



TRIBUNAL REGIONAL ELEITORAL DE PERNAMBUCO  
Av. Gov. Agamenon Magalhães, 1.160 - Bairro Graças - CEP 52010904 - Recife - PE

## RELATÓRIO DE MONITORAMENTO

Dando continuidade aos procedimentos típicos de auditoria, em consonância com os arts. 14 e 19 da Resolução TRE – PE n.º 389/2021, vem esta Coordenadoria de Auditoria Interna – COAUD iniciar, por meio do presente relatório, a etapa atinente ao monitoramento das recomendações provenientes da Auditoria no Processo de Gestão de Segurança da Informação (1959836), nos moldes dos art. 38 e 39 da supracitada Resolução.

Inicialmente, cumpre destacar que a análise sobre o atendimento das recomendações/determinações provenientes da presente auditoria deve ser computado com vistas a propiciar a mensuração dos indicadores estratégicos deste Tribunal, sob responsabilidade desta Secretaria, sendo eles:

- **Indicador 7:** Índice de atendimento de recomendações de auditoria institucionais;
- **Indicador 8:** Índice de cumprimento de planos de ação estabelecidos para atender recomendações de auditoria institucionais.

Pois bem, passa-se a análise das evidências e considerações apresentadas pelas unidades envolvidas a fim de comprovar o atendimento às recomendações encaminhadas.

À saída, importa registrar que a grande maioria das recomendações formuladas na presente auditoria **se encontram dentro do prazo acordado** com as unidades gestoras, em particular são 24 recomendações com prazos regulares, as quais serão ao final transcritas.

Por sua vez, percebem-se por **atendidas as recomendações a seguir elencadas.**

**ACHADO 7:** Insuficiência de controles voltados para desabilitar contas inativas

**Recomendação 7.5:** Que a Diretoria Geral oriente as unidades deste Tribunal para que se apropriem do conteúdo da [IN TRE-PE n.º 59/2021](#), especialmente quanto ao disposto no art. 37, de modo que os chefes imediatos passem a cumprir o comando estabelecido para inclusão, alteração, bloqueio exclusão de contas e acessos. Prazo: Junho de 2023. **ATENDIDA.**

**ACHADO 8:** Insuficiência de controles para manutenção da atualização dos acessos concedidos a usuários

**Recomendação 8.2:** Que a DG determine a todas unidades gestoras que, nos termos do art. 41 da [IN TRE-PE n.º 59/2021](#), definam o perfil de acesso à rede local dos usuários lotados em sua área de atuação, levando em conta os acessos e sistemas restritos ao desempenho de suas atividades. Prazo: Junho de 2023. **ATENDIDA.**

No que concerne às recomendações 7.5 e 8.2, observa-se abertura do processo SEI n.º 0006200-96.2023.6.17.8000 a fim de atender as recomendações em tela. Pela análise das providências

tomadas no mencionado feito, verifica-se que a Diretoria-Geral emitiu orientação às unidades do Tribunal, através do DESPACHO DG N° 1445/2023/GABDG (2167918), com vistas a dar conhecimento das recomendações da auditoria em questão, assim como dos objetivos e benefícios relacionados com as orientações emanadas. Ainda percebe-se que as mesmas orientações foram objeto de repasse aos Cartórios Eleitorais, através de e-mail (2175768), conforme solicitado pela Diretoria-Geral. Destarte, ponderando a atuação da Diretoria-Geral, **reputam-se por atendidas as recomendações em apreço.**

Em viés distinto, considerando a **ausência de informações**, no presente processo, sobre as providências realizadas para implementar a recomendação 10.5, computa-se como não atendida a mencionada recomendação, sendo ela:

**ACHADO 10:** Fragilidades nos controles de acessos físicos com potenciais impactos na segurança da informação.

**Recomendação 10.5:** Que a ASSEG estabeleça rotina de monitoramento para as atividades executadas pelos profissionais terceirizados que prestam serviço na recepção do prédio sede, visando assegurar que estejam realizando adequadamente as atividades e controles relacionados à permissão de acessos e coleta de dados de identificação dos colaboradores não alocados de serviços de TIC. Prazo: Janeiro de 2023. NÃO ATENDIDA.

Por fim, no sentido de melhor facilitar o acompanhamento pelas unidades gestoras, compartilham-se as **recomendações que se encontram dentro do regular prazo acordado.** Vejamos.

**Achado 1: Insuficiência de capacitação direcionada ao planejamento da contratação de TIC com foco em segurança da informação.**

**Recomendação 1:** Que os gestores, a partir das competências desempenhadas pelo integrante técnico da equipe de contratação de TIC, identifiquem novas possibilidades de capacitação e elabore trilhas de aprendizagem, de modo a assegurar o conhecimento necessário para confecção de artefatos da contratação de TIC, com foco na identificação de critérios e requisitos de segurança da informação. Prazo: **Junho de 2023.**

**Achado 2: Insuficiência nos controles dos requisitos de segurança da informação adotados nas contratações da área de tecnologia.**

**Recomendação 2.1:** Que a STIC formalize a atuação da SEGOR para verificação dos requisitos de segurança presentes nos artefatos produzidos na fase de planejamento das contratações de TIC, podendo instituir checklist, manuais de procedimentos, dentre outros que a unidade reputar válidos. Antes da formalização recomendada, a SEGOR deve avaliar as reais causas para as falhas evidenciadas na auditoria, dentre outras que venham a ser identificadas pela unidade, para aprimoramento do controle estabelecido. Prazo: **Junho de 2023.**

**Recomendação 2.2:** Que a STIC formalize, de forma sucinta, as orientações complementares ou boas práticas de segurança da informação, relevantes, que venham a ser repassadas à contratada nas reuniões iniciais de alinhamento de expectativas. Pode ser avaliada, por exemplo, a pertinência de incluir no modelo da ata tópico específico para registrar orientações à segurança da informação do Tribunal, que forem afetas ao objeto da contratação. Prazo: **Junho de 2023.**

**Recomendação 2.3:** Que a STIC implemente ações para atualizar o modelo do termo individual de ciência utilizado nas suas contratações, mantendo-os atualizados, na medida em que são editados, alterados ou revogados normativos relacionados à segurança da informação. Prazo: **Junho de 2023.**

**Recomendação 2.4:** Que a STIC avalie e estabeleça procedimentos ou mecanismos para revisar os requisitos de segurança da informação nas suas contratações, sempre que se fizer necessário e oportuno ao aprimoramento da relação contratual, em especial a de provedores de serviços. Prazo: **Dezembro de 2023.**

### **Achado 3 – Análise de riscos da contratação de provedores de serviços externos não formaliza adequadamente os riscos à segurança da informação.**

**Recomendação 3.1:** Que a STIC avalie riscos à segurança da informação nas contratações de provedor de serviços externo ou que envolvam alguma forma de assistência ou serviços de manutenção, considerando todo o ciclo de vida processo de contratação. Prazo: **Junho de 2023.**

**Recomendação 3.2:** Que a STIC adote procedimentos para gerenciar os riscos associados à segurança da informação durante a execução contratual, especialmente nas contratações de provedor de serviços externos. Prazo: **Junho de 2023.**

### **Achado 4 – Ausência de classificação e de inventário de provedores de serviços.**

**Recomendação 4:** Que a STIC estabeleça o inventário e classifique os provedores de serviços com as informações e critérios recomendados nos controles 15.1 e 15.3, respectivamente, do CIS Controls v. 8.0. Se reputar necessário, recomenda-se que a STIC elabore plano com as ações necessárias à implementação das referidas medidas de segurança, com cronograma e responsáveis. Prazo: **Dezembro de 2023.**

### **Achado 5: Ausência de política de gestão de provedores de serviços**

**Recomendação 5.1:** que o CGSI realize estudos a fim de apresentar à Alta Administração proposta de normativo instituindo a política de gestão de provedores de serviços do Tribunal, que contemple, no mínimo, as medidas de segurança recomendadas pelo controle 15 do [CIS Controls v. 8.0](#) ou outra mais atualizada, bem como das demais normas complementares que julgar necessária à aplicação das diretrizes estabelecidas na política. Prazo: **Dezembro de 2023.**

**Recomendação 5.2:** Que a STIC, enquanto não for instituída a política de gestão de provedores de serviços, estabeleça procedimento de monitoramento das contratações de provedores de serviços, definindo o que deve ser objeto de registro em segurança da informação e, no que for possível, adote padrão para o registro e acompanhamento das ocorrências **quanto ao tema pelas unidades gestoras da execução contratual.** Prazo: **Dezembro de 2023.**

### **Achado 6: Insuficiência de controles aplicados à gestão de contas.**

**Recomendação 6.1:** Que a STIC adote e implemente a rotina de realização de inventário de contas de usuários, administradores e serviços, com periodicidade definida, contendo no mínimo, nome da pessoa, nome do usuário, datas de início/término e departamento, visando assegurar que todas as contas ativas estejam autorizadas ([CIS Controls v. 8.0](#) – medida de segurança 5.1). Prazo: **Dezembro de 2023.**

### **ACHADO 7: Insuficiência de controles voltados para desabilitar contas inativas**

**Recomendação 7.1:** Que o CGSI avalie a possibilidade de propor a redução do prazo utilizado como referência no art. 42 da [IN TRE-PE n.º 59/2021](#), passando a desabilitar contas inativas após um período de 45 dias, aumentando a periodicidade do controle, seguindo a tendência da medida de segurança 5.3 recomendada pelo [CIS Controls v. 8.0](#). Prazo: Junho de 2023.

**Recomendação 7.2:** Uma vez acatadas as sugestões para melhoria dos controles instituídos, que se proceda, antecipadamente, a revisão da [IN TRE-PE n.º 59/2021](#), cujo prazo para tanto está previsto para 2025, tendo em vista as demandas surgidas a partir das fragilidades decorrentes deste trabalho de auditoria. Prazo: Dezembro de 2023.

**Recomendação 7.3:** Face às constantes e inovadoras ameaças cibernéticas relacionadas ao mal uso de recursos de TIC, que o CGSI avalie a oportunidade e conveniência de reduzir o prazo de revisão da [IN TRE-](#)

[PE n.º 59/2021](#) de 4 anos para 2 anos, a fim de adequá-la as recomendações do [CIS Controls v. 8.0](#). Prazo: Dezembro de 2023.

**Recomendação 7.4:** Que a CGSI, crie ou adapte formulário SEI específico para solicitação de abertura de contas e novos acessos, e que a obrigatoriedade de utilização do documento, devidamente preenchido, seja formalizado às unidades usuárias por meio da mesma comissão, conforme melhor interpretação do art. 37 da IN n.º 59/2021. Prazo: Junho de 2023

#### **ACHADO 8: Insuficiência de controles para manutenção da atualização dos acessos concedidos a usuários.**

**Recomendação 8.3:** Que a STIC estabeleça rotinas e controles que viabilizem a atualização dos acessos a recursos de TIC em casos de mudança de lotação. A título de controle, considerando a boa prática estabelecida pelo art. 17 da [Portaria TSE n.º 454/2021](#), sugere-se o estabelecimento de um perfil mínimo/padrão de acesso para usuários, para o qual deverão retornar em caso de mudança de lotação, a partir da formalização de exclusão de acessos de TIC prevista na recomendação 1. Prazo: **Dezembro de 2023**.

**Recomendação 8.4:** Que o CGSI apresente proposta de modelo de Termo de Responsabilidade e Confidencialidade para utilização de recursos de TIC, conforme previsto no art. 8º da [IN TRE-PE n.º 59/2021](#), submetendo-o à DG para que a unidade ciente a todos os gestores a necessidade de inclusão do documento na deflagração do procedimento. Prazo: **Junho de 2023**.

#### **Achado 09: Ausência de implementação de MFA para as contas de acesso administrativo em todos os ativos corporativos.**

**Recomendação 9.1:** Que a STIC apresente cronograma referente ao processo de aquisição da ferramenta MFA, e, tão logo consiga adquirir e implementar a aplicação do controle para as contas de acesso administrativo em todos os ativos corporativos, bem como para os sistemas administrativos críticos, ciente a unidade de auditoria para que atualize o monitoramento das recomendações. Prazo: **Junho de 2023**.

**Recomendação 9.2:** Que a STIC apresente planejamento com o respectivo plano de ação para implementação do MFA, também, para todos os novos sistemas desenvolvidos internamente, conforme informado pela COSIS no item 8. Prazo: **Dezembro de 2023**.

#### **ACHADO 10: Fragilidades nos controles de acessos físicos com potenciais impactos na segurança da informação.**

**Recomendação 10.1:** Que o Comitê de Governança de Segurança da Informação – CGSI, nos termos do art. 11 da Res. TSE n.º 23.644, estude a viabilidade de propor alteração dos normativos internos para estabelecer:

a) Obrigação de que quaisquer serviços derivados de contratações de TIC, com acesso de prestadores de serviço não alocado às instalações da Justiça Eleitoral de Pernambuco, conquanto dentro do horário de expediente, seja precedido de comunicação prévia formalizada à ASSEG e às demais unidades externas fora da sede, com indicação do nome, matrícula ou o número da carteira de identidade, nome da empresa, tipo de atividade ou serviço a ser executado, bem como local, data e tempo previsto de permanência. Prazo: **Dezembro de 2023**.

b) O monitoramento presencial da execução dos serviços de TIC pelo fiscal técnico dos contratos ou por outro servidor designado para essa função. Prazo: **Dezembro de 2023**.

**Recomendação 10.2:** Que a STIC, enquanto não houver apreciação da recomendação 1.1, adote a rotina de encaminhar, sempre que possível, aviso prévio para ASSEG, bem como para as demais unidades externas à sede, quando da ocorrência de quaisquer serviços de TIC realizados dentro do horário do expediente, cujo teor deve conter no mínimo: o serviço a ser realizado, as datas e horários previstos, o nome da empresa, o nome

completo do(s) terceirizados que realizarão o serviço e o nome do gestor do contrato ou do responsável pelo acompanhamento do terceirizado e do serviço. Prazo: **Junho de 2023**.

**Recomendação 10.3:** Que o CGSI, com a participação Conselho de Zonas Eleitorais – CONZE, defina controles a serem implementados nas demais instalações da Justiça Eleitoral, externos à sede, visando o estabelecimento e padronização dos registros de dados relacionados a todos os profissionais não alocados prestadores de serviço de TIC. Prazo: **Dezembro de 2023**.

**Recomendação 10.4:** Que o CGSI avalie a oportunidade e conveniência de propor melhoria nas normas específicas direcionadas ao controle de acesso físico e lógico relacionados à segurança da informação, podendo, a título de exemplo, avaliar os comandos adotados pela [Portaria TSE n.º 454/2021](#). Prazo: **Dezembro de 2023**.

**Recomendação 10.6:** Que a ASSEG estabeleça procedimento e controles de acesso ao Centro de Processamento de Dados – CPD, com o registro da visita de colaborador para prestação de serviço de TIC contendo, no mínimo, as informações estabelecidas no art. 5º da [IN TRE-PE n.º 58/2021](#), acrescida das informações da empresa contratada. Prazo: **Junho de 2023**.

É o relatório de monitoramento, o qual submeto à apreciação superior.

Respeitosamente,



Documento assinado eletronicamente por **MARIA ROBERTA REIS LINS**, **Coordenador(a)**, em 03/05/2023, às 12:43, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site [http://sei.tre-pe.jus.br/sei/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](http://sei.tre-pe.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0) informando o código verificador **2199603** e o código CRC **733EABED**.

