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

RELATÓRIO 2/2019 - SEAUG

RELATÓRIO DE AUDITORIA - TRE/SE

PREÂMBULO

Processo: 0013197-49.2018.6.25.8000

Objetivo: Auditar a Gestão da Segurança da Informação e o Controle de Acessos aos Ativos de Tecnologia da Informação.

Ato de designação: Comunicação Interna 438 (0566897).

Período abrangido pela auditoria: 26 de junho de 2018 a 21 de fevereiro de 2019

Período(s) de Realização: Planejamento (26/06/18 - 10/08/18), Execução (11/08/18 - 15/10/18) e Relatórios (16/10/18 - 21/02/19).

Unidade(s) Auditada(s): Secretaria de Tecnologia da Informação.

RESUMO

A presente auditoria em Segurança da Informação teve como objeto verificar a conformidade do ambiente informatizado com as normas emanadas pelos TSE e TRE/SE, a exemplo, respectivamente, das Resoluções 23.501/2016 e 180/2013, entre outras, bem como com os padrões internacionalmente aceitos (ABNT NBR ISO/TEC 27.002:2013). Os objetivos específicos foram definidos na forma de Questões de Auditoria, conforme consta no Programa de Auditoria 5 (0548087). Exames de documentos, visitas *in loco*, entrevista através de questionário e correlação das informações obtidas permitiram constatar falhas tanto na permissão como no controle do acesso aos ativos de tecnologia da informação. Constatou-se a ausência de cancelamento automático de acesso à rede para as contas de estagiários e prestadores de serviços, ausência de parecer para o uso compartilhado de acesso aos recursos da rede nos computadores do plenário do Tribunal, fragilidade na qualidade das senhas e no acesso à rede corporativa e ausência de revisão em intervalos regulares dos direitos de acesso. Verificou-se, ainda, que as regras existentes para a concessão do direito de acesso aos ativos de tecnologia da informação estão incompletas. Foram expedidas recomendações para o fortalecimento dos mecanismos de controle, a fim de evitar a ocorrência de falhas da mesma natureza. Observou-se que a Administração vem envidando esforços para o implemento das recomendações, conforme Plano de Ação apresentado.

SUMÁRIO

I. INTRODUÇÃO

Visando intensificar as avaliações na área de Tecnologia da Informação e Comunicação, face às demandas do CNJ em Auditoria Coordenada e no Levantamento de Governança, Gestão e infraestrutura de TIC - iGovTIC -JUD, decidiu-se durante o Exercício 2018 efetuar exames de auditoria, também, na Gestão da Segurança da Informação.

Compuseram a equipe de auditoria do Tribunal Regional Eleitoral de Sergipe - TRE/SE os servidores Ana Maria Rabelo de Carvalho Dantas, Ivanildo Alves de Medeiros, Jurene Barreto Santos e Wilson Fernandes de Souza Filho.

Os principais achados encontrados e as respectivas recomendações emitidas por esta Unidade foram consubstanciados no Relatório de Achados (0588327).

As Unidades Auditadas se manifestaram quanto ao Relatório de Achados e suas respostas foram consideradas e incluídas neste Relatório Conclusivo de Auditoria.

Todos os exames realizados se pautaram em procedimentos e técnicas de auditoria aplicáveis à Administração Pública e nenhuma restrição foi imposta quanto ao método ou à extensão dos trabalhos realizados.

II. VISÃO GERAL DO OBJETO AUDITADO

A Segurança da Informação visa garantir a integridade, confidencialidade, autenticidade e disponibilidade das informações processadas pela Instituição. A integridade, a confidencialidade e a autenticidade de informações estão intimamente relacionadas aos controles de acesso.

O Sistema de Gestão de Segurança da Informação (SGSI) compreende políticas, procedimentos, diretrizes, assim como os recursos e as atividades associadas, gerenciados coletivamente pela organização, com o propósito de proteger seus ativos de informação.

Ativo de Informação compreende a informação (mensagens, textos, dados de um sistema, idéias, vídeos, etc.) e tudo aquilo que lhe dá suporte ou dela faz uso (tecnologias, pessoas, processos, ambientes, etc.).

III. OBJETIVO DA AUDITORIA

Avaliar se o TRE/SE considera, na gestão da segurança da informação e no controle de acessos às informações e aos recursos de processamento da informação, os preceitos dos normativos superiores e os padrões internacionalmente aceitos, como a ISO 27002:2013 - Código de Prática para Controles de Segurança da Informação, o Manual de Boas Práticas em Segurança da Informação do TCU, os Acórdãos do TCU e a Resolução do TSE nº 23.501/2016, a qual instituiu a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral.

IV. ESCOPO

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.

V. CRITÉRIOS

Os critérios utilizados como parâmetros para fundamentar as avaliações apresentadas neste trabalho foram os preceitos normativos, os padrões internacionalmente aceitos e os estudos técnicos que regulamentam a matéria, a seguir exemplificados: Resolução TSE nº 23.501/2016[1], Resolução TRE/SE nº 180/2013[2], ABNT NBR ISO/TEC 27.002:2013[3], COBIT 5.0[4], Manual do TCU – Boas Práticas de Segurança da Informação[5], Portaria TRE/SE 1018/2016 - Plano Estratégico de Segurança da Informação (PESI) 2016-2020[6], Resolução TRE/SE nº 116/2017[7] e Portaria TRE/SE 192/2018[8].

---

1 Institui a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral.
2 Adota, no âmbito do Tribunal Regional Eleitoral de Sergipe, as diretrizes da Política de Segurança da Informação da Justiça Eleitoral, estabelecidas pela Resolução TSE n° 22.780, de 24 de abril de 2008 e dispõe sobre a instituição de Programa de Gestão de Segurança da Informação - PGSI.
3 Estabelece código de melhores práticas para apoiar a implantação do Sistema de Gestão de Segurança da Informação (SGSI) nas organizações.
4 Framework de boas práticas criado pela ISACA (Information Systems Audit and Control Association) para a governança de tecnologia de informação (TI).
5 Apresenta as boas práticas em segurança da informação, a qualquer pessoa que interaja de alguma forma com ambientes informatizados, desde profissionais de TI envolvidos com segurança de informações até auditores, usuários e dirigentes preocupados em proteger o patrimônio, os investimentos e os negócios da instituição, em especial, os gestores da Administração Pública Federal.
6 Define as diretrizes, objetivos e metas de segurança da informação, que nortearão a alocação de recursos, a priorização e execução de atividades, a aprovação de políticas, a definição e aceitação de riscos, tendo em vista a garantia da confidencialidade, integridade e disponibilidade das informações coletadas, manuseadas, armazenadas, transportadas e descartadas pelos processos de negócio.
7 Regulamento Interno da Secretaria do Tribunal.
8 Institui a política de controle de acesso às informações e aos recursos de processamento da informação, no âmbito do Tribunal Regional Eleitoral de Sergipe (TRE-SE).

VI. METODOLOGIA

De início, foi elaborado o Levantamento de Informações (0547522) no qual consta, em linhas gerais, levantamento de dados, informações necessárias para conhecer o objeto da auditoria e sua complexidade, legislação aplicável, conhecimento da estrutura da unidade auditada, cronograma com as etapas da auditoria. A partir daí, foram delineados os procedimento para execução dos trabalhos de auditoria, através da Matriz de Planejamento (0566482), direcionando-os por meio de Questões de Auditoria, técnica que consiste na determinação do direcionamento dos trabalhos de auditoria, das metodologias e testes a adotar e dos resultados que se pretende atingir, estabelecendo com clareza o foco de investigação, as dimensões e os limites que deverão ser observados durante a execução dos trabalhos pela equipe de auditoria.

Por conseguinte, definido a extensão dos exames, técnicas e a natureza dos trabalhos a serem executados, solicitou-se às unidades auditadas por meio do Programa de Auditoria 5 (0548087) documentos e o preenchimento do Questionário (0566449). As respostas às solicitações constam dos documentos SEI 0573357, 0573403, 0573387, 0573371, 0571148, 0571151, 0573109, 0573107, 0571188, 0571189 e 0573108. Após os exames desses documentos SEI, visitas *in loco* foram realizadas para verificar as medidas de controle e de fiscalização adotadas pela STI, bem como para esclarecimentos de tópicos específicos relacionados à segurança da informação. Também nesta fase, foram identificados achados de auditoria, para os quais houve recomendações documentadas no Relatório 1 (0588327). Por fim, em virtude das recomendações, foi apresentado Plano de Trabalho STI (0623590).

VII. ACHADOS DE AUDITORIA

Os achados de auditoria representam o resultado da aplicação dos testes de auditoria previstos no Programa de Auditoria 5(0548087).

Conforme o Tribunal de Contas da União: "Achado é a discrepância entre a situação existente e o critério. Achados são situações verificadas pelo auditor durante o trabalho de campo que serão usadas para responder às questões de auditoria. O achado contém os seguintes atributos: critério (o que deveria ser), condição (o que é), causa (razão do desvio com relação ao critério) e efeito (consequência da situação encontrada). Quando o critério é comparado com a situação existente, surge o achado de auditoria. (ISSAI 3000/4.3, 2004)" - Manual de Auditoria Operacional do TCU, pág. 30.

Avaliamos, a seguir, os principais achados:

Achado 1 - Ausência de cancelamento automático de acesso.

Situação encontrada: A STI foi questionada se as contas de estagiários e prestadores de serviços são configuradas para expirarem automaticamente ao término do prazo de vigência do contrato e respondeu negativamente. Informou que as contas dos prestadores de serviços são configuradas para expirarem 1 ano após a sua criação e as contas dos estagiários são criadas sem prazo de expiração automática. Quanto a essas últimas contas, a desativação ocorre mediante solicitação da Secretaria de Gestão de Pessoas (SGP), registrada no sistema Helpdesk/Central de Serviços de TI.

Critério(s) de Auditoria:

- Portaria TRE/SE 192/2018:

> Art. 10 As contas de estagiários e prestadores de serviço serão configuradas para expirarem automaticamente, ao término do prazo de vigência do contrato.

- ISO 27.002:2013:

> 9.2.1 Registro e cancelamento de usuário
>
> (…)
>
> b) a imediata remoção ou desabilitação do ID de usuário que tenha deixado a organização (ver 9.2.5);

Evidência(s):

- Questionário (0573387).

Causa(s): Inobservância de determinações normativas.

Consequência(s) do Achado: Permitir que prestadores de serviços ou estagiários permaneçam com acesso válido mesmo após desligamento, ocasionando vulnerabilidade nos sistemas.

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.

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.

Resposta(s) do(s) Auditado(s):

STI:

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”.

Análise da Equipe de Auditoria:

A STI em sua manifestação informa que até dezembro de 2018 providenciará a adequação do procedimento em uma ação conjunta com a SGP. Diz que a SGP/SEGED adota o procedimento de desligamento de acesso dos estagiários por meio de chamado aberto via Help Desk (SEI 0623590 e 0623586). No Plano de Trabalho STI (0623590), a recomendação consta o status de implementada.

Contudo, o procedimento adotado não se coaduna com o teor da recomendação, tendo em vista o art. 10 da Portaria TRE/SE 192/2018 determinar a configuração das contas de estagiários e prestadores de serviços para expirarem automaticamente, ao término do prazo de vigência do contrato.

Quanto à revisão das contas dos estagiários e prestadores de serviços, a STI informa a implementação da recomendação no dia 07/11/18 com base em lista enviada pela Seção de Gestão de Desempenho.

Achado 2 - Ausência de parecer para o uso compartilhado de acesso aos recursos da rede.

Situação encontrada: 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.
A operacionalização do acesso aos membros foi efetivada visando minimizar os problemas relacionados ao uso das credenciais, durante as sessões plenárias, conforme solicitação verbal da Coordenadoria de Registros, Processamentos, Acórdãos e Resoluções (COREP).

Critério(s) de auditoria:

- Portaria TRE/SE 192/2018

> Art. 12 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 Secretaria de Tecnologia da Informação acerca da possibilidade de aceitação dos riscos associados.

- ISO 27.002:2013

> 9.2.1 Registro e cancelamento de usuário
>
> (...)
>
> a) o uso de um ID de usuário único, para permitir relacionar os usuários com suas responsabilidades e ações; o uso compartilhado de ID de usuário somente será permitido, onde eles são necessários por razões operacionais ou de negócios e convém que seja aprovado e documentado;

Evidência(s): Questionário (0573387)

Causa(s): Inobservância de determinações normativas.

Consequência(s) do Achado: Ausência de transparência no ato de concessão de uso compartilhado de senhas.

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.

Resposta(s) do(s) Auditado(s):

Primeira Manifestação da STI:

A STI providenciará parecer acerca da aceitação dos riscos associados ao uso compartilhado das credenciais, conforme previsto no art. 12 da Portaria 192/2018, até o dia 31/08/2018.

Segunda Manifestação da STI/SEAPU:

Foram criadas contas para os membros.

Será realizado um trabalho de esclarecimento e orientação para a devida identificação.

Análise da Equipe de Auditoria:

No Plano de Tralho (0623590), a STI relata em sua segunda manifestação que foram criadas contas para os membros, e que será realizado um trabalho de esclarecimento e orientação para devida identificação no período de 01/01/19 a 31/07/19.

Por conseguinte, depreende-se que foram adotadas medidas no sentido de evitar os casos de identificação genérica e de uso compartilhado para acesso aos recursos da rede e que as providências a serem implementadas de esclarecimento e orientação estão em conformidade com a recomendação emitida.

Achado 3 – Fragilidade na qualidade das senhas e no acesso.

Situação encontrada: 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, COPEG e ASJUR, verificou-se que é possível acessar o SisDesktop com a mesma senha por mais de 90 dias.

Critério(s) de Auditoria:

- Portaria TRE/SE 192/2018,

> Art. 13 As senhas vinculadas às contas de acesso à rede corporativa deverão atender, obrigatoriamente, aos seguintes critérios:
>
> I – devem ter o tamanho mínimo de 10 (dez) caracteres;
>
> II – devem ser formados pela combinação de letras minúsculas e maiúsculas, números e símbolos;
>
> III – não podem ser iguais à última senha utilizada; e
>
> IV – devem ser alteradas a cada 90 (noventa) dias.

- ISO 27002

9.3.1 Uso da informação de autenticação secreta

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

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)

9.4.2 Procedimentos seguros de entrada no sistema (log-on)

Convém que um bom procedimento de entrada no sistema (log-on):

e) proteja contra tentativas forçadas de entrada no sistema (log-on);

9.4.3 Sistema de gerenciamento de senha

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 bloquei a reutilização;

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

- Manual de Boas Práticas em Segurança da Informação do TCU

2.5.1 Como deve ser projetado um processo de logon para ser considerado eficiente?

(...)

limitar o número de tentativas de logon sem sucesso (é recomendado um máximo de três tentativas), (...)

- Questionário para levantamento de informações (0573387), questão 2, item c

O Sistema de Gerenciamento de Senhas está configurado com o limite de bloqueio de conta após 10 tentativas de logon inválidas.

Evidência(s):

- Papel de Trabalho 08 - Teste de Observância_Senha de Acesso;
- Comunicado STI 13/07/2017: http://intranet.tre-se.gov.br/comunicados/sti/com-0001019-politica-de-senhas-mais-rigorosas

Causa(s): Inobservância de determinações normativas.

Consequências dos Achados: Vulnerabilidades no acesso ao sistema SisDescktop e permitir o cadastramento de senhas com baixa qualidade.

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.

Resposta(s) do(s) Auditado(s):

STI:

Nova política de senha implementada.

Envio de mensagem, com cartilha em anexo, orientando os usuários.

Análise da Equipe de Auditoria:

A STI informou que adotou o procedimento que possibilita a utilização dos 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 em 26/11/2018 e que houve o envio de mensagem por e-mail, com cartilha em anexo, orientando os usuários em 30/11/18.

As providências adotadas estão em conformidade com a recomendação emitida.

Achado 4 – Ausência de Revisão nos Direitos de Acesso.

Situação encontrada: A STI foi questionada se os direitos de acesso dos usuários são analisados criticamente em intervalos regulares.

Informou que realiza "o papel de "custodiante" dos ativos de tecnologia da informação, não cabendo a ela, todavia, definir quem pode acessar determinado recurso e qual nível de privilégio pode ser concedido, até porque, não possui autorização ou conhecimento para tanto." Seu papel seria de "…fornecer subsídios (listagens contendo usuários/privilégios, por exemplo) para que as unidades gestoras da solução pudessem indicar as inconsistências encontradas."
Nos termos do art. 3º, inciso IX da Portaria 192/2018, depreende-se que a unidade gestora da solução é responsável pela análise crítica dos direitos de acesso em intervalos regulares.

Nesse sentido, observa-se que os direitos de acesso dos usuários não são analisados criticamente em intervalos regulares.

Critério(s) de Auditoria:

- Portaria TRE/SE 192/2018

> Art. 3° Para os efeitos desta Portaria, considera-se:
>
> IX – unidade gestora da solução: unidade responsável pelas definições relativas aos processos de trabalho, regras de negócio e requisitos de uma solução de TI, bem como por acordar níveis de serviço para a solução, definir perfis de acesso e aprovar ou reprovar solicitações de autorização de acesso aos ativos sob sua responsabilidade;
>
> Art. 15 Cabe a cada titular de unidade solicitar, via sistema Helpdesk, a criação de diretórios de rede, a liberação e a restrição dos privilégios de acesso aos documentos de sua Unidade.

- ISO 27.002:2013

> Convém que a análise crítica dos direitos de acesso considerem as seguintes orientações:
>
> a) os direitos de acesso de usuários sejam revisados em intervalos regulares e depois de quaisquer mudanças, como promoção, remanejamento ou encerramento do contrato (ver 7);
>
> b) os direitos de acesso de usuários sejam analisados criticamente e realocados quando movidos de um tipo de atividade para outra na mesma organização;
>
> c) autorizações para direitos de acesso privilegiado especial sejam revisadas em intervalos mais frequentes;
>
> d) as alocações de privilégios sejam verificadas em intervalo de tempo regular para garantir que privilégios não autorizados não foram obtidos;
>
> e) as modificações para contas privilegiadas sejam registradas para análise crítica periódica.

Evidência(s): Questionário (0573387)

Causa(s): Inobservância de determinações normativas.

Consequência(s) do Achado: Permitir que servidores, prestadores de serviços ou estagiários permaneçam com acesso válido mesmo após desligamento, ocasionando vulnerabilidade nos sistemas.

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.

Resposta(s) do(s) Auditado(s):

Primeira Manifestação da STI:

A STI, com o envolvimento de todas as unidades gestoras de solução, pretende iniciar em 2019 projeto de longo prazo destinado a formalizar procedimento de auditoria no âmbito do TRE-SE para analisar criticamente os direitos de acesso dos usuários.

Segunda Manifestação da STI:

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.

Análise da Equipe de Auditoria:

A STI informou que iniciou, no período de 28/11/18 a 28/02/19, procedimento para identificar os ativos da informação por secretaria do tribunal, o que servirá de base para análise e identificação oficial dos responsáveis pelos ativos da informação.

As providências a serem implementadas se coadunam com a recomendação emitida, ao permitir as unidades gestoras da solução fazer uma análise crítica dos direitos de acesso dos usuários, a intervalos regulares, em conformidade com o disposto nos arts. 8º, 15, 33 da Portaria TRE/SE 192/2018.

Achado 5 – Regras de Acesso incompletas.

Situação encontrada:

O processo de Gerenciamento de Acesso e Uso de Recursos de TIC – Manual EPO 12 indica a utilização do documento denominado D1 – Regras de Acesso para utilização pelo Atendente de Chamado na Atividade "1. VERIFICAR requisição".

Para o referido processo, no tópico Termos e Definições, "regras de acesso" referem-se às políticas (ex: Política de Controle de Acesso) e regulamentos que definem quem pode ter acesso a determinado recurso de TIC, em quais circunstâncias o acesso pode ser

concedido, alterado ou removido e quais os privilégios de acesso de determinado perfil de usuário, por exemplo.

Da análise da Portaria 192/2018 – Política de Controle de Acesso e do documento D1 - "Regras de Acesso", enviado pela STI, verificamos que são incompletos para subsidiar a atividade do Atendente de Chamado na concessão de acessos, pois não possibilita concluir quais ativos estão sob a responsabilidade da unidade gestora da solução que solicitou a autorização de acesso.

Critério(s) de Auditoria:

- Manual de Processo de Trabalho de Gerenciamento de Acesso e Uso de Recursos de TIC – MANUAL EPO 12

  http://www.justicaeleitoral.jus.br/arquivos/tre-se-manual-do-processo-de-trabalho-de-gerenciamento-de-acesso-e-recursos-de-tic

- Portaria 192/2016

  Art. 4º O acesso às informações produzidas ou custodiadas pelo Tribunal Regional Eleitoral de Sergipe, que não sejam de domínio público, deve ser limitado às atribuições necessárias ao desempenho das respectivas atividades dos destinatários desta política, na forma descrita no caput do art. 2º.

Evidência(s): Regra de Acesso – D1 (0571188).

Causa(s): Ausência de levantamento dos ativos de informação sob responsabilidade das unidades gestoras da solução.

Consequência(s) do Achado: Possibilitar ao atendente do chamado conceder acesso a ativos de informação a unidades gestoras da solução sem vínculo com suas atividades.

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.

Resposta(s) do(s) Auditado(s):

STI:

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.

Análise da Equipe de Auditoria:

A STI informou que iniciou, no período de 28/11/18 a 28/02/19, procedimento para identificar os ativos da informação por secretaria do tribunal, o que servirá de base para análise e identificação oficial dos responsáveis pelos ativos da informação.

As providências a serem implementadas estão em conformidade com a recomendação emitida.

VIII. CONCLUSÃO

Em face dos testes aplicados e exames realizados nas atividades relacionadas à gestão da segurança da informação e ao controle de acessos aos ativos de tecnologia da informação, concluiu-se pela necessidade de se aperfeiçoar controles mediante adoção de procedimentos previstos em alguns normativos.

As Unidades Auditadas apresentaram Plano de Trabalho com vistas à implementação das recomendações emitidas por esta Unidade. Posteriormente, será realizado monitoramento do Plano de Trabalho STI (0623590) para assegurar a efetiva implementação das recomendações.

IX. PROPOSTA DE ENCAMINHAMENTO

Diante do exposto, submete-se o presente Relatório Conclusivo de Auditoria à consideração da Presidência, para ciência e encaminhamento à Secretaria de Tecnologia da Informação.

Documento assinado eletronicamente por **IVANILDO ALVES DE MEDEIROS**, **Chefe de Seção**, em 21/02/2019, às 11:21, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **ANA MARIA RABELO DE CARVALHO DANTAS**, **Coordenador**, em 27/02/2019, às 11:09, 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 **0637483** e o código CRC **1C5899A6**.