Tribunal Regional Eleitoral
do Pará

AUDITORIA INTEGRADA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Relatório de Monitoramento – 1º Ciclo

(Processo nº 0008530-84.2022.6.14.8000)

SEAUD
SECRETARIA DE AUDITORIA

Sumário

1. APRESENTAÇÃO

Em atenção ao Plano Anual de Auditoria (PAA) 2023, a SEAUD, por meio da Seção de Auditorias Coordenadas e Integradas (SECOI), apresenta o relatório do 1º ciclo de monitoramento das recomendações expedidas no âmbito da Auditoria Integrada da Justiça Eleitoral 2022, cujo objeto foi a verificação o nível de implementação dos processos de cibersegurança, adotados pelo setor de tecnologia da informação (TI), com práticas e medidas de segurança (controles internos) recomendadas pelo framework CIS Controls V8.

Com base no resultado dos testes e exames efetuados, foram emitidas originalmente 06 (seis) recomendações à área responsável, visando à adoção de boas práticas de segurança cibernética conforme indicado pelo framework CIS Controls V8. Após manifestação da unidade auditada (STI/CGSI), obteve-se insumos para elaboração deste relatório.

Este 1º ciclo de monitoramento foi realizado nos meses de setembro e outubro/2023, com o objetivo de verificar o cumprimento das recomendações resultantes da auditoria. Além disso, procurou-se aferir os resultados obtidos, alcançando-se os seguintes benefícios:

- Efetividade das recomendações emitidas nas auditorias aludidas
- Aperfeiçoamento dos mecanismos de controle de segurança cibernética do TRE
- Redução das deficiências que propiciem a ocorrência de riscos de alto e médio impacto
- Implementação tempestiva de ações corretivas adequadas.

2. METODOLOGIA APLICADA

A técnica de análise documental foi aplicada no monitoramento, no estágio preliminar de análise do cumprimento das recomendações (etapa de planejamento), por meio da busca por evidências e dados objetivos, para dar suporte à tomada de providências por parte dos gestores.

A análise documental também foi aplicada nos testes de monitoramento, a partir de informações repassadas pelas unidades à SECOI, conforme despacho CGSI (Coordenadoria de Gestão da Segurança da Informação) apresentado no evento nº 2030151 (SEI 0008530-84.2022.6.14.8000). Nesse sentido, o objetivo dos testes foi obter informações mais precisas sobre o contexto do cumprimento das recomendações, propiciando uma avaliação mais segura à equipe responsável pelo monitoramento.

Além da análise documental, foram realizados exames de registros, através de consultas a processos SEI, que tratam de ações empreendidas pelos gestores no cumprimento das recomendações.

3. ANÁLISE PRELIMINAR SOBRE O CUMPRIMENTO DAS RECOMENDAÇÕES

No relatório final da auditoria (evento SEI nº 1648308), foram apontadas 06 (seis) recomendações a serem cumpridas, todas direcionadas à STI (Secretaria de Tecnologia da Informação. Visando as providências para o cumprimento das recomendações,

A STI/CGSI, apresentou o plano de ação acostado no Processo SEI 0008530-84.2022.6.14.8000, evento nº 1903062.

Em observação e análise preliminar do processo, a equipe de auditoria já pôde notar o andamento de ações relativas ao referido plano.

4. TESTES DE MONITORAMENTO

Nos testes realizados, além da análise documental e exames de registros no processo SEI, aplicaram-se papéis de trabalho para a obtenção de informações dos gestores, como forma de prospecção de evidências sobre o status de implementação das recomendações.

A STI/CGSI informou através da planilha de levantamento (evento SEI nº 2038609) acostada no Processo SEI 0008530-84.2022.6.14.8000, o status e evidências de cada recomendação emitida na auditoria.

Para aferição do grau de implementação das referidas recomendações, adotou-se a seguinte classificação:

Quadro 1 - Classificação das Recomendações

Implementada (I)	Recomendação cumprida totalmente;
Em Implementação (EI)	Quando iniciadas ações objetivando o cumprimento da recomendação que, por questões operacionais, ainda não foi cumprida totalmente;
Não Implementada (NI)	Quando não iniciadas ações objetivando o cumprimento da recomendação;
Prejudicada (P)	Superveniência de fatos que tornem inexequível o cumprimento da recomendação, ou configuração de contexto em que a recomendação não seja mais aplicável ou relevante.

O quadro 1 apresenta as recomendações com seus status resultantes das análises realizadas pela equipe de auditoria no ciclo atual. Neste ponto, destaca-se que as análises detalhadas sobre o cumprimento de cada recomendação, bem como das conclusões da equipe de auditoria, são apresentadas no Apêndice II - **Detalhamento da Avaliação das Evidências**.

Quadro 2 - Status das recomendações - 1º Ciclo

RECOMENDAÇÃO	UNIDADE	STATUS (4ºCiclo)
R1: Estabeleça procedimento para normatização acerca de uma política de gestão de provedores de serviços. Essa política deve abordar a classificação, inventário, avaliação, monitoramento e descomissionamento de provedores de serviços. Além disso, a política instituída deve estabelecer também períodos de revisão e atualização periódica.	STI (CGSI)	EI
R2: Implemente um inventário de prestadores de serviços, que forneça um repositório de todos os provedores de serviços, com seu respectivo contato corporativo. Esse inventário, pode classificar os provedores através de características, tais como sensibilidade de dados, volume de dados, requisitos de disponibilidade, regulamentos aplicáveis. O inventário implementado deve ser revisto e atualizado periodicamente.	STI (CGSI)	I
R3: Inicie procedimentos para formalização de um processo de gestão contratual, que inclua aspectos específicos de segurança da informação (SI), abrangendo o planejamento, a execução de contratos (conclusão e rescisão - descomissionamento) e o gerenciamento de riscos. Além de itens que assegurem a notificação e resposta a incidentes de segurança e/ou violação de dados, requisitos de criptografia de dados e compromissos de descarte de dados (termos de compromissos/confidencialidade/sigilo).	STI (CGSI)	I
R4: Implemente mecanismos de configuração de senhas que assegurem a utilização de senhas fortes (letras, números e, se possível, caracteres especiais), por parte dos usuários. Como por exemplo, práticas recomendadas incluem, no mínimo, uma senha de 8 caracteres para contas que usam MFA (Autenticação Multifator) e uma senha de 14 caracteres para contas que não usam MFA.	STI (CGSI)	I

RECOMENDAÇÃO	UNIDADE	STATUS (4ºCiclo)
R5: Estabeleça políticas, padrões e guias que exijam a implementação de recursos de MFA (Autenticação Multifator) em sistemas expostos externamente, para acesso remoto à rede interna do TRE (ex: VPN). O que deve também ser observado, de forma combinada, com a Recomendação R4.	STI (CGSI)	I
R6: Normatize os procedimentos de controle de acesso físico aos setores institucionais, por parte dos prestadores de serviços de TI. Envolvendo também, mecanismos de monitoramento e revogação do acesso, obedecendo os requisitos de segurança da informação.	STI (CGSI)	I

I - Implementada / EI - Em implementação

5. CONCLUSÃO

O aumento do nível de segurança cibernética da informação na Justiça Eleitoral tem recebido importante atenção por parte da alta administração. O atendimento das recomendações observadas nesta auditoria, direcionadas à adoção de padrões, práticas e modelos nos processos de trabalho, tem impulsionado a implementação de inovação e melhorias no objeto auditado.

Ao término deste 1º ciclo de monitoramento observa-se que apenas 01 (uma) recomendação, das 6 (seis) emitidas, está em andamento, e as demais estão concluídas.

Outrossim, segundo análise da equipe de auditoria, não se considera esta recomendação ainda pendente de implementação, como crítica, que seria uma situação que caso não fosse tratada de modo urgente, poderia comprometer e trazer prejuízos relevantes à gestão.

Sendo assim, com base nos apontamentos realizados neste relatório, submete-se à decisão da Presidência a realização de um 2º ciclo de monitoramento no próximo exercício, a fim de que se possa avaliar a implementação da recomendação R1, ainda em implementação (conforme apresentado no Quadro 2).

É o Relatório.

Belém, 10 de novembro de 2023.

gov.br Documento assinado digitalmente
CLAUDIA MYLENE PINHEIRO RIBEIRO
Data: 13/11/2023 13:27:57-0300
Verifique em https://validar.iti.gov.br

CLÁUDIA MYLENE PINHEIRO RIBEIRO

SECRETÁRIA DE AUDITORIA

gov.br Documento assinado digitalmente
SALOMAO FERNANDES DE FREITAS JUNIOR
Data: 10/11/2023 14:50:51-0300
Verifique em https://validar.iti.gov.br

SALOMÃO FERNANDES DE FREITAS JÚNIOR

SEÇÃO DE AUDITORIAS COORDENADAS E INTEGRADAS – SECOI

gov.br Documento assinado digitalmente
MARCO ANTONIO FAGUNDES DE MORAES
Data: 13/11/2023 09:56:05-0300
Verifique em https://validar.iti.gov.br

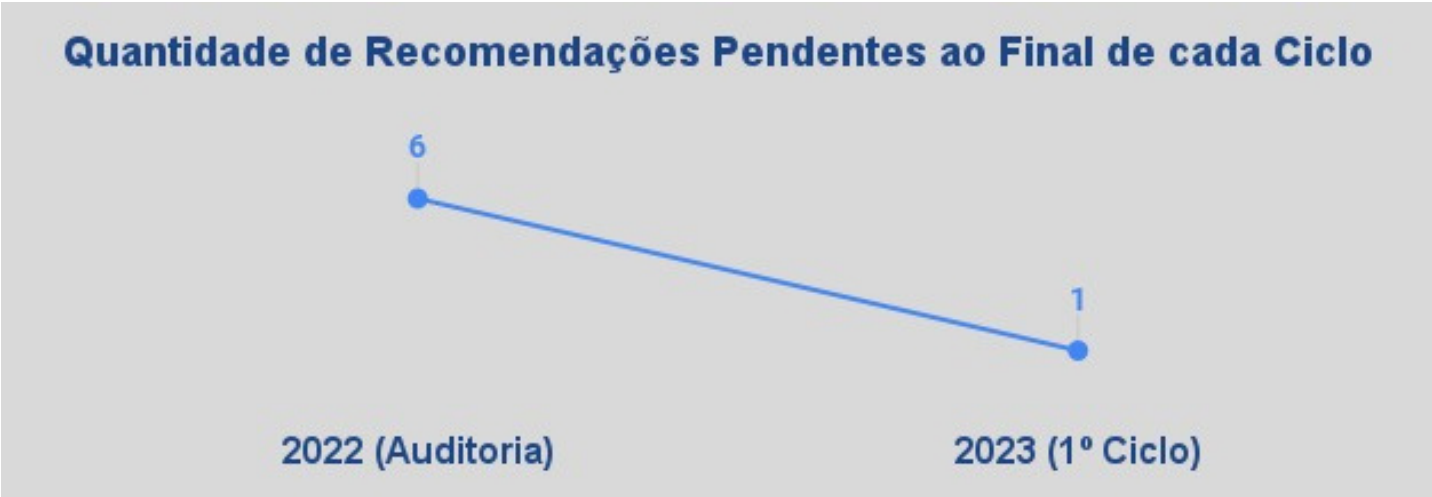
MARCO ANTONIO FAGUNDES DE MORAES

SEÇÃO DE AUDITORIAS COORDENADAS E INTEGRADAS - SECOI

APÊNDICE I – HISTÓRICO DE MONITORAMENTO

Figura A.1 – Histórico de monitoramentos

Figura A.2 – Quantidade de Recomendações Pendentes ao longo dos ciclos



APÊNDICE II – DETALHAMENTO DA AVALIAÇÃO DAS EVIDÊNCIAS

1º CICLO DE MONITORAMENTO DAS RECOMENDAÇÕES DA AUDITORIA INTEGRADA DE AVALIAÇÃO DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Recomendação R1: Estabeleça procedimento para normatização acerca de uma política de gestão de provedores de serviços. Essa política deve abordar a classificação, inventário, avaliação, monitoramento e descomissionamento de provedores de serviços. Além disso, a política instituída deve estabelecer também períodos de revisão e atualização periódica.
Destinatário da recomendação: Secretaria de Tecnologia da Informação (STI) / Coordenadoria de Gestão da Segurança da Informação (CGSI)

Evidências apresentadas:

Referência normativa: Art. 58. (CAPÍTULO VII) da proposta de Portaria de GESTÃO DE IDENTIDADE E O CONTROLE DE ACESSO FÍSICO E LÓGICO (minuta de Portaria, evento 2018816).
Essa proposta para normatização de política de gestão de provedores de serviços foi formalizada e incluída na minuta de norma Complementar à PSI/JE processo SEI 0009809-08.2022.

Após análise das evidências apresentadas, conclui-se que a recomendação possui o seguinte status:
( ) Implementada (**X**) Em implementação ( ) Não implementada ( ) Prejudicada

Considerações do auditor:

Os esforços empreendidos pela unidade auditada, para cumprimento da recomendação, estão evidenciados pela elaboração da minuta da portaria, sendo que o seu status somente será modificado para "implementada" após a publicação da Portaria de Gestão de Identidade e o Controle de Acesso Físico e Lógico.

Assim, de acordo com o contexto apresentado, conclui-se que a unidade auditada está trabalhando para a conclusão desta recomendação, razão pela qual a equipe de auditoria entende que a mesma classifica-se com o status Em implementação (EI).

Recomendação R2: Implemente um inventário de prestadores de serviços que forneça um repositório de todos os provedores de serviços, com seu respectivo contato corporativo. Esse inventário, pode classificar os provedores através de características, tais como sensibilidade de dados, volume de dados, requisitos de disponibilidade, regulamentos aplicáveis. O inventário implementado deve ser revisto e atualizado periodicamente.

Destinatário da recomendação: Secretaria de Tecnologia da Informação (STI) / Coordenadoria de Gestão da Segurança da Informação (CGSI)

Evidências apresentadas:

Conforme evento nº 1903062 (0008530-84.2022.6.14.8000), a CGSI desenvolveu o inventário baseado em planilha de prestadores de serviços. O modelo proposto tem como base o Controle 15 - "Gestão de provedor de serviços" do CIS Controls V 8. A planilha está disponível em:https://docs.google.com/spreadsheets/d/1MMTGn8QKNAYNFmK048xE_3-ESIgv8IrGNdUmd4uv688/edit?usp=sharing (Acesso em 06/11/2023)

Após análise das evidências apresentadas, conclui-se que a recomendação possui o seguinte status:

(**X**) Implementada ( ) Em implementação ( ) Não implementada ( ) Prejudicada

Considerações do auditor:

Os esforços empreendidos pela unidade auditada, para cumprimento da recomendação, estão evidenciados no inventário elaborado e disponível pela CGSI .

Assim, de acordo com o contexto apresentado, conclui-se que a unidade auditada atendeu o previsto no critério utilizado, razão pela qual a equipe de auditoria entende que a mesma classifica-se com o status implementada (I).

Recomendação R3: Inicie procedimentos para formalização de um processo de gestão contratual, que inclua aspectos específicos de segurança da informação (SI), abrangendo o planejamento, a execução de contratos (conclusão e rescisão - descomissionamento) e o gerenciamento de riscos. Além de itens que assegurem a notificação e resposta a incidentes de segurança e/ou violação de dados, requisitos de criptografia de dados e compromissos de descarte de dados (termos de compromissos/confidencialidade/sigilo).

Destinatário da recomendação: Secretaria de Tecnologia da Informação (STI) / Coordenadoria de Gestão da Segurança da Informação (CGSI)

Evidências apresentadas:

Sobre a revisão de critérios associados à gestão contratual a CGSI apresentou o Guia Orientativo com Modelos De Cláusulas Gerais à Proteção de Dados Pessoais no âmbito do TRE-PA (evento n º 1769793). Somando-se às seguintes evidências: (1) Contrato Nº 34 / 2023 (evento 1900779) - Cláusula Décima Quarta - Da Proteção de Dados Pessoais; e (2) Contrato Nº 57 / 2023 (evento 1929607) - Cláusula Décima Quinta - Da Proteção de Dados Pessoais.

Após análise das evidências apresentadas, conclui-se que a recomendação possui o seguinte status:

(**X**) Implementada ( ) Em implementação ( ) Não implementada ( ) Prejudicada

Considerações do auditor:

Os esforços empreendidos pela unidade auditada, para cumprimento da recomendação, estão evidenciados no guia orientativo, e nas cláusulas implementadas nos contratos informados.

Assim, de acordo com o contexto apresentado, conclui-se que a unidade auditada atendeu o previsto no critério utilizado, razão pela qual a equipe de auditoria entende que a mesma classifica-se com o status implementada (I).

Recomendação R4: Implemente mecanismos de configuração de senhas que assegurem a utilização de senhas fortes (letras, números e, se possível, caracteres especiais), por parte dos usuários. Como por exemplo, práticas recomendadas incluem, no mínimo, uma senha de 8 caracteres para contas que usam MFA (Autenticação Multifator) e uma senha de 14 caracteres para contas que não usam MFA.

Destinatário da recomendação: Secretaria de Tecnologia da Informação (STI) / Coordenadoria de Gestão da Segurança da Informação (CGSI)

Evidências apresentadas:
A CSGI implementou um novo sistema de configuração de senhas, assegurando a utilização de senhas fortes (letras, números e caracteres especiais), com no mínimo 10 caracteres, foi implementado em 28/09/2022. Este novo sistema está disponível no processo de troca de senha: https://acesso.tre-pa.jus.br/portal/#/recuperar-senha. Conforme Art. 36, inciso I, minuta de Portaria - evento nº 2018816.

Após análise das evidências apresentadas, conclui-se que a recomendação possui o seguinte status:
(**X**) Implementada ( ) Em implementação ( ) Não implementada ( ) Prejudicada

Considerações do auditor:
Os esforços empreendidos pela unidade auditada, para cumprimento da recomendação, estão evidenciados na implementação de novo sistema de configuração de senhas disponível pela CGSI e da portaria que normatiza a matéria.

Assim, de acordo com o contexto apresentado, conclui-se que a unidade auditada atendeu o previsto no critério utilizado, razão pela qual a equipe de auditoria entende que a mesma classifica-se com o status implementada (I).

Recomendação R5: Estabeleça políticas, padrões e guias que exijam a implementação de recursos de MFA (Autenticação Multifator) em sistemas expostos externamente, para acesso remoto à rede interna do TRE (ex: VPN). O que deve também ser observado, de forma combinada, com a Recomendação R4.

Destinatário da recomendação: Secretaria de Tecnologia da Informação (STI) / Coordenadoria de Gestão da Segurança da Informação (CGSI)

Evidências apresentadas:

A CGSI implementou duas formas de acesso aos sistemas externos, conforme Plano de Ação (evento 1903062): (1) Acesso a sistemas expostos externamente utilizando Autenticação Multifator (MFA) foi disponibilizado por meio do novo Portal de Acesso (https://portal.tre-pa.jus.br); e (2) Acesso à VPN com autenticação usando credenciais do Google Workspace e implementação de 2FA (https://connect.tre-pa.jus.br). Estes acesso estão conforme previsto no Art. 34, § 2º da Minuta de Portaria - evento nº 2018816.

Após análise das evidências apresentadas, conclui-se que a recomendação possui o seguinte status:

(**X**) Implementada ( ) Em implementação ( ) Não implementada ( ) Prejudicada

Considerações do auditor:

Os esforços empreendidos pela unidade auditada, para cumprimento da recomendação, estão evidenciados na implementação de novo mecanismo de acesso a sistemas externos disponível pela CGSI e da portaria que normatiza a matéria.

Assim, de acordo com o contexto apresentado, conclui-se que a unidade auditada atendeu o previsto no critério utilizado, razão pela qual a equipe de auditoria entende que a mesma classifica-se com o status implementada (I).

Recomendação R6: Normatize os procedimentos de controle de acesso físico aos setores institucionais, por parte dos prestadores de serviços de TI. Envolvendo também, mecanismos de monitoramento e revogação do acesso, obedecendo os requisitos de segurança da informação .

Destinatário da recomendação: Secretaria de Tecnologia da Informação (STI) / Coordenadoria de Gestão da Segurança da Informação (CGSI)

Evidências apresentadas:

A CGSI apontou a implementação do controle através do Art. 16. da PORTARIA TRE-PA Nº 21586/2022 TRE/PRE/DG/GPJ (evento nº 1716006).

Após análise das evidências apresentadas, conclui-se que a recomendação possui o seguinte status:

(**X**) Implementada ( ) Em implementação ( ) Não implementada ( ) Prejudicada

Considerações do auditor:

A indicação do normativo pela unidade auditada evidencia o cumprimento da recomendação, uma vez que regulamenta procedimentos de controle de acesso físico a setores institucionais, inclusive à área de tecnologia do TRE/PA.

Assim, de acordo com o contexto apresentado, conclui-se que a unidade auditada atendeu o previsto no critério utilizado, razão pela qual a equipe de auditoria entende que a mesma classifica-se com o status implementada (I).