TRIBUNAL REGIONAL ELEITORAL DE SERGIPE

CENAF, Lote 7, Variante 2 - Bairro Capucho - CEP 49081-000 - Aracaju - SE - http://www.tre-se.jus.br

Relatório de Auditoria 10/2021 - SEAUG

RELATÓRIO Monitoramento

INTERESSADO(S) Secretaria de Tecnologia da Informação e Comunicação.

SUMÁRIO

I. INTRODUÇÃO

1.1 Visão Geral do Objeto Monitorado

Trata-se do 1º Relatório de Monitoramento da Auditoria em Segurança da Informação, que teve como objetivos:

- Identificar o atendimento às diretrizes de segurança da informação contidas em normativos e referenciais de boas práticas;
- Identificar o estabelecimento e funcionamento, na estrutura da Instituição, dos papéis e responsabilidades em funções de segurança da informação;
- Avaliar controles relacionados ao acesso dos usuários às informações e aos recursos de processamento da informação.

A partir dos exames realizados, verificou-se a necessidade de adequação de alguns procedimentos, e, por isso, emitiram-se recomendações para a Secretaria de Tecnologia da Informação - STI.

1.2 Objetivo

O objetivo do Monitoramento consistiu em averiguar o atendimento das seguintes recomendações:

- Estabelecer procedimentos para que a Seção de Lotação e Gestão de Desempenho e os gestores de contratos informem o término do prazo de vigência do contrato, quando da solicitação da criação de credenciais de acesso de estagiários e prestadores de serviços, conforme o disposto no art. 10 da Portaria TRE/SE 192/2018;
- Revisar as configurações atuais das contas dos estagiários e prestadores de serviços a fim de adequá-las ao disposto no art. 10 da Portaria TRE/SE 192/2018;
- 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;
- 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;
- Fornecer subsídio que viabilize a análise crítica dos direitos de acesso dos usuários pelas unidades gestoras da solução, a intervalos regulares, em conformidade com o disposto nos arts. 8º, 15, 33 da Portaria TRE/SE 192/2018;
- Identificar os ativos da organização e definir as responsabilidades apropriadas para a proteção dos ativos, conforme o art. 7º da Resolução TSE 23.501/2016.

Destaca-se que os normativos do TRE/SE e TSE referenciados nas recomendações foram revogados e as normas atuais vigentes são a Portaria TRE/SE 41/2020 e a Resolução TSE 23.644/2021. As considerações sobre as mudanças nas legislações são relatadas nas análises do atendimento das recomendações.

As manifestações das unidades foram analisadas, verificando-se a adequação às normas e boas práticas citadas acima. Testes foram realizados para avaliação prática da adequação do sistema de cadastro de senhas.

Compuseram a Equipe responsável pelas constatações: Ivanildo Alves de Medeiros e Anna Carolina do Valle Conceição, a supervisão foi desempenhada por Adail Vilela de Almeida.

Não houve nenhuma limitação quanto aos exames realizados.

II. ANÁLISE DO ATENDIMENTO DAS RECOMENDAÇÕES

2.1 Recomendação

À STI:

Estabelecer procedimentos para que a Seção de Lotação e Gestão de Desempenho e os gestores de contratos informem o término do prazo de vigência do contrato, quando da

solicitação da criação de credenciais de acesso de estagiários e prestadores de serviços, conforme o disposto no art. 10 da Portaria TRE/SE 192/2018.

2.1.1 Situação que levou à proposição da recomendação

A ausência de cancelamento automático das contas de prestadores de serviços e estagiários, quando do encerramento do contrato, permitindo que estes permaneçam com acesso válido mesmo após desligamento, ocasionando vulnerabilidade nos sistemas.

2.1.2 Providências adotadas e comentário dos gestores

1ª Manifestação da STI (0573387 e 0623590)**:** A Secretaria de Tecnologia da Informação (STI) providenciará a adequação do procedimento, aos ditames da Portaria 192/2018, até dezembro de 2018, haja vista a necessidade de ajustes envolvendo a SGP. Além disso, toda a equipe da STI está envolvida nos preparativos para as eleições deste ano. Há um procedimento na SGP/SEGED para o desligamento do estagiário conforme anexo “Help desk solicitando desligamento estagiário.pdf”.

2.1.3 Evidências: Portaria TRE/SE 41/2020, em seu anexo II, item 3, 3.1.2, 3.1.3, 3.1.3.1, 3.6, 3.7.

2.1.4 Análise

A Portaria TRE/SE 41/2020, em seu anexo II, item 3, estabelece os procedimentos relativos ao acesso à rede corporativa, conforme transcrito abaixo:

3.1.2 Para estagiários – após a abertura de chamado na CSTI, através de ferramenta na intranet, pela Seção de Lotação e Gestão de Desempenho (SEGED), informando o nome completo, unidade de atuação, matrícula do estagiário, **vigência do contrato** e título eleitoral.

3.1.3 Para prestadores de serviço – após a abertura de chamado na CSTI, através de ferramenta na intranet, pelo gestor do contrato, informando o nome completo, unidade de atuação, número e **vigência do contrato**, nome da empresa contratada, matrícula na empresa contratada (ou outro documento legalmente válido) e título eleitoral.

3.1.3.1 Nas substituições eventuais, caberá ao responsável **informar o período para a configuração adequada da conta de acesso** do prestador de serviço.

3.6 As contas de estagiários e prestadores de serviço **serão configuradas para expirarem automaticamente, ao término do prazo de vigência do contrato**.

3.7 As unidades responsáveis por autorizar a criação de novas credencias deverão informar à CSTI, através de ferramenta na intranet, o **desligamento**, afastamento ou movimentação de lotação dos respectivos usuários, para que sejam tomadas providências de bloqueio e posterior eliminação da conta, quando necessário.

2.1.5 Conclusão

Os procedimentos estabelecidos atendem ao recomendado.

2.2 Recomendação

À STI:

Revisar as configurações atuais das contas dos estagiários e prestadores de serviços a fim de adequá-las ao disposto no art. 10 da Portaria TRE/SE 192/2018.

2.2.1 Situação que levou à proposição da recomendação

A ausência de cancelamento automático das contas de prestadores de serviços e estagiários, quando do encerramento do contrato, permitindo que estes permaneçam com acesso válido mesmo após desligamento, ocasionando vulnerabilidade nos sistemas.

2.2.2 Providências adotadas e comentário dos gestores

1ª Manifestação da STI (1046542)**:** A Seção de Lotação e Gestão de Desempenho (SEGED) solicitou, por meio do chamado n° Ticket#2020081010000133 (ENCERRAMENTO DE ESTÁGIO), o encerramento das contas de rede dos 46 estagiários que possuíam contratos ativos com o TRE de Sergipe, em virtude disso, desde o dia 14 de agosto de 2020, não há em nossa base de usuários do domínio (Active Directory), contas de estagiário ativas que possam evidenciar as informações solicitadas.

Em relação aos prestadores de serviços, elencamos alguns contratos dentre os diversos existentes no Tribunal, com o intuito de evidenciarmos (1046552) as informações solicitadas, são eles:

1. Contrato 01/2020 - MANSEG - MANUTENÇÃO E SERVIÇOS GERAIS LTDA - Vigência 3/2/2020 a 2/2/2022.

2. Contrato 03/2021 - SANTANA EMPREENDIMENTOS EIRELI - Vigência 16/05/2021 a 15/05/2023.

3. Contrato 11/2019 - GETI COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA - Vigência 6/12/2019 a 5/12/2022.

4. Contrato 11/2020 - CROSOFTEN TECNOLOGIA E INOVAÇÃO LTDA - Vigência 1/10/2020 a 30/09/2023.

2.2.3 Evidências: Portaria TRE/SE 41/2020, em seu anexo II, item 3.6. Dados do sistema de gerenciamento de senhas (1046552).

2.2.4 Análise

A Portaria TRE/SE 41/2020, em seu anexo II, item 3, estabelece os procedimentos relativos ao acesso à rede corporativa, conforme transcrito abaixo:

3.6 As contas de estagiários e prestadores de serviço serão configuradas para expirarem automaticamente, ao término do prazo de vigência do contrato.

A unidade auditada apresentou prints de tela (documento SEI 1046552), demonstrando os dados extraídos do sistema de gerenciamento de senhas, contendo número razoável de cadastros de prestadores de serviços, dos quais se observou que constam as especificações de data de encerramento do contrato.

Quanto aos estagiários, a unidade auditada, informou (documento SEI 1046542) que não existem contas ativas de estagiário, tendo em vista o encerramento dos contratos em agosto de 2020.

Verificou-se através dos documentos apresentados pela unidade auditada que foram realizadas as adequações no sistema, de forma que ocorra a expiração das contas no dia seguinte ao último dia de vigência do contrato.

2.2.5 Conclusão

As contas de prestadores de serviço estão configuradas de acordo com o recomendado e com o normativo vigente: Portaria TRE/SE 41/2020. Quanto as contas dos estagiários, não foi possível evidenciar a conformidade com o dispositivo, tendo em vista que não existem contas ativas.

2.3 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 (Revogada pela Portaria TRE/SE 41/2020).

2.3.1 Situação que levou à proposição da recomendação

A STI foi questionada se há casos de identificação genérica e de uso compartilhado para acesso aos recursos da rede e se em caso positivo, há justificativa e parecer da STI autorizando essa forma de acesso. Informou que o único caso de uso compartilhado de credenciais, para acesso a recursos da rede, ocorre nos computadores do plenário do Tribunal. No entanto, não há justificativa formalizada, nem parecer da STI acerca da possibilidade de aceitação dos riscos associados.
Ausência de parecer para uso compartilhado de acesso aos recursos da rede, contrariando o disposto no item 3.8 do anexo II, da Portaria TRE/SE 41/2020.

2.3.2 Providências adotadas e comentário dos gestores

1ª Manifestação da STI (1046542)**:** Os computadores utilizados pelos juízes membros desta corte, durante as sessões plenárias, ainda autenticam-se na rede corporativa do Tribunal Regional Eleitoral de Sergipe por meio de usuários genéricos, estes são restritos aos computadores do plenário e tem acesso individualizado, ou seja, cada um deles possui credencias particulares:

- plenario100 (Classe Advogado)
- plenario200 (Classe Juiz de Direito)
- plenario300 (Classe Juiz de Direito)
- plenario400 (Secretário da Sessão)
- plenario500 (Presidente da Sessão)
- plenario600 (Procurador Eleitoral)
- plenario700 (Vice-presidente da Sessão)
- plenario800 (Classe Juiz Federal)
- plenario900 (Classe Advogado)

Com o intuito de garantir um trabalho técnico proativo nas sessões, o procedimento de acesso aos computadores do local, conforme acordado entre a Secretária de Tecnologia da Informação e a Secretária Judiciária, está sendo executado da seguinte forma: 30 (trinta) minutos antes da abertura da sessão, um técnico da CSTI (Central de Serviços) liga os equipamentos (notebooks e impressoras) que serão utilizados, em seguida o juiz membro faz a autenticação com o usuário e senha referente a sua posição, voltando a disponibilizá-lo ao técnico plantonista que fará uma avaliação prévia dos principais recursos necessários ao bom andamento da sessão, podemos especificar alguns deles: Impressora ativa, Pidgin ativo, Leitor de PDF funcionando (Acrobat Reader), editor de texto funcionando (LibreOffice), browser de navegação funcionando (Firefox e Chrome), entre outras aplicações demandadas pelo membro.

A Portaria 41/2020 cita, em seu item 3.8, que não haverá identificação genérica e de uso compartilhado para acesso aos recursos da rede, excetuando-se os casos de necessidade, reproduzido a seguir.

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 criação desses usuários genéricos surgiu da necessidade de atenderemos aos membros de nossa corte de forma proativa, cabendo à equipe técnica aplicar restrições objetivas nestes usuários, mitigando os riscos envolvidos, entre as quais cita-se:

- Acesso restrito aos computadores do plenário, não possuindo privilégios na rede corporativa do Tribunal;

- Não mapeiam as unidades de trabalho e não possuem permissão para autenticar nos sistemas de informações disponíveis (Ipleno, PJe, SEI, Webmail, ELO, ODIN, entre outros), inclusive todos os acessos dos membros aos sistemas judiciais e administrativos são realizados por meio de suas credenciais pessoais, ou seja, título eleitoral e senha de acesso pessoal, similar a um segundo fator de autenticação nestes dispositivos.

2ª Manifestação da STI (1090700)**:** A COINF adotará o rito abaixo descrito:

1. Realização de consulta, via processo SEI 0018326-30.2021.6.25.8000, ao setor negocial sobre a possibilidade de retificação do acesso, ou seja, cada membro deverá acessar o computador com a sua identificação pessoal (título de eleitor).
2. Havendo anuência a proposta apresentada na referida consulta, o procedimento será arquivado sem a necessidade da emissão do parecer da STI, visto que fica evidenciado a perda do objeto.
3. Constatando a necessidade de ser manter o atual cenário, as motivações expostas serão submetidas à Seção de Segurança da Informação para que emita o parecer.
4. Ato contínuo, os autos serão submetidos ao Secretário de Tecnologia da Informação para conhecimento e providências que entender pertinentes.

2.3.3 Evidências: Portaria TRE/SE 41/2020, item 3.8 do anexo II. Manifestação da STI (1090700).

2.3.4 Análise

A unidade auditada apresentou prints de tela (documento SEI 1046649), demonstrando as configurações extraídas do sistema de gerenciamento de senhas, contendo a comprovação da criação das contas individuais para todos os membros da corte.

A SEJUE apresentou tabela (documento SEI 1039922) contendo a relação dos membros titulares e substitutos e seus respectivos períodos de atuação na corte. Os prints de tela (documento SEI 1046649) comprovam a data de expiração da conta, um dia após a data final do biênio.

Outro aspecto apresentado pela STI, na Informação 2969 (1046542), é a declaração de que há utilização de usuários genéricos, durante as sessões plenárias, tendo sido aplicadas restrições.

Verificou-se que permanece a identificação genérica e não foi apresentado o parecer da STI acerca da possibilidade de aceitação dos riscos associados. As dificuldades expostas pela unidade, justificando o uso de identificação genérica, não a isentam da necessária apresentação do parecer técnico, tendo em vista os riscos do uso compartilhado do acesso aos recursos da rede.

Em resposta à CI (1089176), a STI informa no documento SEI (1090700) a necessidade de manutenção da identificação genérica e condiciona a apresentação de parecer, até que haja a resposta à consulta direcionada ao setor negocial.

2.3.5 Conclusão

A auditada aguarda resultado da consulta realizada através do processo SEI 0018326-30.2021.6.25.8000. Após, reavaliará necessidade de apresentação do parecer. Como permanece a desconformidade em relação ao disposto na Portaria TRE/SE 41/2020, a situação atual da recomendação é não implementada. As informações da STI não têm os requisitos de um plano de ação, por exemplo, não têm prazo, devendo ser comunicada à presidência a necessidade da unidade apresentar plano de ação, conforme modelo, e que as recomendações a serem implementadas serão objeto de futuro monitoramento.

2.4 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.

2.4.1 Situação que levou à proposição da recomendação

Após testes realizados, nos dias 13 e 25/09/2018, para verificar o atendimento aos critérios do art. 13 da Portaria 192/2016 e ISO 27002:2013 itens 9.3.1, 9.4.2 e 9.4.3, relacionados ao cadastro de senhas vinculadas às contas de acesso à rede corporativa, constatou-se que no SisDesktop o próprio usuário pode modificar sua senha, sem visualização da senha digitada na tela e com o procedimento de confirmação de alteração, além disso o usuário é obrigado a alterar a senha temporária fornecida pela TI para acessar o Sisdesktop, no entanto, permitiu-se as seguintes inconsistências:

1. Cadastrar senha com apenas 9 dígitos;

2. Cadastrar senha apenas com números e letras;

3. Cadastrar a mesma senha utilizada anteriormente;

4. Acessar o sistema após 11 tentativas seguidas errôneas de logon.

Além, disso, mediante entrevista com 6 servidores lotados na COCIN (atual COAUD), COPEG e ASJUR, verificou-se que é possível acessar o SisDesktop com a mesma senha por mais de 90 dias.

2.4.2 Providências adotadas e comentário dos gestores

1ª Manifestação da STI (0623590)**:** Nova política de senha implementada. Envio de mensagem, com cartilha em anexo, orientando os usuários.

2ª Manifestação da STI (1090700)**:** A COINF é solidária com as boas práticas recomendadas pelo TCU, mas entende que estas devem ser adequar a realidade de órgão, visto que, segundo nossa experiência, considerando o atual nível de complexidade das senhas, adotar uma política de troca 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.

Diante do exposto acima, apresentar-se-ão sugestões de melhoria em nossa portaria objetivando acolher o posicionamento da política de troca de senha adotada pelo Egrégio Tribunal Superior Eleitoral, disciplinada por meio da Portaria nº 454, de 13 de julho de 2021 (SEI 1092245), que estabelece no artigo 25 que as senhas devem ser modificadas em intervalos regulares de, no máximo, 6 (seis) meses.

Cabe informar que este ponto também será objeto de sugestão para adequar-se a política impositiva do sistema de gerenciamento de senha da ferramenta (SEI 1092243) que estabelece o uso de pelo menos 03 das condições de complexidade para ter acesso aos serviços, conforme informação extraída do link da Microsoft (A senha deve atender aos requisitos de complexidade (Windows 10) - Windows security | Microsoft Docs). Em outras palavras, devemos nos adequar à restrição técnica imposta pelo fabricante.

Por fim, informa-se que manteremos, em nosso domínio de rede, o período de alteração das senhas a cada 12 meses, previsto na Portaria TRE/SE 41/2020, e a política impositiva do sistema de gerenciamento de senha até conclusão da revisão necessária da atual Política de Controle de Acesso Lógico, pelo Comitê de Segurança da Informação (CSI) e, posteriormente, sancionada pelo Presidente. Após tal revisão, as alterações aprovadas serão efetivadas pela equipe técnica imediatamente.

2.4.3 Evidências: Portaria TRE/SE 41/2020 que revogou a portaria 192/2018; Manifestação da STI (1090700) e Arquivos de vídeos referentes aos testes de cadastro de senhas, salvos no diretório da SEAUG que estão disponíveis para verificação.

2.4.4 Análise

A Portaria TRE/SE 41/2020, em seu anexo II, estabelece os seguintes procedimentos, conforme transcrito abaixo:

3.5 As senhas vinculadas às contas de acesso à rede corporativa deverão atender, obrigatoriamente, aos seguintes critérios:

3.5.1 Devem ter o tamanho mínimo de 10 (dez) caracteres.

Este dispositivo está em conformidade com o manual de boas práticas do TCU, que recomenda evitar senhas com menos de 6 caracteres.

3.5.2 Devem ser formados pela combinação de letras minúsculas e maiúsculas, números e símbolos.

Este dispositivo está em conformidade com o manual de boas práticas do TCU, que indica como boas senhas, aquelas que incluem, na composição, letras (maiúsculas e minúsculas), números e símbolos embaralhados; Em conformidade, também, com a ISO 27002:2013, que recomenda que o sistema de gerenciamento de senhas obrigue a escolha de senhas de qualidade.

3.5.3 Não podem ser iguais à última senha utilizada.

Análise: Este dispositivo está em conformidade com a ISO 27002:2013, que recomenda que o sistema de gerenciamento de senhas mantenha um registro das senhas anteriores utilizadas e bloqueie a reutilização; Em conformidade com o manual de boas práticas do TCU, que recomenda evitar reutilizar as mesmas senhas.

3.5.4 Devem ser alteradas a cada 12 (doze) meses.

Análise: Este dispositivo está em conformidade com a ISO 27002:2013, que recomenda que o sistema de gerenciamento de senhas force as mudanças de senha a intervalos regulares, conforme necessário; e em desconformidade com o manual de boas práticas do TCU, que considera como uma boa prática, a troca da senha a cada 60/90 dias.

A ISO 27002:2013 trouxe algumas diretrizes para implementação, quanto ao uso da informação de autenticação secreta e quanto ao sistema de gerenciamento de senhas, conforme transcrito abaixo:

9.3.1. a) manter a confidencialidade da informação de autenticação secreta, garantindo que ela não é divulgada para quaisquer outras partes, incluindo autoridades e lideranças;

b) evitar manter anotadas a informação de autenticação secreta (por exemplo, papel, arquivos ou dispositivos móveis), a menos que elas possam ser armazenadas de forma segura e o método de armazenamento esteja aprovado (por exemplo, sistema de gerenciamento de senha;

c) alterar a informação de autenticação secreta, sempre que existir qualquer indicação de possível comprometimento do sistema ou da própria senha;

d) Quando as senhas são usadas como informação de autenticação secreta, selecione senhas de qualidade com um tamanho mínimo que sejam:

1) fáceis de lembrar;

2) não baseadas em nada que alguém facilmente possa adivinhar ou obter usando informações relativas à pessoa, por exemplo, nomes, números de telefone e datas de aniversário;

3) não vulneráveis a ataque de dicionário (por exemplo, não consistir em palavras inclusas no dicionário);

4) isentas de caracteres idênticos consecutivos, todos numéricos ou todos alfabéticos sucessivos;

5) caso a senha seja temporária, ela deve ser mudada no primeiro acesso (*log-on*).

e) não compartilhar a informação de autenticação secreta de usuários individuais;

f) garantir adequada proteção de senhas quando as senhas são usadas como informação de autenticação secreta em procedimentos automáticos de acesso (*log-on)* e são armazenadas;

g) não utilizar a mesma informação de autenticação secreta para uso com finalidades profissionais e pessoais.

9.4.3. Sistema de gerenciamento de senhas:

Convém que o sistema de gerenciamento de senha:

a) obrigue o uso individual de ID de usuário e senha para manter responsabilidades;

b) permita que os usuários selecionem e modifiquem suas próprias senhas, incluindo um procedimento de confirmação para evitar erros;

c) obrigue a escolha de senhas de qualidade;

d) obrigue os usuários a mudarem as suas senhas temporárias no primeiro acesso ao sistema;

e) force as mudanças de senha a intervalos regulares, conforme necessário;

f) mantenha um registro das senhas anteriores utilizadas e bloqueie a reutilização;

g) não mostre as senhas na tela quando forem digitadas;

h) armazene os arquivos de senha separadamente dos dados do sistema da aplicação;

i) armazene e transmita as senhas de forma protegida.

Segundo o Manual de Boas Práticas em Segurança da Informação do TCU (Páginas 20-21), os usuários devem evitar senhas compostas de elementos facilmente identificáveis por possíveis invasores, como por exemplo:

- nome do usuário;
- identificador do usuário (ID), mesmo que os caracteres estejam embaralhados;
- nome de membros de sua família ou de amigos íntimos;
- nomes de pessoas ou lugares em geral;
- nome do sistema operacional ou da máquina que está sendo utilizada;
- nomes próprios;
- datas;
- números de telefone, de cartão de crédito, de carteira de identidade ou de outros documentos pessoais;
- placas ou marcas de carro;
- palavras que constam de dicionários em qualquer idioma;
- letras ou números repetidos;
- letras seguidas do teclado do computador (ASDFG, YUIOP);
- objetos ou locais que podem ser vistos a partir da mesa do usuário (nome de um livro na estante, nome de uma loja vista pela janela);
- qualquer senha com menos de 6 caracteres.

Ainda segundo o Manual de Boas Práticas em Segurança da Informação do TCU (Página 20), os usuários devem ser orientados a:

- manter a confidencialidade das senhas;
- não compartilhar senhas;
- evitar registrar as senhas em papel;
- selecionar senhas de boa qualidade, evitando o uso de senhas muito curtas ou muito longas, que os obriguem a escrevê-las em um pedaço de papel para não serem esquecidas (recomenda-se tamanho entre seis e oito caracteres);

- alterar a senha sempre que existir qualquer indicação de possível comprometimento do sistema ou da própria senha;
- alterar a senha em intervalos regulares ou com base no número de acessos (senhas para usuários privilegiados devem ser alteradas com maior frequência que senhas normais);
- evitar reutilizar as mesmas senhas;
- alterar senhas temporárias no primeiro acesso ao sistema;
- não incluir senhas em processos automáticos de acesso ao sistema (por exemplo, armazenadas em macros).

O Manual de Boas Práticas em Segurança da Informação do TCU indica como escolher boas senhas: Geralmente são consideradas boas senhas aquelas que incluem, na composição, letras (maiúsculas e minúsculas), números e símbolos embaralhados, totalizando mais de seis caracteres. Porém, para ser boa mesmo, a senha tem que ser difícil de ser adivinhada por outra pessoa, mas de fácil memorização, para que não seja necessário anotá-la em algum lugar. Também é conveniente escolher senhas que possam ser digitadas rapidamente, dificultando que outras pessoas, a certa distância ou por cima dos ombros, possam identificar a sequência de caracteres. Um método bastante difundido hoje em dia é selecionar uma frase significativa para o usuário e utilizar os primeiros caracteres de cada palavra que a compõe, inserindo símbolos entre eles. É também recomendável não utilizar a mesma senha para vários sistemas. Se um deles não for devidamente protegido, a senha poderá ser descoberta e utilizada nos sistemas que, a priori, estariam seguros. Se você realmente não conseguir memorizar sua senha e tiver que escrevê-la em algum pedaço de papel, tenha pelo menos o cuidado de não identificá-la como sendo uma senha. Não pregue esse pedaço de papel no próprio computador, não guarde a senha junto com a sua identificação de usuário e nunca a envie por e-mail ou armazene em arquivos do computador. Página 21

O sistema de controle de senhas deve ser configurado para proteger as senhas armazenadas contra uso não autorizado, sem apresentá-las na tela do computador, mantendo-as em arquivos criptografados e estipulando datas de expiração (normalmente se recomenda a troca de senhas após 60 ou 90 dias). Página 22

Foram realizados testes em 1º e 4 de outubro de 2021, os quais demonstraram que foi possível o cadastramento de senha, contrariando o disposto no item 3.5.2 do anexo II da portaria TRE/SE nº 41/2020:

Teste 9 - A senha composta por 10 (dez) caracteres e pela combinação de letras minúsculas, maiúsculas e números foi alterada, apesar de não conter símbolo;

Teste 10 - A senha composta por 10 (dez) caracteres e pela combinação de letras minúsculas, maiúsculas e símbolos foi alterada, apesar de não conter número;

Teste 12 - A senha composta por 10 (dez) caracteres e pela combinação de letras minúsculas, números e símbolos foi alterada, apesar de não conter letras maiúsculas;

Teste 13 - A senha composta por 10 (dez) caracteres e pela combinação de letras maiúsculas, números e símbolos foi alterada, apesar de não conter letra minúscula.

Após solicitação de manifestação (1089176), a STI (1090700) faz ponderações quanto ao cadastro de senhas e intervalo de troca, propondo a revisão da Portaria 41/2020 para adequação à Portaria TSE 454/2021 que prevê que as trocas de senhas ocorram a cada 6 meses, bem como, a adequação da portaria à política impositiva do sistema de gerenciamento de senha da Microsoft.

2.4.5 Conclusão

A auditada manifesta que a revisão da Portaria TRE/SE 41/2020 disporá quanto ao intervalo de troca de senha, bem como, quanto ao uso de, no mínimo, 3 das condições de complexidade. Como as medidas propostas de ajustes nos critérios de cadastro de senhas não foram efetivadas, a situação atual da recomendação é não implementada. As informações da STI não têm os requisitos de um plano de ação, por exemplo, não têm prazo, devendo ser comunicada à presidência a necessidade da unidade apresentar plano de ação, conforme modelo, e que as recomendações a serem implementadas serão objeto de futuro monitoramento.

2.5 Recomendação

À STI:

Fornecer subsídio que viabilize a análise crítica dos direitos de acesso dos usuários pelas unidades gestoras da solução, a intervalos regulares, em conformidade com o disposto nos arts. 8º, 15, 33 da Portaria TRE/SE 192/2018 (Revogada pela Portaria TRE/SE 41/2020).

2.5.1 Situação que levou à proposição da recomendação

A constatação de que os direitos de acesso dos usuários são analisados criticamente, permitindo que servidores, prestadores de serviços ou estagiários permaneçam com acesso válido mesmo após desligamento, ocasionando vulnerabilidade nos sistemas.

2.5.2 Providências adotadas e comentário dos gestores

1ª Manifestação da STI (0623590)**:** Os ativos da informação foram identificados por secretaria. Serão enviados formulários solicitando informações sobre os ativos (processo de negócio relacionado, vulnerabilidade, criticidade, etc).

2.5.3 Evidências: Portaria TRE/SE 41/2020, em seu anexo V, itens 4.6, 3.1, 3.2, 3.3, 3.3.1, 3.4, 3.5, 3.6 e 3.7.

2.5.4 Análise

A Portaria TRE/SE 41/2020, em seu anexo V, estabelece os procedimentos relativos ao acesso aos sistemas de informação do Tribunal, conforme transcrito abaixo:

4.6 Os direitos de acesso dos usuários deverão ser revisados, em intervalos regulares, pela unidade gestora da solução, sobretudo quando ocorrer mudança de função do servidor, alteração de lotação ou desligamento.

3.1 Na hipótese de o Sistema de Informação possuir módulo específico para a manutenção e criação de contas, habilitado para uso do Gestor do Sistema, a responsabilidade pela criação e manutenção de contas é de exclusiva responsabilidade deste. Portanto, o Gestor de Sistema de Informação deverá zelar pela base de usuários de sistema de forma que somente pessoas autorizadas tenham acesso ao sistema.

3.2 Quando não houver módulo específico para uso do Gestor do Sistema de Informação, este deverá realizar chamado à CSTI, através da ferramenta na intranet, fornecendo todos os dados necessários para a realização do cadastro e para a alteração ou exclusão de contas no sistema.

3.3 É responsabilidade do Gestor do Sistema de Informação definir o perfil, ou perfis, de acesso ao sistema em que cada usuário deverá ser incluído, bem como determinar as mudanças de perfil que se fizerem necessárias.

3.3.1 O perfil de acesso aos sistemas de informação deve estar de acordo com a política de classificação das informações do Tribunal.

3.4 A CSTI somente atenderá solicitações de criação e manutenção de contas de acesso a sistemas de informação que sejam feitas pelos Gestores de Sistema de Informação ou por servidores por eles autorizados e designados formalmente para realizar esse tipo de solicitação.

3.5 Em caso de acesso temporário, o Gestor de Sistema de Informação poderá indicar data para a expiração automática da autorização de acesso concedida. Não o fazendo, é responsabilidade dele solicitar a revogação da autorização ao término do tempo previsto para a utilização do sistema pelo usuário temporário.

3.6 O Gestor do Sistema de Informação ou servidor designado para controlar os acessos ao Sistema de Informação ficará responsável por providenciar a assinatura pelo usuário de Termo de Responsabilidade, anexo VIII, atestando estar ciente dos direitos, responsabilidades e possíveis sanções pelo uso indevido da conta do sistema.

3.7 É responsabilidade do Gestor do Sistema de Informação solicitar o cancelamento da conta de acesso ao sistema ou a alteração de perfil quando do desligamento, mudança de lotação/atribuição ou afastamento do agente público.

A Portaria 41/2020 forneceu os subsídios necessários para a análise dos direitos de acesso.

2.5.5 Conclusão

A Portaria TRE/SE 41/2020 viabiliza a análise crítica dos direitos de acesso pelas unidades gestoras, atendendo à recomendação.

2.6 Recomendação

À STI:

Identificar os ativos da organização e definir as responsabilidades apropriadas para a proteção dos ativos, conforme o art. 7º da Resolução TSE 23.501/2016 (Revogada pela Resolução 23.644/2021).

2.6.1 Situação que levou à proposição da recomendação

A ausência de levantamento dos ativos de informação, dificultando o processo de atendimento de solicitações de concessão, alteração ou remoção de acesso de servidores aos sistemas, bem como de verificação das responsabilidades das unidades solicitantes das autorizações de acesso.

2.6.2 Providências adotadas e comentário dos gestores

1ª Manifestação da STI (0623590)**:** Os ativos da informação foram identificados por secretaria. Serão enviados formulários solicitando informações sobre os ativos (processo de negócio relacionado, vulnerabilidade, criticidade, etc). Ressaltamos que as informações possibilitarão a criação do inventário dos ativos da informação, base para análise e identificação oficial dos responsáveis.

2.6.3 Evidências: Artigos 6º, inciso III, art. 8º, inciso VI e art. 9º, inciso II, alínea a, da Resolução TSE 23.644/2021; art. 4º da Portaria TRE/SE 769/2019.

2.6.4 Análise

A Resolução TSE 23.501/2016 foi revogada, porém o seu art. 7º considerado na elaboração da recomendação se coaduna com o art. 6º, inciso III, art. 8º, inciso VI e art. 9º, inciso II, alínea a da Resolução TSE 23.644/2021.

Art. 6º São objetivos da PSI da Justiça Eleitoral:

III - definir as ações necessárias para evitar ou mitigar os efeitos de atos acidentais ou intencionais, internos ou externos, de destruição, modificação, apropriação ou divulgação indevida de informações, de modo a preservar os ativos de informação e a imagem da instituição;

Art. 8º Os destinatários desta PSI, relacionados no caput do art. 7º, são corresponsáveis pela segurança da informação, de acordo com os preceitos estabelecidos nesta Resolução, e têm como deveres:

VI - utilizar os ativos sob sua responsabilidade de forma segura, em observância ao disposto nesta PSI e em eventuais normativos a ela subordinados.

Art. 9º A estrutura normativa referente à Segurança da Informação será estabelecida e organizada conforme definido a seguir:

II - Nível Tático: Normas Complementares sobre Segurança da Informação, que contemplam obrigações a serem seguidas de acordo com as diretrizes estabelecidas nesta PSI, a serem editadas por todos os tribunais que compõem a Justiça Eleitoral, e devem abarcar, no mínimo, os seguintes temas:

a. Gestão de Ativos;

A Portaria TRE/SE 769/2019, lista os responsáveis pelos ativos de informação do Tribunal Regional Eleitoral de Sergipe em seu anexo I.

2.6.5 Conclusão

A Portaria TRE/SE 769/2019, em seu anexo I, identifica os ativos de informação e as unidades responsáveis por cada um, conforme recomendação.

III. BENEFÍCIOS EFETIVOS DAS RECOMENDAÇÕES

A implementação das recomendações resultou em:

a) Aperfeiçoamento dos controles de acesso aos recursos de TI;

b) Identificação das unidades responsáveis pelos ativos de TI.

IV. CONCLUSÃO

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

Recomendação

Estabelecer procedimentos para que a Seção de Lotação e Gestão de Desempenho e os gestores de contratos informem o término do prazo de vigência do contrato, quando da solicitação da criação de credenciais de acesso de estagiários e prestadores de serviços, conforme o disposto no art. 10 da Portaria TRE/SE 192/2018 (Revogada pela Portaria TRE/SE 41/2020).

Grau de Implementação

Implementada

Recomendação

Revisar as configurações atuais das contas dos estagiários e prestadores de serviços a fim de adequá-las ao disposto no art. 10 da Portaria TRE/SE 192/2018 (Revogada pela Portaria TRE/SE 41/2020).

Grau de Implementação

Implementada

Recomendação

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).

Grau de Implementação

Não implementada

Recomendação

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.

Grau de Implementação

Não implementada

Recomendação

Fornecer subsídio que viabilize a análise crítica dos direitos de acesso dos usuários pelas unidades gestoras da solução, a intervalos regulares, em conformidade com o disposto nos arts. 8º, 15, 33 da Portaria TRE/SE 192/2018 (Revogada pela Portaria TRE/SE 41/2020).

Grau de Implementação

Implementada

Recomendação

Identificar os ativos da organização e definir as responsabilidades apropriadas para a proteção dos ativos, conforme o art. 7º da Resolução TSE 23.501/2016 (Revogada pela Resolução 23.644/2021).

Grau de Implementação

Implementada

Ressalta-se que haverá futuros monitoramentos para averiguação das recomendações ora não implementadas (itens 2.3 a 2.4.5 deste relatório), bem como segue modelo de plano de ação (1094800) para essas recomendações, a ser preenchido pela unidade auditada.

RETORNAR AO SUMÁRIO

Documento assinado eletronicamente por **ADAIL VILELA DE ALMEIDA**, **Coordenadora/Coordenador**, em 19/10/2021, às 09:29, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **IVANILDO ALVES DE MEDEIROS**, **Chefe de Seção**, em 19/10/2021, às 09:31, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **ANNA CAROLINA DO VALLE CONCEIÇÃO**, **Técnico Judiciário**, em 19/10/2021, às 09:32, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://apps.tre-se.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1089730** e o código CRC **0F3A192C**.