AUDITORIA INTERNA - AI

SEÇÃO DE AUDITORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO E DE GOVERNANÇA - SATIG

RELATÓRIO DE AUDITORIA n. 3/2025

PROCESSO DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

SÃO LUIS – MA, 2025.

PREÂMBULO

PROCESSO: SEI n. 0006899-40.2025.6.27.8000.

ATO ORIGINÁRIO: Plano de Auditoria de Longo Prazo (PALP) 2022-2025, aprovado pela Portaria TRE/MA n. 1.581/2021 (SEI n. 0009517-94.2021.6.27.8000), e Plano Anual de Auditoria (PAA) 2025, aprovado pela Portaria TRE/MA n. 1.870/2024 (SEI n. 0018797-84.2024.6.27.8000).

OBJETIVO: Avaliar a gestão de segurança da informação no âmbito do TRE-MA, de modo a avaliar a existência, adequação e eficácia das políticas, procedimentos e planos de recuperação de dados do tribunal, utilizando como critério principal o *framework CIS Controls* (*The Center for Internet Security*) versão 8.

ATO DE DESIGNAÇÃO: Memorando n. 605/2025 – TRE-MA/PR/AI/SATIG, de 31/07/2025 (id. 2525488, SEI n. 0006899-40.2025.6.27.8000).

PERÍODO ABRANGIDO PELA AUDITORIA: agosto/2025 a novembro/2025.

PERÍODO DE REALIZAÇÃO DA AUDITORIA: a) Planejamento – agosto/2025; b) Execução – setembro a outubro/2025; e c) Relatório – novembro a dezembro/2025.

UNIDADE AUDITADA: Secretaria de Tecnologia da Informação e Comunicação – STIC.

RESUMO

A presente auditoria, realizada no Tribunal Regional Eleitoral do Maranhão, teve como objeto avaliar a gestão de cópias de segurança (*backup*), utilizando como critério o Controle 11 do *framework CIS Controls* versão 8, que se concentra na Recuperação de Dados (*Data Recovery*).

Em síntese, os objetivos desta ação de controle consubstanciaram-se em verificar a eficácia da arquitetura de *backup* e a maturidade dos processos de validação e governança. Registra-se, contudo, que a conclusão dos trabalhos demandou uma extensão do prazo inicialmente planejado, em razão da necessidade de a unidade auditada dispor de tempo adicional para a resposta completa às requisições de informações, sendo este ajuste devidamente justificado pelos desafios técnicos e operacionais momentaneamente enfrentados.

Ao término dos trabalhos, a auditoria confirmou que a arquitetura é tecnicamente robusta, atendendo ao isolamento e criptografia, conforme as exigências de segurança do Pregão Eletrônico n. 29/2021 (Contratação de serviços de backup em nuvem com armazenamento em datacenter no Brasil para proteção de dados do TRE-MA em ambiente externo).

No entanto, a principal inconformidade identificada foi a ausência de um controle de governança maduro, representado pela falta de formalização da frequência de revisão da Política de *Backup* (Portaria DG n. 101/2023) e pela omissão da exigência de Autenticação Multifator (MFA) para o acesso privilegiado ao ambiente de *backup* (CIS 11.3). A não formalização desses requisitos aumenta o risco de obsolescência da política e de acesso indevido à infraestrutura de recuperação.

Os benefícios decorrentes da implementação das medidas corretivas propostas são qualitativos, correspondentes ao aperfeiçoamento da gestão e governança de TIC, garantindo que a documentação formal acompanhe o alto nível de segurança técnica já implementado.

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
AI	Auditoria Interna
CIS	*The Center for Internet Security*
CNJ	Conselho Nacional de Justiça
DG	Diretoria Geral – TRE/MA
ENSEC-PJ	Estratégia Nacional de Segurança Cibernética do Poder Judiciário
ISO	*International Organization for Standardization*
MFA	*Multi-Factor Authentication*
PAA	Plano Anual de Auditoria – TRE/MA
PALP	Plano de Auditoria de Longo Prazo – TRE/MA
PCN	Plano de Continuidade de Negócios
PSI	Política de Segurança da Informação
PT	Papel de Trabalho
RDIM	Requisição de Detalhamento de Informações
SATIG	Seção de Auditoria de Tecnologia da Informação e Comunicação e de Governança – TRE/MA
SEI	Sistema Eletrônico de Informações
SERED	Seção de Gestão de Redes
STIC	Secretaria de Tecnologia da Informação e Comunicação
TIC	Tecnologia da Informação e Comunicação
TRE/MA	Tribunal Regional Eleitoral do Maranhão
TRT	Tribunal Regional do Trabalho
TSE	Tribunal Superior Eleitoral
VM	*Virtual Machine*

SUMÁRIO

I. INTRODUÇÃO

1. A presente auditoria tem como objetivo avaliar a gestão de segurança da informação no âmbito do Tribunal Regional Eleitoral do Maranhão (TRE-MA), com base nos critérios estabelecidos pelo *CIS Controls (The Center for Internet Security)*, versão 8, especificamente o Controle 11 – Recuperação de Dados (*Data Recovery*). Este controle visa desenvolver e manter uma capacidade de recuperação de dados por meio de políticas, planos, procedimentos, funções definidas e da garantia de que as cópias de segurança são seguras e testadas, preparando a organização para restabelecer os serviços rapidamente após um desastre ou ataque.

2. A gestão de cópias de segurança é um processo fundamental para proteger os ativos de informação contra ameaças diversas, garantindo a disponibilidade e a integridade dos dados. Em um cenário cada vez mais digital e conectado, a capacidade de recuperar dados de maneira eficiente e eficaz, especialmente após incidentes como o *ransomware*, torna-se crucial. A ausência de uma gestão robusta de *backup* pode levar a perdas significativas e interrupções de serviço.

3. O Controle 11 do *CIS Controls* versão 8 enfatiza a importância de uma abordagem estruturada para a recuperação. Isso inclui o desenvolvimento de políticas e planos detalhados, a implementação de mecanismos de isolamento para as cópias, e a realização de testes periódicos de restauração (*restore*). Essas práticas não apenas melhoram a prontidão da organização para enfrentar perdas de dados, mas também permitem a validação e o aprimoramento contínuo das políticas e procedimentos de segurança.

4. Dessa forma, a auditoria visa certificar-se da conformidade do TRE-MA com os requisitos do Controle 11, identificando áreas de melhoria e recomendando ações para fortalecer a postura de segurança da informação e a capacidade de resiliência da instituição.

5. Cabe destacar a atuação consonante desta Seção de Auditoria de Tecnologia da Informação e Comunicação e de Governança – SATIG, em cumprimento ao estabelecido no Plano de Auditoria de Longo Prazo (PALP) 2022 a 2025, aprovado pela Portaria TRE/MA n. 1.581/2021 (SEI n. 0009517-94.2021.6.27.8000), e Plano Anual de Auditoria (PAA) 2025, aprovado pela Portaria TRE/MA n. aprovado pela Portaria TRE/MA n. 1.870/2024 (SEI n. 0018797-84.2024.6.27.8000), realizando exames de auditoria no processo de gestão de cópias de segurança.

6. Neste contexto, a presente auditoria apoiou-se no Plano de Trabalho n. 01/2025 (id. 2594963, SEI n. 0006899-40.2025.6.27.8000) estabelecido pela SATIG.

7. Compuseram a equipe de auditoria a servidora Sara Aguiar Gomes (matrícula 3099950) e o servidor Moisés Dantas Linhares (matrícula 30990117).

8. Os possíveis achados encontrados e as respectivas recomendações emitidas por esta unidade foram materializados no Quadro de Achados (id. 2638833, SEI n. 0006899-40.2025.6.27.8000) e encaminhados para a unidade auditada.

9. A unidade auditada se manifestou quanto ao possível achado, e suas respostas foram consideradas e incluídas neste Relatório de Auditoria.

10. Todos os exames realizados se pautaram em procedimentos e técnicas de auditoria aplicáveis à Administração Pública e nenhuma restrição foi imposta quanto ao método ou à extensão dos trabalhos realizados.

II. VISÃO GERAL DO OBJETO AUDITADO

11. O objeto auditado nesta análise é o processo de Gestão de Cópias de Segurança (*Backup*) e Recuperação de Dados do Tribunal Regional Eleitoral do Maranhão (TRE-MA), com foco específico no Controle 11 – Recuperação de Dados (*Data Recovery*), conforme estabelecido pelo *framework CIS Controls (The Center for Internet Security)*, versão 8. Este controle é fundamental para garantir que a organização esteja preparada para restaurar a integridade e a disponibilidade dos ativos de informação após um desastre ou ataque, minimizando os impactos adversos e assegurando a continuidade das operações.

12. Um programa de segurança cibernética deve incluir proteção, detecção, resposta e recuperação. Muitas instituições negligenciam a fase de recuperação, focando apenas na proteção. A gestão de cópias de segurança visa garantir a confiabilidade da restauração de dados críticos. O *CIS Control* 11 oferece passos prioritários para o uso da arquitetura de backup e a validação da integridade dos dados recuperados.

13. A equipe de tecnologia deve garantir que os procedimentos de *backup* e *restore* sejam rigorosamente seguidos e que as cópias de segurança sejam protegidas. O Controle CIS 11 enfatiza a necessidade de políticas formais (como a Portaria DG n. 101/2023) e a proteção lógica (criptografia e controle de acesso privilegiado) para evitar que um atacante comprometa as próprias cópias de recuperação.

14. Através desta auditoria, buscamos identificar áreas de melhoria na governança documental e nos controles de acesso (MFA) e revisão de políticas, recomendando ações que possam aprimorar a capacidade do TRE-MA em recuperar dados de forma eficaz, assegurando uma gestão de segurança da informação sólida e confiável.

15. Esta visão geral oferece um contexto abrangente para a leitura do relatório, destacando o processo de gestão de cópias de segurança do TRE-MA. A análise detalhada subsequente abordará as conclusões da auditoria e fornecerá recomendações práticas para aprimorar ainda mais a capacidade do TRE-MA em garantir a disponibilidade e integridade de seus dados críticos.

III. OBJETIVO DA AUDITORIA

16. Este trabalho de auditoria tem como objetivo avaliar a gestão de segurança da informação no âmbito do TRE-MA, de modo a certificar-se da conformidade e da adoção de um programa robusto de Gestão de Cópias de Segurança e Recuperação de Dados, utilizando como critério principal o *framework CIS Controls (The Center for Internet Security)* versão 8, especificamente o Controle 11 – Recuperação de Dados (*Data Recovery*).

IV. QUESTÕES DA AUDITORIA

17. Os testes para a realização desta auditoria foram elaborados pela SATIG a partir das seguintes questões de auditoria, conforme tabela abaixo:

Questões de Auditoria
Q1. A organização realiza, de forma regular e automática, cópias de segurança (*backups*) da sua principal base de dados?
Q2. A organização realiza, regularmente, cópias de segurança (*backups*) integrais dos servidores/máquinas que hospedam seu principal sistema?
Q3. A organização realiza, periodicamente, testes de restauração das cópias de segurança (*backups*) citadas nas questões anteriores?

Q4. A organização implementa mecanismos de controle de acesso para proteger as cópias de segurança (*backups*)?
Q5. A organização armazena as cópias de segurança (*backups*) em ao menos um destino não acessível remotamente?

V. ESCOPO

18. O escopo é importante para direcionar os trabalhos e dar conhecimento mais abrangente da auditoria para a Alta Administração e para a unidade auditada.

19. A necessidade de se proteger dados é premente na sociedade moderna. Para os órgãos da Administração Pública, a segurança da informação se torna fundamental. A Recuperação de Dados é a linha de defesa final contra a perda total ou a indisponibilidade prolongada.

20. Diante disso, selecionou-se como objeto de avaliação para esta auditoria o Controle 11 do *The Center for Internet Security (CIS Controls)* versão 8, denominado Recuperação de Dados (*Data Recovery*). Segundo o CIS, esse é um programa para desenvolver e manter uma capacidade de recuperação por meio de políticas, planos e procedimentos, garantindo que as cópias de segurança sejam isoladas, seguras e testadas, permitindo à organização restabelecer as operações rapidamente após um ataque ou desastre.

VI. CRITÉRIOS

21. Os critérios utilizados como parâmetros para fundamentar as avaliações apresentadas neste trabalho foram:

a) *CIS Controls Framework* – Versão 8 (Maio/2021);

b) Resolução CNJ n. 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

c) Resolução TSE n. 23.644/2021, que dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

d) Portaria CNJ n. 162/2021, que trata sobre Protocolos e Manuais criados pela Resolução CNJ n. 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

e) Decreto n. 9.637/2018, que Institui a Política Nacional de Segurança da Informação;

f) Portaria DG n. 101/2023, que Atualiza a Política de *Backup* e *Restore* de Dados no âmbito deste Regional, com o objetivo de estabelecer diretrizes para o processo de cópia e armazenamento dos dados, visando garantir a sua integridade e disponibilidade;

g) Lei n. 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD);

h) Lei n. 12.527/2011, Lei de Acesso à Informação;

i) Norma ABNT NBR ISO/IEC 27001:2013, SGSI – Requisitos; A.12.3 Cópias de Segurança;

j) Norma ABNT NBR ISO/IEC 27001:2013, SGSI – Código de prática; 12.3 Cópias de Segurança.

VII. ACHADOS DE AUDITORIA

22. Os achados representam o resultado dos testes de auditoria aplicados, das informações coletadas e da correlação dos documentos normativos internos (Portaria DG n. 101/2023) com os critérios externos de segurança (*CIS Controls* v8).

23. Não foram identificados achados que comprometam a arquitetura principal de resiliência (*air-gap* e criptografia, mitigados pelo Pregão Eletrônico n. 29/2021). Os achados concentram-se na esfera da Governança Documental.

24. **Achado 1 - Ausência de frequência de revisão formal da Política de *Backup*.**

Situação Encontrada	Conforme análise documental, constatou-se que a Portaria DG n. 101/2023 (Art. 5º, IX) prevê a proposição de modificações na política, mas não estabelece uma frequência mínima formal para a sua revisão (ex.: anual).
Critérios de Auditoria	*CIS Controls* v8 (Controle 11); ABNT NBR ISO/IEC 27001 (requisito de revisão e melhoria contínua de políticas).

Evidências	PT.E.1.0 - Formulário de coleta de dados (Questão 1.2).
Causas	Deficiência na Governança Documental por não institucionalizar o ciclo de vida e a revisão periódica da política.
Consequências	Risco de obsolescência da política frente à rápida evolução das ameaças cibernéticas e falha no processo de melhoria contínua da segurança.
Recomendações	Alterar ou complementar a Portaria DG n. 101/2023 para estabelecer uma frequência de revisão mínima anual da Política de *Backup*.

25. **Achado 2 - Lacuna na exigência formal de controles lógicos (MFA) para acesso privilegiado.**

Situação Encontrada	Após análise da Portaria DG n. 101/2023, constatou-se a omissão em seu texto principal quanto à exigência formal do uso de Autenticação Multifator (MFA) para acesso de gestão e administração ao ambiente de *backup* e seus consoles.
Critérios de Auditoria	*CIS Controls* v8 (Controle 11, Medida de Segurança 11.3 – Proteção de Cópias de *Backup*); Boas Práticas de Segurança da Informação (Acesso privilegiado).
Evidências	PT.E.2.0 - Verificação da Formalização do Controle de Acesso Privilegiado (MFA).
Causas	Deficiência na Governança Documental por não formalizar um controle de acesso crítico e básico em norma interna, embora seja uma boa prática de segurança amplamente reconhecida.
Consequências	Risco de Comprometimento de Credenciais e posterior uso de contas privilegiadas para sabotar ou excluir as cópias de segurança (neutralizando a resiliência do sistema).
Recomendações	Criar e formalizar uma norma de segurança que estabeleça a obrigatoriedade do uso de Autenticação Multifator (MFA) para todo acesso de gestão e administração ao ambiente de *backup*.

26. **Manifestação da unidade auditada sobre os achados:**

Despacho n. 89967/2024 – TRE-MA/PRES/DG/STIC/COINF/SERED (id. 2639008, SEI n. 0006899-40.2025.6.27.8000): “Em atenção ao Memorando nº 1129/2025 - TRE-MA/PRES/AI/SATIG (id. 2638756), manifesto minha concordância com os itens A1 –

Ausência de frequência de revisão da Política – e A2 – Falta de exigência formal na Política de Controles Lógicos (MFA), constantes na Planilha nº 2638833– Matriz de Achados –, bem como com as respectivas recomendações."

27. **Análise sobre a manifestação da unidade auditada:**

A unidade auditada corrobora o achado, motivo pelo qual apresentamos a seguinte proposta de encaminhamento.

28. **Proposta de encaminhamento:** Ante o exposto, recomenda-se:

À Secretaria de Tecnologia da Informação e Comunicação (STIC), a implementação das seguintes ações:

a) Formalização da Governança Documental: alterar ou complementar a Portaria DG n. 101/2023, para estabelecer o Planejamento e Procedimento de Revisão Anual da Política de *Backup*, garantindo a conformidade contínua e a atualização da norma frente à evolução das ameaças (ISO 27001);

b) Formalização de Controle de Acesso (MFA): criar e formalizar uma norma de segurança que estabeleça a obrigatoriedade do uso de Autenticação Multifator (MFA) para todo acesso de gestão e administração aos ambientes privilegiados de *backup* (servidores, consoles e repositórios).

29. **Conclusão:**

A manifestação da unidade auditada corrobora os achados de auditoria e as recomendações apresentadas no Quadro de Achados (id. 2638833, SEI n. 0006899-40.2025.6.27.8000), razão pela qual mantém-se a proposta de encaminhamento constante no item 28 deste Relatório.

VIII. CONCLUSÃO

30. No cenário mundial, as informações são um dos ativos organizacionais mais valiosos e, portanto, protegê-las adequadamente de ameaças digitais tornou-se meta essencial para garantir a sobrevivência e a confiança da sociedade na continuidade dos serviços prestados. A Gestão de Cópias de Segurança (*Backup*) e Recuperação de Dados faz parte de um conjunto abrangente de práticas, políticas e controles planejados para proteger as informações contra ameaças cibernéticas, interrupções de serviço e perdas acidentais, garantindo a disponibilidade e integridade dos dados.

31. Além disso, a Gestão de Cópias de Segurança é tida como medida essencial em um sistema de proteção organizacional, pois sabe-se que, em termos de segurança da informação e segurança cibernética, não existem sistemas ou organizações 100% seguros. Portanto, para que sistemas, serviços e processos possam ter maior resiliência e resistir a eventos de risco, contar com mecanismos eficientes de *backup*, isolamento e validação de restauração é parte fundamental para o sucesso na proteção organizacional.

32. Esta auditoria interna teve como objetivo avaliar a gestão de segurança da informação no âmbito do Tribunal Regional Eleitoral do Maranhão (TRE-MA), com base nos critérios estabelecidos pelo *CIS Controls (The Center for Internet Security)*, versão 8, especificamente o Controle 11 – Recuperação de Dados (*Data Recovery*). Este controle visa desenvolver e manter uma capacidade de recuperação por meio de políticas, planos, procedimentos, isolamento e testes, preparando a organização para restabelecer os serviços rapidamente após uma perda de dados.

33. No tocante à implementação do Controle 11 do *CIS Controls* v8 – Desenvolvimento e implementação de uma infraestrutura de *backup* e *restore* – verificou-se que o Tribunal, embora tenha estabelecido práticas significativas para a arquitetura de *backup*, apresenta lacunas de governança que necessitam de formalização: a frequência de revisão da política de *backup* e a exigência de Autenticação Multifator (MFA) para acesso privilegiado. Esses requisitos são essenciais para validar os planos existentes, proteger o ambiente de recuperação e garantir que a documentação acompanhe a evolução técnica do sistema.

IX. PROPOSTAS DE RECOMENDAÇÃO

34. Diante do exposto, submete-se o presente relatório à consideração do Dirigente da Auditoria Interna (AI), para posterior encaminhamento ao Exmo. Presidente deste Egrégio Tribunal, destacando as recomendações sugeridas à Secretaria de Tecnologia da Informação e Comunicação (STIC), conforme detalhamento a seguir:

35. a) Recomendar que a STIC altere ou complemente a Portaria DG n. 101/2023, para estabelecer o Planejamento e o Procedimento de Revisão Anual da Política de *Backup*, garantindo a melhoria contínua e a adequação da norma frente à evolução das ameaças cibernéticas (ISO/IEC 27001);

36. b) Criar e formalizar norma de segurança que estabeleça a obrigatoriedade da Autenticação Multifator (MFA) para todo acesso de gestão e administração ao ambiente de *backup* (*CIS Control* 11.3).

É o Relatório.

São Luís/MA, 11 de dezembro de 2025.

gov.br Documento assinado digitalmente
SARA AGUIAR GOMES
Data: 12/12/2025 07:34:12-0300
Verifique em https://validar.iti.gov.br

Sara Aguiar Gomes

Auditora interna
Técnico Judiciário - matrícula 3099950
Chefe da SATIG