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

SUMÁRIO EXECUTIVO

AUDITORIA INTEGRADA NO PROCESSO DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

DESTINATÁRIOS: Presidência e Diretoria-Geral.

CLIENTE DA AUDITORIA: Secretaria de Tecnologia da Informação (STI).

CONCLUSÃO DOS TRABALHOS: a partir de todos os dados coletados, informações apresentadas, análises realizadas e considerando as respostas oferecidas pelo cliente da auditoria (ID 1261284 e 1264236), 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 Justiça Eleitoral (2021 a 2024) e na observância dos prazos nela estabelecidos. Não obstante existir outras demandas igualmente relevantes, há foco em segurança da informação 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 segurança da informação já em execução ou em vias de implantação, há ainda grande margem para aperfeiçoamento das ações de cibersegurança no TRE/MS. Desse modo, há situações, que apresentaram desconformidades e foram enquadradas como achados de auditoria e sinalizam oportunidades de melhoria, devidamente alinhadas com a referida Estratégia Nacional de Cibersegurança. As recomendações à STI e demais Secretarias impactadas (SAF e SGP) estão sintetizadas no quadro-resumo abaixo.

RECOMENDAÇÕES DO RELATÓRIO FINAL (1267006):

ACHADO	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 Segurança da Informação (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 *Active Directory* (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 Múltiplo Fator de Autenticação (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).

O Relatório Final (ID 1267006), Tópico IX, indicou sugestões de melhoria na área de SI que, mesmo não estando vinculadas a achados, podem ser úteis e, assim como as recomendações acima, capazes de contribuir para o aperfeiçoamento dos controles internos e ganho de qualidade no processo de gestão de segurança da informação. Por conseguinte, é imperioso apreciá-las e, caso julgadas convenientes e oportunas (mérito administrativo), colocadas em prática, no todo ou em parte.

Campo Grande/MS, *na data da assinatura eletrônica*.

Alessandra Falcão Gutierres de Souza

Supervisora

Nivaldo Azevedo dos Santos

Líder Equipe

Flávio Alexandre Martins Nichikuma

Auditor

Manuela Baptista Velasquez Shoji

Auditor

Documento assinado eletronicamente por **ALESSANDRA FALCÃO GUTIERRES DE SOUZA**, **Coordenador(a)**, em 23/08/2022, às 18:16, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **FLÁVIO ALEXANDRE MARTINS NICHIKUMA**, **Analista Judiciário**, em 23/08/2022, às 18:39, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **NIVALDO AZEVEDO DOS SANTOS**, **Analista Judiciário**, em 24/08/2022, às 10:21, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **MANUELA BAPTISTA VELASQUEZ SHOJI**, **Técnico Judiciário**, em 24/08/2022, às 12:25, 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 **1269765** e o código CRC **53FCB962**.

0003545-29.2022.6.12.8000 1269765v10