AUDITORIA NO PROCESSO DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO
SEI nº. 0006899-40.2025.6.27.8000

O QUE FOI AUDITADO?

A Seção de Auditoria de Tecnologia de Informação e Comunicação e Governança – SATIG realizou a Auditoria no Processo de Gestão de Segurança da Informação, com foco na Gestão de Cópias de Segurança (*Backup*) e Recuperação de Dados, utilizando-se como critério principal o *framework CIS Controls (The Center for Internet Security)* versão 8, especificamente o Controle 11 – Recuperação de Dados.

Foram realizados exames de auditoria 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. 1.870/2024 (SEI n. 0018797-84.2024.6.27.8000).

O QUE FOI CONSTATADO?

Os achados representam o resultado dos testes de auditoria aplicados e da correlação de normas internas com os critérios de segurança.

Após a realização dos testes, e com base nas informações respondidas pela área de Tecnologia da Informação, chegou-se aos achados de auditoria, apresentados a seguir:

Achado 1: Ausência de frequência de revisão da Política de *Backup*.

Risco associado: A Portaria DG n. 101/2023 não estabelece prazo formal para revisão, comprometendo a melhoria contínua e a atualização da norma frente a novas ameaças (referência: ISO 27001).

Achado 2: Lacuna na exigência formal de MFA.

Risco associado: Ausência de exigência explícita de Autenticação Multifator (MFA) em norma interna para acesso ao ambiente de *backup*, deixando o controle de acesso privilegiado vulnerável ao roubo de credenciais (referência: CIS 11.3).

O QUE A SATIG RECOMENDA?

Para aprimorar a governança documental e o controle de acesso, foram realizadas as seguintes recomendações à Secretaria de Tecnologia da Informação e Comunicação (STIC):

Formalização da revisão: alterar ou complementar a Portaria DG n. 101/2023, para estabelecer o planejamento e o procedimento de revisão anual da Política de *Backup*;

Formalização da exigência de MFA: criar e formalizar norma de segurança que estabeleça a obrigatoriedade de MFA para todo acesso de gestão e administração ao ambiente de backup (servidores, consoles e repositórios).