TRIBUNAL REGIONAL ELEITORAL DE SERGIPE
CENAF, Lote 7, Variante 2 - Bairro Capucho - CEP 49081-000 - Aracaju - SE - http://www.tre-se.jus.br
seaug@tre-se.jus.br(79) 3209-8847

RELATÓRIO DE AUDITORIA 6/2024 - SEAUG

RELATÓRIO		**Preliminar**		**Conclusivo**	**x**	**Monitoramento**	
INTERESSADO(S)	Secretaria de Tecnologia da Informação e Comunicação (STI) Secretaria Judiciária (SJD)						

SUMÁRIO

I. INTRODUÇÃO

1.1 Visão Geral do Objeto Monitorado:

Trata-se do 2º Relatório de Monitoramento da Auditoria na Gestão de Segurança da Informação e no controle de Acessos às Informações e aos Recursos de Processamento das Informações, sendo objeto de avaliação as recomendações emitidas pela Coordenadoria de Auditoria Interna – COAUD e ainda não implementadas por ocasião do 1º monitoramento, conforme Relatório de Auditoria 6 (1544184).

Durantes os trabalhos foram necessárias a solicitação de manifestação das unidades envolvidas e a realização de testes, subsidiando, juntamente com outros exames, as avaliações quanto à situação de implementação das recomendações. Os procedimentos e conclusões são descritos ao longo deste relatório.

A equipe responsável pela avaliação foi composta por Luiz Fernando Brito de Carvalho e Ivanildo Alves de Medeiros (revisor), sob a supervisão de Adail Vilela de Almeida. Os trabalhos foram realizados sem limitações para a execução dos exames necessários.

1.2 Objetivo

O presente monitoramento verificou o atendimento das recomendações referenciadas no item II deste relatório.

Destaca-se que ocorreram alterações em normativos relativos aos temas das recomendações:

- Alteração da Portaria TRE/SE 41/2020, pela Portaria 506/2022;
- Atualização da norma ISO 27002 em 2022.

Os exames realizados consideraram as alterações nas normas citadas.

II. RESULTADOS DAS AVALIAÇÕES DAS RECOMENDAÇÕES

2.1 A STI demonstrou atendimento aos aspectos formais prescritos no item 3.8, Anexo II, da Portaria 41/2020, portanto a recomendação relativa à identificação genérica e ao uso compartilhado dos computadores foi implementada.

Recomendação À STI: Adotar medidas para que a identificação genérica e o uso compartilhado dos computadores do plenário do Tribunal revistam-se dos aspectos formais prescritos no art. 12 da Portaria TRE/SE 192/2018.

2.1.1. Instrumentos avaliados:

Portaria TRE/SE 41/2020 (que revogou a Portaria 192/2018), alterada pela Portaria 506/2022.

2.1.2. 1ª Avaliação:

Após a emissão do 1º Relatório de Monitoramento da Auditoria em Segurança da Informação, Relatório de Auditoria 10 (1089730), a COINF manifestou-se por meio da Informação 4768/2021 (1097501) quanto a implementação da seguinte ação: "Inicializar o processo de consulta, por meio do processo SEI nº 0018326-30.2021.6.25.8000, ao setor negocial para formalizar o disposto no art. no art. 12 da Portaria TRE/SE 192/2018 (Revogada pela Portaria TRE/SE 41/2020)."

Formalizado o processo de consulta à SJD, esta, por meio da COREP (Informação 4848/2021 – SEI 1099493), apontou que a dinâmica da sessão plenária "exige que os computadores que serão utilizados pelos Membros desta Corte estejam ligados e testados antes do início do ato solene, evitando-se assim qualquer intercorrência que atrase ou impeça a sua realização", acrescentando sugestão para que "seja implementada nova rotina nos computadores do plenário mencionados na Consulta SESOP 1092070, no sentido de que sejam logados por um servidor específico do NAP (Núcleo de Apoio às Sessões Plenárias), o qual será detentor das informações (usuários e senhas) para acesso às referidas máquinas", ressaltando a necessidade de manutenção de "um técnico da Central de Serviços que dê o suporte necessário, caso ocorra qualquer problema técnico".

A COINF (Informação 4886/2021 – SEI 1100929) indicou a viabilidade técnica do proposto pela COREP, e encaminhou o processo ao Gab-Ciberseg para avaliação de riscos e emissão de parecer.

O Gab-Ciberseg apresentou **Relatório de Análise de Riscos** por meio da Informação 3452/2022 (SEI 1210237), manifestando-se para que "seja acatada a solicitação de continuidade do acesso por identificação genérica, de acordo com a exceção preceituada no item 3.8 do Anexo II (Acesso à Rede Corporativa) da Portaria TRE-SE 41/2020", apresentando, "sob pena de revogação imediata desta forma de acesso não pessoal àqueles computadores, além das demais sanções previstas para os responsáveis", as seguintes **diretrizes**:

> a) As credenciais genéricas atribuídas aos membros devem ser restritas ao acesso aos computadores localizados no plenário.
>
> b) A unidade técnica, na administração dos acessos genéricos, deve observar estritamente o princípio do mínimo privilégio, excluindo qualquer acesso a recursos não indispensáveis para o andamento da sessão plenária. Todas as demais atividades devem ser executadas exclusivamente pelas contas pessoais dos magistrados.
>
> c) O servidor que detiver as credenciais de acesso genéricas correspondentes aos membros do Tribunal para acesso aos computadores do plenário deve observar o item 4.4 do Anexo II (Acesso à Rede Corporativa) da Portaria TRE-SE 41/2020. Em hipótese alguma será permitida a divulgação ou o compartilhamento das senhas, mesmo que para superiores hierárquicos. Caso seja necessário, por qualquer razão, o acesso às credenciais por servidor diverso daquele inicialmente designado, as senhas devem ser alteradas imediatamente, garantindo-se que apenas uma única pessoa tenha o seu conhecimento.
>
> d) A SJD deve manter controle estrito de qual dos seus servidores é o responsável, a cada período de tempo, pela detenção das credenciais de acesso, consignando no termo de responsabilidade próprio (Anexo IX da Portaria TRE-SE 41/2020) os períodos inicial e final - contendo data, hora e minuto - em que cada servidor alterou ou tomou conhecimento de qualquer uma das senhas atribuídas às credenciais genéricas, permitindo posteriores auditorias, caso necessárias.

2.1.3. Resposta das Unidades Auditadas:

Foram solicitados, por meio da Comunicação Interna 16/2024 (1487739), manifestação e documentos que evidenciem a implementação das diretrizes indicadas no Relatório de Análise de Riscos do Gab-Ciberseg (SEI 1210237), sendo obtidas as seguintes respostas:

A STI, por meio da Informação 2269 – SESOP (1520149), evidenciou que:

> 1. As credenciais genéricas são restritas ao acesso dos computadores do plenário;
>
> 2. Foi aplicada atribuição de mínimo privilégio às credenciais de acesso genérico, com exclusão de acesso a recursos não indispensáveis à sessão plenária.

A SJD, por meio da Informação 2114/2024 - COREP (1517279), respondeu que:

> 1. As credenciais de acesso genérico são geradas e gerenciadas pela titular do Núcleo de Apoio às Sessões Plenárias, tendo substitutas designados em caso de afastamentos (licenças e/ou férias);
>
> 2. As sessões plenárias são realizadas, ou no meio do expediente, ou após, conferindo tempo suficiente à chegada da titular;
>
> 3. Não há histórico de atraso ou não realização de sessão plenária;
>
> 4. Os servidores da Coordenadoria são orientados a comunicar à chefia imediata, com antecedência ou de imediato (caso fortuito ou força maior), que avaliando os riscos, adota providências

necessárias, pela indicação de substituto ou avocação das atividades para si;

5. Não existe possibilidade de atraso ou não realização de sessões plenárias, visto que a Coordenadoria, substitutos automáticos e serventuárias, possuem pleno domínio das tarefas atinentes à realização da sessão, caso ocorra impontualidade ou ausência do servidor detentor das credenciais;

6. O compartilhamento das credenciais, no caso de substituição, é precedido das devidas orientações afetas aos cuidados cibernéticos;

7. O controle dos termos de responsabilidade (Anexo IX da Portaria TRE-SE 41/2020) e de histórico (período inicial e final), encontra-se em fase de implantação.

2.1.4. 2ª Avaliação:

O critério de avaliação, adotado por esta unidade de auditoria, referencia-se no item 3.8, Anexo II, da Portaria 41/2020 (regra que substituiu o art. 12 a Portaria 192/2018), transcrito abaixo:

> 3.8 Não haverá identificação genérica e de uso compartilhado para acesso aos recursos da rede, excetuando-se os casos de necessidade, justificada e acompanhada de parecer da STI, acerca da possibilidade de aceitação dos riscos associados.

A STI demonstrou, por meio do Processo 0018326-30.2021.6.25.8000, atendimento aos aspectos formais prescritos na norma, estabelecendo:

- Consulta à SJD acerca da necessidade de identificação genérica nos computadores em uso nas sessões plenárias (1092070);
- Justificativa da necessidade de manutenção da identificação genérica, apresentada pela SJD, por meio da Informação 4848/2021 - COREP (1099493);
- Análise de riscos apresentado em Relatório de Análise de Riscos emitido pelo Gabinete de Cibersegurança meio da Informação 3452/2022 - GAB-CIBERSEG (1210237).

Quanto às diretrizes elencadas pelo Gab-Ciberseg, foi evidenciado, por meio das respostas das Unidades que:

- As credenciais “estão restritas ao acesso apenas dos computadores do Plenário” e “possuem atribuição de mínimo privilégio, com acesso restrito aos três grupos essenciais para a utilização durante a Sessão Plenária”, conforme Informação 2269/2024 - SESOP (1520149), cumprindo as diretrizes “a” e “b” do Relatório de Análise de Riscos;
- Há indicação de descumprimento da diretriz “c”, referente ao item 4.4 do Anexo II (Acesso à Rede Corporativa) da Portaria TRE-SE 41/2020, pela ocorrência de “compartilhamento das credenciais, no caso de substituição”, ainda que “precedido das devidas orientações afetas aos cuidados cibernéticos”, conforme Informação 2114/2024 - COREP (1517279).
- Há indicação de descumprimento da diretriz “d”, visto que “o controle dos termos de responsabilidade (Anexo IX da Portaria TRE-SE 41/2020) e de histórico (período inicial e final), encontra-se em fase de implantação”, também conforme Informação 2114/2024 - COREP (1517279).

As evidências coletadas, apontam para uma possível desconformidade, não relacionada com a recomendação avaliada, identificada a partir das diretrizes constantes no Relatório de Análise de Riscos, ensejando na necessidade de novas diligências e avaliação posterior, emitida por meio de Nota de Auditoria (1547329).

2.1.5. Situação Final da Recomendação:

A partir das análises efetuadas, ficou evidenciado que a recomendação foi implementada pela STI.

2.2 Critérios de formação e período de troca de senha atendem às normas vigentes, evidenciando a implementação de recomendação.

Recomendação À STI: Implementar os critérios de cadastro de senhas vinculadas às contas de acesso à rede corporativa, conforme o disposto no art. 13 da Portaria TRE/SE 192/2018, bem como nas boas práticas da ISO 27002:2003 (itens 9.3.1 e 9.4.3) e do Manual de Boas Práticas em Segurança da Informação do TCU.

2.2.1. Instrumentos avaliados:

- Portaria TRE/SE 41/2020 que revogou a portaria 192/2018;
- ISO 27002:2013 (itens 9.3.1 e 9.4.3);
- Manual de Boas Práticas em Segurança da Informação do TCU (4a. Edição, 2012).

2.2.2. Avaliação:

Após a emissão do 1º Relatório de Monitoramento da Auditoria em Segurança da Informação, Relatório de Auditoria 10 (1089730), a COINF manifestou-se por meio da Informação 4768/2021 (1097501) quanto a implementação da seguinte ação: "Propor mudança na Portaria nº 41/2020, por meio do processo SEI nº 0018859-86.2021.6.25.8000 no tocante aos itens apontados."

Conforme Plano de Ação a SESOP (1096629) apresentou as seguintes sugestões para modificação do texto da Portaria TRE-SE 41/2020:

- O período de alteração das senhas (item 3.5.4, do Anexo II) de a cada 12 meses para “devem ser alteradas em intervalos regulares de, no máximo, 6 (seis) meses, conforme necessidade”.
- O critério de formação da senha (item 3.5.2, do Anexo II) alterado para “a senha deve conter pelo menos 3 dos 4 tipos de caracteres seguintes: números, letras, alternando-as entre maiúsculas e minúsculas, e caracteres especiais, como $@#&%.”

O Gabinete de Cibersegurança/STI preparou minuta com as sugestões apresentadas (Informação 3463/2022 – SEI 1210409 / Minuta Política de Controle Acesso Lógico SEI 1210413). As alterações foram publicadas no DJE 136/2022, de 03/08/22, pela Portaria TRE-SE 506/2022 (1213962). Os dispositivos alterados estão abaixo citados:

> 3.5 As senhas vinculadas às contas de acesso à rede corporativa deverão atender, obrigatoriamente, aos seguintes critérios:
>
> …
> 3.5.2 Devem conter pelo menos 3 dos 4 tipos de caracteres seguintes: números, letras maiúsculas, letras minúsculas e caracteres especiais, como $@#&%. Deve existir pelo menos uma unidade de cada um dos tipos de caracteres escolhidos. (Alterado pela Portaria TRE-SE 506/2022)
>
> …
> 3.5.4 Devem ser alteradas em intervalos regulares de, no máximo, 6 (seis) meses, conforme necessidade. (Alterado pela Portaria TRE-SE 506/2022)

Quanto às alterações realizadas na Portaria TRE-SE 41/2020, convém observar:

1. Alteração das senhas: intervalo regular de no máximo 6 (seis) meses, atendendo ao critério do item 9.4.3 da ISO 27002:2003, vigente à época.

   Quanto ao critério do manual Boas Práticas em Segurança da Informação (4ª ed. ano 2012), do TCU, a COINF (Informação 4540/2021 SESOP - SEI 1090700), entende que as boas práticas recomendadas pelo TCU devem se adequar “a realidade de órgão”, e que “adotar uma política de troca [de] senhas durante curtos períodos de tempo (entre 60 e 90 dias) leva o usuário a expor sua senha em local visível para terceiros, como por exemplo as anotações em papéis, podendo esta ser capturada por meio de engenharia social e, consequentemente, facilitando o seu uso por pessoas mal intencionadas”.

   A situação descrita pela COINF é reconhecida no manual citado, ressaltando “que a troca muito frequente de senhas também pode confundir o usuário, que poderá passar a escrever a senha em algum lugar visível ou escolher uma senha mais fácil, comprometendo, assim, a segurança” (item 2.5.8, pg. 22).

   Ademais, a versão mais recente da norma ISO 27002 (2022) é silente quanto ao período de troca de senha, apesar de citar diversas providências quanto autenticação e senhas.

2. Critério de formação: senha composta por 3 dos seguintes tipos de caracteres: números, letras maiúsculas, letras minúsculas e caracteres especiais, como $@#&%, com, pelo menos, uma unidade de cada um dos tipos de caracteres escolhidos.

   A COINF havia se manifestado (Informação 4540/2021 SESOP – SEI 1090700) quanto à necessidade de adequação à restrição técnica descrita na documentação da Microsoft, que “estabelece o uso de pelo menos 03 condições de complexidade para ter acesso aos serviços”. Sendo assim, a portaria adequou os critérios de complexidade de formação da senha a 3 fatores (tipos de caracteres), resultando na adequação à restrição técnica.

Para avaliação do novo critério de formação das senhas, fez-se necessário a realização de novos testes, para verificação da implementação dos critérios alterados. Os testes foram realizados em 28/05/2024, indicando o atendimento dos critérios estabelecidos na alteração da Portaria TRE-SE 41/2020.

2.2.3. Situação da Recomendação:

Em relação ao período de troca de senha, a alteração realizada na Portaria TRE-SE 41/2020 atende ao disposto na norma ISO 27002:2003. A atualização da norma ISO em 2022, não determina a necessidade de período de troca da senha, mas cita diversas providências quanto autenticação e senhas, que poderão ser objeto de futura avaliação.

Quanto ao novo critério de formação de senha, estabelecido na alteração da Portaria TRE-SE 41/2020, testes realizados em 28/05/2024 indicaram a implementação e cumprimento dos critérios definidos na norma.

Diante do exposto, conclui-se que a recomendação foi implementada.

III. BENEFÍCIOS EFETIVOS DAS RECOMENDAÇÕES

A implementação das recomendações resultou em:

a) Aperfeiçoamento e exercício dos procedimentos de justificativa, análise e tratamento de riscos associados à identificação genérica e de uso compartilhado para acesso aos recursos da rede;

b) Aperfeiçoanento da segurança em equipamentos utilizados com credenciais genéricas, pela definição e implementação de restrições de acesso a recursos e atribuição de mínimo privilégio;

c) Aprimoramento, adequação e atualização de normativos e procedimentos relacionados aos critérios de cadastro de senhas vinculadas às contas de acesso à rede corporativa.

IV. CONCLUSÃO

Diante das informações obtidas, a situação de implementação das recomendações é a seguinte:

Recomendação	**Grau de Implementação**
Adotar medidas para que a identificação genérica e o uso compartilhado dos computadores do plenário do Tribunal revistam-se dos aspectos formais prescritos no art. 12 da Portaria TRE/SE 192/2018 (Revogada pela Portaria TRE/SE 41/2020).	Implementada
Implementar os critérios de cadastro de senhas vinculadas às contas de acesso à rede corporativa, conforme o disposto no art. 13 da Portaria TRE/SE 192/2018 (Revogada pela Portaria TRE/SE 41/2020), bem como nas boas práticas da ISO 27002:2003 (itens 9.3.1 e 9.4.3) e do Manual de Boas Práticas em Segurança da Informação do TCU.	Implementada

Documento assinado eletronicamente por **ADAIL VILELA DE ALMEIDA**, **Coordenador(a)**, em 13/06/2024, às 09:42, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **IVANILDO ALVES DE MEDEIROS**, **Técnica(o) Judiciária(o)**, em 13/06/2024, às 09:44, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **LUIZ FERNANDO BRITO DE CARVALHO**, **Técnica(o) Judiciária(o)**, em 13/06/2024, às 09:45, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-se.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1544184** e o código CRC **BA85524C**.

0013197-49.2018.6.25.8000 1544184v1

Criado por 015166042100, versão 82 por 000628402194 em 13/06/2024 09:06:44.