todas as fases da contratação de TIC, em consonância com o Eixo Estruturante E2: Políticas e Normatização e Eixo Estruturante E5: Sensibilização e Conscientização da Estratégia Nacional de Cibersegurança do TSE e TRE's – 2021 a 2024.

b) Para **STI** e **SAF**:

1. Sem prejuízo de outras disposições normativas, dar efetividade aos normativos regulatórios de SI, naquilo que for aplicável a este Regional;

2. Incluir nas licitações/contratações a obrigatoriedade de observância dos normativos relativos à SI.

A8	AUSÊNCIA DE ADOÇÃO DE MÚLTIPLO FATOR DE AUTENTICAÇÃO (MFA) NOS SISTEMAS CRÍTICOS

SITUAÇÃO ENCONTRADA: a) Não há no âmbito do TRE a adoção do MFA para os sistemas críticos e externamente expostos; b) No RDIM, a CODESC reportou que não há classificação dos sistemas considerados críticos, entretanto, eles são diferenciados em operacional, tático e estratégico e; c) Durante a fase de levantamento de dados para entendimento do objeto, foi coletada a informação, em entrevista com os gestores, que o TRE/MS pretende adotar o MFA para o próximo exercício, sendo que o estudos preliminares para a contratação já estariam sendo feitos.

EVIDÊNCIAS: a) RDIM (ID 1246156) – SEI nº 0005159-69.2022.6.12.8000; b) Entrevistas com gestores e; c) Informação (ID 1217630).

CRITÉRIOS: a) Controles 6.3, 6.4 e 6.5 do CIS *Controls* Versão 8; b) Resolução TRE/MS nº 663/19, art. 2º, VI.

POSSÍVEIS CAUSAS: a) Auto custo para adequação dos sistemas atuais; b) Restrição orçamentária; c) Inexistência de classificação e definição dos sistemas críticos; d) Insuficiência de capacitação em SI.

POSSÍVEIS CONSEQUÊNCIAS: a) Vulnerabilidade dos ativos de TIC; b) Exposição e elevação do risco de invasão cibernética; c) Danos à imagem da organização e; d) Vazamento/furto de informações sigilosas.

MANIFESTAÇÃO DO CLIENTE: A STI manifestou de acordo e esclareceu que será implantado o método de Multifator de Autenticação (MFA), assim que for liberada a adesão pelo TRE/BA (SEI 0003706-39.2022.6.12.8000 e 0003679-56.2022.6.12.8000).

CONCLUSÃO DA EQUIPE DE AUDITORIA:

Foi confirmado que o TRE/MS já abriu procedimento para realizar a contratação de uma solução de autenticação por múltiplos fatores para 700 usuários por 60 meses (SEI 0003706-39.2022.6.12.8000), mediante sistema de registro de preços, através de adesão prévia na licitação a ser realizada pelo TRE/BA, perante o qual já houve a manifestação de interesse deste Regional em figurar como órgão partícipe. A COPEG promoveu a reserva orçamentária para concretização desta despesa (ID 1252453). O procedimento segue seu curso regular.

Achado mantido, pois a medida ainda não foi concretizada, com o registro de que a Administração já iniciou as providências necessárias para implantação do MFA no âmbito deste Regional. A finalização da contratação e o efetivo uso da ferramenta deverá constar do Plano de Ação a ser elaborado pelo cliente de auditoria e serão oportunamente objeto de avaliação em processo de monitoramento.

►**RECOMENDAÇÃO (para STI):** Implementar o MFA nos acessos remotos à rede, bem como nos sistemas críticos, após a necessária classificação e respeitada a disponibilidade orçamentária.

A9	DEFICIÊNCIA NA GESTÃO DE SENHAS E AUTENTICAÇÃO DE USUÁRIO

SITUAÇÃO ENCONTRADA: a) Apurou-se que nos sistemas internos desenvolvidos pelo TRE/MS, bem como nos sistemas de terceiros implantados nesta Corte, é possível a utilização de senhas fracas, de senhas com sequenciais numéricos ou letras, senhas de fácil adivinhação, não utilização de caracteres especiais, bem como não há adoção da prática de troca de senha periódica pelo usuário; b) No RDIM, a CODESC informou que não há controle sobre essa atividade.

EVIDÊNCIAS: a) RDIM (ID 1246156) - SEI nº 0005159-69.2022.6.12.8000; b) Entrevistas com gestores e; c) Informação (ID 1217630).

CRITÉRIOS: a) Controles 6.6 e 6.7 do CIS *Controls* Versão 8; b) Resolução TRE/MS nº 663/19, art. 17 e ss.; c) Resolução CNJ nº 396/2021, art. 28, I; d) Resolução TSE nº 23.644/2021, art. 9º, II, "b"; e) Portaria 162/2021 CNJ, item 7 c/c item 2.8 - *checklist*, c/c item 2.5 do capítulo - Requisitos para Adequação dos Ativos de Tecnologia da Informação.

POSSÍVEIS CAUSAS: a) Ausência de parametrização dos requisitos para definição de senhas; b) Inexistência da obrigatoriedade de trocas periódicas de senhas, após certo tempo de uso; c) Indefinição e falta de classificação dos sistemas críticos; d) Ausência de obrigatoriedade do uso de caracteres especiais.

POSSÍVEIS CONSEQUÊNCIAS: a) Desconformidade com normativos em SI; b) Vulnerabilidade dos ativos de TIC; c) Exposição e elevação do risco de invasão cibernética.

MANIFESTAÇÃO DO CLIENTE: A STI não discordou do achado, todavia, sugeriu que a primeira proposta de encaminhamento seja desconsiderada, justificando que existem estudos que comprovam que a obrigatoriedade de senhas "fortes" leva à fragilidade na segurança, uma vez que é necessária a anotação da senha para ser lembrada. Concomitantemente, sugeriu como proposta substitutiva a implantação do Múltiplo Fator de Autenticação (MFA). Não houve discordância quanto à segunda recomendação.

CONCLUSÃO DA EQUIPE DE AUDITORIA:

Inicialmente, convém registrar que a implantação do MFA já constou da recomendação do Achado 8, inclusive com o esclarecimento da STI que a contratação já está em andamento, o que foi confirmado (SEI 0003706-39.2022.6.12.8000 e SEI 0003679-56.2022.6.12.8000).

A autenticação por múltiplos fatores certamente vai aumentar o nível de segurança dos usuários ao acessar equipamentos e aplicações da Justiça Eleitoral, criando uma forte barreira de proteção aos ativos de informação do TRE/MS. Com o uso do MFA, as senhas deixarão de ser o principal fator de segurança cibernética, entretanto, sua importância não será esvaziada e não deixarão de ser utilizadas.

As novas ferramentas tecnológicas que serão contratadas (MFA e Single Sign-On), em conjunto com a implantação do Domínio Único em fase final de implantação, promoverão um salto de qualidade nos controles internos de cibersegurança deste Regional, ampliando, em larga escala e eficiência, as camadas de proteção aos sistemas e ativos de informação, devidamente alinhados com a Estratégia Nacional de Cibersegurança da Justiça Eleitoral 2021-2024, Eixo 3: Ferramentas Automatizadas. Também promovem aderência com as medidas de segurança do controle 6.3 do CIS *Controls* V.8.

Fato é que as referidas inovações tecnológicas pretendidas, e outras que futuramente virão, criarão novas camadas de segurança, além das senhas dos usuários, ampliando os escudos protetores de cibersegurança. Pelo que foi possível apurar, nenhuma delas substituirá as senhas, que continuarão em uso. Haverá apenas um somatório de forças contra ataques cibernéticos.

Diante deste cenário, esta unidade de auditoria mantém a primeira recomendação para o achado apontado, no sentido de que se dê efetividade à política de senhas prevista expressamente nos arts. 18 a 22 da Resolução TRE/MS n. 663/2019. Caso as regras de senhas não sejam atualmente eficazes ou apresentem desconformidades com a realidade tecnológica atual, suas disposições deverão ser aperfeiçoadas. Do mesmo modo, fica mantida a segunda recomendação.

►**RECOMENDAÇÃO (para STI):**

1. Dar cumprimento à norma regulamentadora da gestão de acesso deste Regional (Resolução nº 663/2019), principalmente quanto aos requisitos da política de senhas prevista expressamente nos arts. 18 a 22 da Resolução TRE/MS n. 663/2019;

2. Promover o aperfeiçoamento e a atualização da Resolução nº 663/2019, com adoção das diretrizes trazida pela Resolução TSE 23.644/2021 (PSI).

IX – BOAS PRÁTICAS DETECTADAS NOS EXAMES E SUGESTÕES DE MELHORIA EM SI

Os testes aplicados permitiram a identificação de achados positivos (boas práticas) relacionadas à segurança da informação, evidenciados por atividades e controles internos aplicados, com eficiência e eficácia, no âmbito do TRE/MS. Da mesma forma, foram detectados pontos com margem para aperfeiçoamento do processo de trabalho, ou seja, com a oportunidade de avanço através de práticas que poderão dar suporte e apoiar a gestão na concretização de medidas efetivas de cibersegurança, aqui classificadas como sugestões de melhoria. São eles:

1 - Controle de Acesso Físico

Boa Prática: Há cautelas adequadas e controles efetivos sobre o acesso físico de colaboradores das contratadas. Nas visitas técnicas presenciais, ocorre uma ação conjunta e ordenada da CITIS/Núcleo de Segurança Institucional/recepção/vigilantes).

►**Sugestão de melhoria:** Promover a formalização do procedimento, em cumprimento ao determinado no art. 6º, parágrafo único, da Resolução TRE/MS n. 663/2019. O procedimento é bem executado na prática, todavia, carece de formalização (SAF- NSI).

2 - Acesso ao SEI e ao PJE

Boa Prática: Adoção de um formulário para solicitação de acesso ao SEI.

►**Sugestão de melhoria:** Padronizar o processo de solicitação de acesso ao PJE, através da adoção de formulário específico, como ocorre com o SEI (ação conjunta CRIP e STI).

3 - Ciência aos colaboradores

►**Sugestão de melhoria:** Fornecimento de uma cartilha ou documento equivalente destacando as regras de SI a serem observadas no âmbito do TRE/MS. Documento de formato amigável (ilustrado se possível), sucinto (uma folha), com conteúdo de fácil compreensão e linguagem acessível.

4 - Fomento à SI no início dos contratos

►**Sugestão de melhoria:** Realizar reunião de inicialização nas novas contratações, com enfoque em segurança da informação (ex. exigir termo de confidencialidade, informar sobre os normativos vigentes, notificação e resposta de incidente de segurança, etc.), e registrar o resultado em ata (SEI).

5 - SI nos contratos a serem formalizados

►**Sugestão de melhoria:** Implementar nas contratações a solicitação de Termo de Compromisso, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes com ênfase em segurança da informação, firmados pelos prestadores de serviços, bem como respectivo Termo de Ciência da referida declaração, firmados pelos empregados da contratada diretamente envolvidos na contratação.

6 - SI nos contratos em andamento

►**Sugestão de melhoria:** Implementar nas contratações em andamento (contratos prorrogados) a solicitação de Termo de Compromisso, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes com ênfase em segurança da informação, firmados pelos prestadores de serviços, bem como respectivo Termo de Ciência da referida declaração, firmados pelos empregados da contratada diretamente envolvidos na contratação.

7 - Monitoramento de SI na execução contratual

►**Sugestão de melhoria**: Estudar a viabilidade para fins de implementação de solução de TI ou outro procedimento para suportar o processo de monitoramento quanto à segurança da informação na execução contratual, especialmente no trabalho remoto.

X – CONCLUSÃO

A partir do Programa de Auditoria no processo de gestão de segurança da informação, definido pelo GTA/SEAUT-TSE, foram aplicados 10 (dez) testes, sendo 8 (oito) obrigatórios para todos os Tribunais Eleitorais e mais 2 (dois) testes adicionais de grande relevância para o resultado da auditoria segundo entendimento da AUDIN.

Nas análises foram aplicados, como critérios de auditoria, os controles 5, 6 e 15 do CIS *Controls* v.8 e normativos do CNJ, TSE e TRE/MS afetos especificamente à segurança cibernética no gerenciamento de provedores de serviço e seus respectivos contratos, bem como no processo de gestão de identidade e de controle de acesso aos ativos de informação do Regional sul-mato-grossense.

Como resultado da comparação entre a situação encontrada e os critérios estabelecidos foram identificados 9 (nove) achados, devidamente comprovados por evidências e documentados em papéis de trabalho.

Com o propósito de agregar valor e melhorar os processos organizacionais de segurança cibernética, para cada achado foram feitas sugestões de recomendações com a finalidade de eliminar as causas dos achados de auditora, mitigar suas consequências ou

até mesmo incorporar uma boa prática.

Referidos achados foram informados aos clientes de auditoria e oportunizada a prévia manifestação para impugnação, justificativa e esclarecimento. Todas as manifestações apresentadas foram consideradas e devidamente avaliadas para fins de manutenção, desconstituição ou alteração dos achados.

Identificou-se que o Tribunal executa de forma satisfatória diversas ações de segurança cibernética e, em grande parte, aplica controles adequados para proteção de seus ativos de informação. Ademais, constatou-se o comprometimento no cumprimento da Estratégia Nacional de Cibersegurança da JE (2021 a 2024) e na observância dos prazos nela estabelecidos.

Não obstante existir outras demandas igualmente relevantes, há foco em SI e a execução, concomitante, de várias medidas operacionais e contratuais voltadas à criação de escudos de proteção contra ataques cibernéticos.

Nesse cenário, mesmo sendo inegável a existência de expressivos avanços em SI já em execução ou em vias de implantação, há ainda grande margem para aperfeiçoamento das ações de cibersegurança no TRE/MS. Os achados indicados neste relatório sinalizam oportunidades de melhoria, devidamente alinhadas com a EN de Cibersegurança da JE (2021/2024), e irão agregar valor no processo de gestão de segurança da informação.

Entre os benefícios esperados desta auditoria, com o cumprimento das sugestões de recomendações apontadas, pode-se mencionar:

a) Aperfeiçoamento da Governança (Adm./TIC), com o aprimoramento dos controles e a mitigação dos riscos de ataques cibernéticos;

b) Corpo técnico qualificado nas atividades de segurança da informação;

c) Ganho de qualidade e eficiência nos processos internos que envolvam segurança cibernética (Ex. licitações/contratos);

d) Cumprimento da EN de Cibersegurança da JE (2021/2024);

e) Alinhamento com as boas práticas internacionais de combate a ataques cibernéticos.

XI - QUADRO-RESUMO DAS PROPOSTAS DE RECOMENDAÇÕES

As propostas de recomendações expostas anteriormente estão sintetizadas no quadro-resumo abaixo:

ACHADO	PROPOSTAS DE RECOMENDAÇÕES
A1	Para a **STI** e **SGP**: 1. Proporcionar que todos os agentes públicos e colaboradores do TRE/MS sejam conscientizados, capacitados e treinados em segurança da informação, de forma a promover o alinhamento do conhecimento em SI e a redução dos riscos na área de segurança cibernética; 2. Sem prejuízo das atividades eleitorais do pleito que se avizinha e de outras demandas igualmente relevantes, priorizar as ações de implantação da plataforma integrada de treinamento *on-line*, especializada na oferta de conteúdos de capacitação e conscientização em Segurança da Informação, cuja contratação já está em andamento (SEI 0004181-92.2022.6.12.8000). Os recursos humanos do TRE/MS devem estar organizados, sensibilizados e dedicados às questões referentes à cibersegurança, exigências contidas no Eixo Estruturante 1: Pessoas e Unidades Organizacionais e no Eixo Estruturante 5: Sensibilização e Conscientização da Estratégia Nacional de Cibersegurança da Justiça Eleitoral 2021 a 2024.
A2	Para **STI** e **SAF**: Implementar modelos de ETP/TR/PB/minuta contratual com elementos mínimos acerca da SI, de forma a padronizar os documentos de planejamento da contratação de TIC (ex. termo de confidencialidade, previsão de glosas ou agravamento de sanções nos casos de violação de dados, notificação e resposta de incidente de segurança, medidas de segurança e privacidade dos dados coletados e armazenados pela contratada, etc.).
A3	a) Para a **STI**: 1. Excluir do AD as contas ativas de usuários que não possuem mais vínculo com o TRE/MS, identificadas pela AUDIN; 2. Elaborar minuta para atualização do normativo editado em 2019 (Res. TRE/MS n. 663), ampliando as normas sobre contas de usuários, de forma a separar a gestão do sistema de autenticação da gestão de aplicações, bem como disciplinar o procedimento específico de revisão, suspensão e cancelamento de contas de usuários; 3. Inserir, na minuta mencionada no item anterior, capítulo próprio com as regras de SI a serem observadas quanto aos provedores de serviços internos e externos, tendo por referência normas internacionais de controle como, por exemplo, CIS Controls v.8 e o ITIL v.4; 4. Estabelecer uma regra para exclusão ou desabilitação de contas com alongado tempo de inatividade (CIS V.8 MS n. 5.3; 5. Instituir, na unidade competente da STI (SGI), rotina para a efetiva realização de revisões periódicas nas contas de usuários do AD, preferencialmente de forma automatizada; 6. Obter das unidades interessadas maior adesão e participação no cumprimento do normativo, através de reuniões de alinhamento de conhecimento ou eventos similares de interação, para maior efetividade das normas de registro, alteração e cancelamento de usuários e acesso às aplicações; 7. Ajustar formalmente (ex. e-mail, termo de compromisso ou doc. similar) com a empresa responsável pelos serviços de suporte ao usuário (Central de Serviços) que comunique imediatamente ao fiscal do contrato o desligamento de colaboradores e; 8. Promover ações de esclarecimento quanto à importância da gestão adequada das credenciais de usuários (login e senha), como medida de combate ao acesso não autorizado a ativos e dados do TRE/MS. b) Para a **SAF**:

	1. Ajustar formalmente (ex. e-mail, termo de compromisso ou doc. similar) com a empresa responsável pelos serviços terceirizados [atendente (protocolo e biblioteca) e secretárias] que comunique imediatamente ao fiscal do contrato a movimentação ou desligamento de colaboradores; 2. Informar imediatamente a STI a movimentação ou desligamento de colaboradores mencionados no item anterior, conforme determina o normativo interno de regência (Resolução nº 663/2019, art. 16). c) Para a **SGP**: Informar imediatamente a STI a movimentação ou desligamento de servidores (efetivos ou requisitados) e estagiários, conforme determina o normativo interno de regência (Resolução nº 663/2019, art. 16).
A4	Para a **STI**: Classificar os provedores de serviço em uso neste Regional, conforme estipulado na norma de controle (CIS *Controls* v.8, MS 15.3).
A5	Para **STI**: Implementar Política de Gestão de Provedores de Serviço no âmbito do TRE/MS.
A6	Para **STI**: Realizar a formalização de inventário dos provedores de serviço.
A7	a) Para a **Comissão de Segurança da Informação (CSI)**: 1. Propor a atualização/adequação da Portaria Presidência nº 170/2018 TRE/PRE/DG/GABDG, que institui a Comissão de Segurança da Informação, aos termos da Resolução TSE nº 23.644/2021(PSI), tendo em vista a revogação da Resolução TSE n.º 23.501/2016 (antigo PSI) que embasava a referida Portaria; 2. Fomentar a cultura de segurança da informação, com ações que visam avançar no processo de adequação às normas de SI, mormente as Resoluções CNJ 396/2021 e Resolução TSE nº 23.644/2021, visando definir e implementar estratégia para atuar preventivamente nas frentes de segurança da informação e privacidade de dados, minimizando os riscos em todas as fases da contratação de TIC, em consonância com o Eixo Estruturante E2: Políticas e Normatização e Eixo Estruturante E5: Sensibilização e Conscientização da Estratégia Nacional de Cibersegurança do TSE e TRE's – 2021 a 2024. b) Para **STI** e **SAF**: 1. Sem prejuízo de outras disposições normativas, dar efetividade aos normativos regulatórios de SI, naquilo que for aplicável a este Regional; 2. Incluir nas licitações/contratações a obrigatoriedade de observância dos normativos relativos à SI.
A8	Para **STI**: Implementar o MFA nos acessos remotos à rede, bem como nos sistemas críticos, após a necessária classificação e respeitada a disponibilidade orçamentária.
A9	Para a **STI**: 1. Dar cumprimento à norma regulamentadora da gestão de acesso deste Regional (Resolução nº 663/2019), principalmente quanto aos requisitos da política de senhas prevista expressamente nos arts. 18 a 22 da Resolução TRE/MS n. 663/2019; 2. Promover o aperfeiçoamento e a atualização da Resolução nº 663/2019, com adoção das diretrizes trazida pela Resolução TSE 23.644/2021 (PSI).

XI - ENCAMINHAMENTOS

Submete-se o presente relatório final à Diretoria-Geral, para **ciência** dos seus termos e das propostas de recomendações acima.

Simultaneamente, submete-se também este relatório à consideração do Excelentíssimo Des. Presidente do TRE/MS para ciência de seus termos, apreciação e para **fixação de prazo** para que os clientes de auditoria apresentem os respectivos planos de ação para adoção das medidas necessárias à implantação das recomendações acima, com os respectivos prazos para atendimento. Solicita-se, em seguida, o envio do processo às unidades GABSTI, GABSAF e GABSGP, para notificação dos gestores acerca da emissão do relatório final e do prazo fixado por Vossa Excelência.

Numa fase seguinte, esta unidade de Auditoria Interna irá monitorar o cumprimento das medidas, bem como sua efetividade, com o objetivo de contribuir para a melhoria do processo de gestão de segurança da informação no âmbito do TRE/MS.

Campo Grande/MS, 19 de agosto de 2022.

Alessandra Falcão Gutierres de Souza
Supervisora - Dirigente AUDIN

Nivaldo Azevedo dos Santos
Líder Equipe - SAPTIC

Flávio Alexandre Martins Nichikuma
Auditor - SAPTIC

Manuela Baptista Velasques Shoji
Auditora - SAPTIC

1 Auditoria Baseada em Riscos (ABR) – IIA/TCU. Risco – é representado pela possibilidade de que um evento ocorrerá e afetará negativamente a realização dos objetivos (COSO ERM).

Documento assinado eletronicamente por **ALESSANDRA FALCÃO GUTIERRES DE SOUZA**, **Coordenador(a)**, em 19/08/2022, às 11:49, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **FLÁVIO ALEXANDRE MARTINS NICHIKUMA**, **Analista Judiciário**, em 19/08/2022, às 12:55, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **NIVALDO AZEVEDO DOS SANTOS**, **Analista Judiciário**, em 19/08/2022, às 13:04, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **MANUELA BAPTISTA VELASQUEZ SHOJI**, **Técnico Judiciário**, em 19/08/2022, às 14:24, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.app.tre-ms.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1267006** e o código CRC **E4046F2C**.

0003545-29.2022.6.12.8000 1267006v120