TRIBUNAL REGIONAL ELEITORAL DO ESPÍRITO SANTO
Rua João Batista Parra, 575 - Bairro Praia do Suá - CEP 29052-123 - Vitória - ES

RELATÓRIO

Assunto: Auditoria Integrada. Relatório de Final sobre o processo de Gestão de Segurança da Informação de TIC do Tribunal Regional Eleitoral do Espírito Santo.

Unidade Auditada: Secretaria de Tecnologia da Informação

Exercício: Referência - 2022.

I - INTRODUÇÃO

Em cumprimento à determinação do Tribunal Superior Eleitoral baseada nos termos da Resolução TSE de n.º 23.500/2016, foi realizada esta auditoria de caráter integrado com as demais Unidades de Auditoria dos Tribunais Regionais Eleitorais, sob supervisão do TSE, para avaliação do Processo de Gestão de Segurança da Informação TIC dos respectivos Regionais.

Após conhecimento do Plano de Auditoria, do Cronograma e do Programa elaborados de forma integrada com os TRE's e consolidados pelo TSE para realização dos trabalhos, a Seção de Auditoria desta Unidade de Auditoria Interna, mediante equipe técnica, cumpriu o planejamento que serviu para dar curso à efetivação da etapa de execução em testes selecionados de controle, tendo por critérios referenciais as regras pertinentes e boas práticas apresentadas por aquele Tribunal Superior.

Foram aplicados os 8 (oito) testes selecionados pelo TSE, sendo apurados 7 (sete) achados, tendo por elementos de análise as informações apresentadas pelos gestores suportadas por evidências correspondentes cujos resultados apurados se encontram na seção "Achados de Auditoria" deste Relatório, na qual a equipe de auditoria procedeu à análise conjunta dos referidos achados bem como das respostas dos auditados, à luz dos referidos critérios e boas práticas pertinentes, para a manifestação acerca do Processo de Gestão de Segurança da Informação deste Tribunal Regional Eleitoral.

II - VISÃO GERAL DO OBJETO AUDITADO

A gestão da Segurança da Informação constitui, sem dúvida, tema de destaque dentre as preocupações dos gestores públicos contempladas em diretrizes estratégicas dos entes políticos e respectivos órgãos e entidades da Administração Pública no bojo da condução da governança e gestão da coisa pública, sobretudo para aqueles que têm por prestação em sua atividade fim a entrega da informação de qualidade ao cidadão-cliente.

Para o Órgão da Justiça Eleitoral, Segurança da Informação constitui processo de suporte fundamental para a prestação dos serviços jurisdicionais desta justiça especializada, haja vista ser essa quem administra um dos maiores banco de dados do País, cobiçado por múltiplos agentes, com os mais variados tipos de interesses, além de visado por hackers para ações nocivas externas e internas que procuram entrar no domínio destas estruturas de informações para acessarem tais registros com outras finalidades, e, até mesmo, para promoverem danos a este patrimônio inestimável gerenciado no âmbito do Poder Judiciário.

Nesse contexto, o Poder Judiciário vem adotando, mediante seus Órgãos de cúpula, políticas direcionadas para mitigar eventuais riscos ao objetivo principal que é a prestação dos serviços

jurisdicionados aos usuários, a exemplo da Portaria CNJ nº 162/2021, que aprovou Protocolos e Manuais criados pela Resolução CNJ nº 396/2021.

Para o âmbito da Justiça Eleitoral, o TSE elaborou a Política de Segurança da Informação, instituída pela Resolução TSE nº 23.644/ 2021.

Durante Pleito Eleitoral, quando esta justiça especializada efetiva a entrega da prestação dos serviços eleitorais para a população a fim de que exerça os direitos de cidadania no processo democrático, sob maior fluxo e intensidade de demandas, os preparativos e procedimentos requerem atenção especial por parte da alta administração e seu corpo de colaboradores (servidores e agentes contratados) mediante concretização de políticas, diretrizes, práticas e protocolos, sob aspectos da legislação pertinente, com a finalidade de salvaguardar o bem sob foco, qual seja, a informação.

Nos limites de atuação deste Tribunal Regional Eleitoral, a Administração por meio de sua Secretaria de Tecnologia de Informação reuniu um conjunto de regras e procedimentos aplicáveis ao Processo de Gestão de Segurança da Informação que também serviram de parâmetros auxiliares para avaliação desta auditoria, dispostos na página da Intranet deste Tribunal conforme link: *http://intranet.tre-es.jus.br/intranet/pages/paginas.aspx?Cod_Pag=2247.*

III - OBJETIVO DA AUDITORIA

Este trabalho de auditoria teve por objetivo avaliar o processo de Gestão de Segurança da Informação, utilizando como critério principal o framework CIS Controls (The Center for Internet Security), versão 8, com destaque para os seguintes pontos:

a) Relativamente sobre a existência e a qualidade dos controles internos instituídos no processo de gerenciamento de provedores de serviço e seus respectivos contratos, no tocante à segurança da informação, de modo que seja verificado o tratamento dos riscos que impactem o alcance dos objetivos;

b) Referente à existência e a qualidade dos controles internos instituídos no processo de gestão de identidade e de controle de acessos aos ativos da organização, de modo que seja verificado o tratamento dos riscos que impactem o alcance dos objetivos; e

c) No que diz respeito ao alcance dos objetivos do processo quanto aos aspectos da eficiência, eficácia, economicidade e legalidade.

É importante destacar que esta avaliação assumiu características de uma auditoria operacional, sem descartar os aspectos da regularidade, na medida em que oportunizou esta equipe de auditoria em se manifestar, com sugestões à Administração do respectivo processo, no sentido da melhoria da gestão da Segurança da Informação, considerando os aspectos da economicidade, eficiência, eficácia e efetividade, em consonância com o que dispõe o Manual de Auditoria Operacional do Tribunal de Contas da União (2020) que conceitua o seguinte:

> *As auditorias operacionais possuem características próprias que as distinguem dos outros tipos de auditoria. Ao contrário das auditorias de conformidade e financeiras, que adotam padrões relativamente fixos, as auditorias operacionais, devido à variedade e complexidade das questões tratadas, possuem maior flexibilidade na escolha de temas, objetos de auditoria, métodos de trabalho e forma de comunicar as conclusões de auditoria. Empregam ampla seleção de métodos de avaliação e investigação de diferentes áreas do conhecimento, em especial das ciências sociais. Além disso, esse tipo de auditoria requer do auditor flexibilidade, imaginação e capacidade analítica.*
>
> *[...] Diversas fontes, além da legislação, podem ser usadas para identificar critérios de auditoria, incluindo regulamentações, normas, princípios e melhores práticas, referenciais de mensuração de desempenho e políticas e procedimentos organizacionais (GUID 3910/57).*

IV - ESCOPO

Para a delimitação do escopo desta auditoria, o Grupo de Trabalho de Auditoria formado com a participação das unidades de auditoria dos Regionais e a área de auditoria da Secretaria de Auditoria do Tribunal Superior Eleitoral consolidaram o escopo desta análise com a delimitação para verificação em três tipos de controles, os quais foram:

1. Gestão de provedor de serviços;
2. Gestão de contas e
3. Gestão do controle de acesso.

Conforme mencionado acima, o framework utilizado como critério para a avaliação foi o The Center for Internet Security (CIS Controls) versão 8, identificando-se o controle 15 - Gestão de Provedores de Serviços como critério a ser utilizado na auditoria. Segundo o CIS, o controle em questão incentiva o desenvolvimento de processo para avaliar os provedores de serviços que mantêm dados sensíveis, ou que são responsáveis por plataformas ou processos de TI críticos de uma organização, para garantir que esses provedores estejam protegendo as plataformas e os dados de forma adequada.

Incidentalmente, os controles 5 e 6, que tratam, respectivamente, da Gestão de Contas e da Gestão do controle de Acesso, também são objeto de avaliação, pois possuem interrelação direta com o controle 15. A gestão dos provedores de serviço envolve o gerenciamento da autorização de credenciais, bem como a utilização de processos e ferramentas para criar, atribuir, gerenciar e revogar credenciais de acesso e privilégios para contas de usuários, administradores e serviços em ativos e softwares corporativos, melhorando, assim, a segurança tecnológica da instituição.

V - ACHADOS DE AUDITORIA

1) Achado 01: Sobre a indicação dos integrantes técnicos no planejamento e fiscalização.

Achado: Ausência de informações acerca de efetiva capacitação em Segurança da Informação dos agentes públicos responsáveis pelo planejamento e fiscalização das contratações de tecnologia da informação deste Tribunal Regional Eleitoral.

Resposta do auditado:

> *No despacho CIS 0770205, informamos que todos os servidores da STI atuam como integrantes e fiscais técnicos nos contratos de TIC. Não identificamos no processo a resposta da SGP quanto ao item 1.2 da requisição UAI 0764712, com relatório de capacitação de cursos relativos à Segurança da Informação (segurança cibernética, firewall, LGPD, CIS controls, etc). Entendemos, smj, que a SGP deve ser consultada a respeito da ausência de informações.*
>
> *No âmbito desta STI, informamos no mesmo despacho CIS 0770205 sobre ações de capacitação em segurança da informação:*
>
> *"A capacitação e conscientização em segurança da informação, não só para os servidores da STI, mas para toda a Justiça Eleitoral, está em fase final de contratação em processo conduzido por este Tribunal (SEI 0001048-53.2022.6.08.8000). Adicionalmente, outra contratação recente de capacitação para os servidores da STI (SEI 0006821-16.2021.6.08.8000) - Plataforma de cursos Udemy - ajudará aprimorar os conhecimentos dos servidores também na área de SI."*

Complementação da resposta do auditado:

Ressalto, entretanto, que com relação ao item 1 (Achado: Ausência de informações acerca de efetiva capacitação em Segurança da Informação dos agentes públicos responsáveis pelo planejamento e fiscalização das contratações de tecnologia da informação deste Tribunal Regional Eleitoral), houve uma confusão inicial no processo, tendo em vista o seu encaminhamento a vários setores ao mesmo tempo, de forma que a STI ficou esperando informação da SGP e a SGP ficou esperando informação da STI.

Quando esta STI compreendeu a falha, encaminhou novamente o processo à SGP, a fim de que a STI pudesse responder, de forma completa, aos questionamentos apresentados, porém a SGP não teve tempo hábil para o levantamento necessário, razão pela qual, para não atrasar o envio das respostas, encaminho o processo com as informações de que disponho até o momento e, tão logo a SGP retorne com a listagem de capacitação dos servidores da TI em segurança da informação, complementaremos a resposta desta unidade.

Manifestação da equipe de auditoria:

Avaliadas as informações prestadas pelos setores responsáveis, verificou-se que foram apresentadas, em resposta ao relatório de achados, as iniciativas para capacitação em Segurança da Informação dos servidores que atuam na STI. No entanto, constatou-se que existem servidores que não possuem capacitação no tema objeto dessa auditoria.

Uma vez que todos podem atuar como fiscais ou integrantes técnicos no planejamento das contratações, tal treinamento e capacitação torna-se necessário, atendendo às orientações previstas no item 14 do CIS Controls (Conscientização sobre segurança e treinamento de competências), boa prática recomendada pelo Tribunal de Contas da União.

Por oportuno, vale ressaltar que por se tratar de tema estratégico no âmbito do planejamento e gestão, sugere-se que esta capacitação seja extensiva aos demais servidores que participam de contratações cujos objetos envolvam Segurança da Informação.

2) Achado 02: A presença de critérios de Segurança da Informação nos documentos (artefatos) de planejamento da contratação (DOD, ETP, TR, PB e termos).

Achado: Ausência de termos (de sigilo e confidencialidade), para as contratações que contemplem Segurança da Informação, verificada na amostra (id 0769947) de processos para análise e constatação dos artefatos que devem compor o planejamento das respectivas aquisições.

Resposta do auditado:

A amostra analisada contempla contratos de toda a espécie, conforme solicitação feita na requisição UAI 0764712, que foi:

2.1) Informar o universo de processos de contratações de bens/serviços de TI vigentes; (STI)

Poucas dessas contratações contemplam aspectos que envolvem Segurança da Informação.

Na amostra trazida no achado (0769947), nos processos que contemplam aspectos de segurança da informação, identificamos a presença de critério de do referido termo de sigilo e confidencialidade:

Item	*Serviço*	*Nº SEI*	*Documento de Planejamento*	*Controle Identificado*
12	*LICENÇAS DE USO DE SOFTWARE MICROSOFT OFFICE 365 E1 NA*	*0004379-14.2020.6.08.8000*	*ETP (Análise de Riscos) (0413278)*	*Risco 7.2 - Risco de aumento de vulnerabilidades*

	MODALIDADE ENTERPRISE AGREEMENT (EA)		*TR (item 5.7) (0458663)*	*relacionadas ás ferramentas online* *5.7. Manter o sigilo de dados e informações que tenha acesso, ficando vedada expressamente a retirada de dados e informações contidas nos armazenamentos do Contratante, sob pena de responsabilidade civil e criminal, na forma da lei. A assinatura dos termos de sigilo (ADENDOS I e II) é compulsória;*
13	*SOFTWARES PARA GESTÃO DE VULNERABILIDADES DOS ATIVOS DE TECNOLOGIA DA INFORMAÇÃO E APLICAÇÕES WEB DO TRE-ES*	*0004763-74.2020.6.08.8000*	*ETP (0422192)*	*2.5 - Requisitos de Segurança* *A empresa contratada deverá respeitar as diretrizes constantes da Política de Segurança da Informação da Justiça Eleitoral (Resolução TSE Nº 23.501/2016), obrigando-se a manter sigilo a respeito de quaisquer informações, dados, processos, fórmulas, códigos, cadastros, fluxogramas, diagramas lógicos, dispositivos, modelos ou outros materiais de propriedade do Tribunal Regional Eleitoral do Espírito Santo aos quais tiver acesso em decorrência do objeto da presente contratação, ficando terminantemente proibida de fazer uso ou revelação destes sob qualquer justificativa;* *O Tribunal Regional Eleitoral da Espírito Santo terá propriedade sobre todos os documentos e procedimentos operacionais produzidos*

				no escopo da presente contratação; *Os documentos eventualmente produzidos deverão ser repassados ao Tribunal tanto em formato não editável (PDF) como também em formato editável (.DOCX).* *O fornecedor assinará, no ato da entrega das licenças e do serviço, Termo de Confidencialidade, em que se comprometerá a não acessar, não divulgar e proteger todos os dados de infraestrutura e de vulnerabilidades do contratante a que tiver acesso, que abrangerá todos os seus colaboradores e terceiros, sob as penas da lei.*
22	*FORNECIMENTO E GARANTIA DE SOLUÇÃO DE SEGURANÇA CONTRA ATAQUES CIBERNÉTICOS E RANSOMWARE*	*0003216-62.2021.6.08.8000*	*TR (0624753)*	*6.3 - MODELOS DE TERMOS RELATIVOS À SEGURANÇA DA INFORMAÇÃO* • *A CONTRATADA se obriga a assinar Termo de Compromisso de Manutenção de Sigilo (Adendo I) emitido pela CONTRATANTE se responsabilizando quanto à manutenção de sigilo absoluto sobre quaisquer dados, informações, códigos-fonte e artefatos, contidos em quaisquer*

documentos e em quaisquer mídias, de que venha a ter conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pela CONTRATANTE, tais documentos.

- *A CONTRATADA não poderá divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto sem autorização por escrito da CONTRATANTE, sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos.*
- *Cada profissional alocado para a prestação do serviço objeto dessa contratação deverá assinar Termo de Ciência e Aceite das Condições de Manutenção de Sigilo (Adendo II), declarando ter ciência do Termo*

				de Compromisso de Manutenção de Sigilo e que, na execução de suas funções referentes ao contrato, cumprirá todas as disposições constantes naquele Termo.
25	*SOLUÇÃO DE GERENCIAMENTO DE ACESSOS PRIVILEGIADOS PARA DISPOSITIVOS, COM GARANTIA TÉCNICA DE 60 MESES*	*0000662-23.2022.6.08.8000*	*TR (0684549)*	*11. OBRIGAÇÕES DA CONTRATADA* *11.7. Fornecer à fiscalização do contrato relação nominal, com os respectivos números de documento de identidade de todo o pessoal envolvido diretamente na execução dos serviços, em até 3 (três) dias úteis após a publicação do extrato do contrato no Diário Oficial da União, bem como informar durante toda a vigência qualquer alteração que venha a ocorrer na referida relação.* *11.8. Fazer com que seus empregados se submetam aos regulamentos de segurança e disciplina durante o período do de permanência nas dependências do contratante, não sendo permitido o acesso dos funcionários que estejam utilizando trajessumários (shorts, chinelos de dedo, camisetas regatas ou sem camisa)* *11.10. Manter o caráter confidencial dos dados e informações obtidos por qualquer meio ou prestados pelo contratante, não os divulgando, copiando, fornecendo ou*

				mencionando a terceiros e nem a quaisquer pessoas ligadas direta ou indiretamente à Contratada, durante e após a vigência do contrato, inclusive em relação aos dados de infraestrutura, arquitetura, organização e/ou qualquer outra informação relativa ao ambiente tecnológico ou procedimentos técnicos do contratante.
26	*SOLUÇÃO DE SEGURANÇA PARA SERVIDORES (LINUX E WINDOWS), COM XDR E SANDBOX, COM MANUTENÇÃO, GARANTIA (UPDATE E UPGRADE) POR 60 MESES*	*0000589-51.2022.6.08.8000*	*TR (0684561)*	*13.9. Fornecer à fiscalização do contrato relação nominal, com os respectivos números de documento de identidade de todo o pessoal envolvido diretamente na execução dos serviços, em até 3 (três) dias úteis após a publicação do extrato do contrato no Diário Oficial da União, bem como informar durante toda a vigência qualquer alteração que venha a ocorrer na referida relação.* *13.10. Fazer com que seus empregados se submetam aos regulamentos de segurança e disciplina durante o período de permanência nas dependências do Contratante, não sendo permitido o acesso dos funcionários que estejam utilizando trajes sumários (shorts, chinelos de dedo, camisetas regatas ou sem camisa).*
32	*SERVIÇO DE DIGITALIZAÇÃO DE PROCESSOS*	*0000218-58.2020.6.08.8000*	*ETP (0636293)*	*REQUISITOS DE SEGURANÇA DA INFORMAÇÃO*

				TR (ADENDO I) - 0649997	*2.25. A contratada deverá manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre as informações, sistemas e documentos do TRE/ES, ou todo e qualquer assunto de interesse do contratante ou de terceiros, que tomar conhecimento em razão da execução do serviço;* *2.26. A contratada deverá assinar um termo de manutenção de sigilo e de responsabilidade na orientação de seus funcionários no sentido de resguardar o sigilo e os procedimentos de segurança;* *2.27. Não será permitida a retirada de qualquer material, documento físico ou arquivo digitalizado do ambiente de trabalho sem a autorização expressa do contratante, sob pena de responsabilidade civil e criminal, na forma da lei;* *2.28. A contratada deverá, ainda, apresentar ficha individual com a identificação dos empregados, mantendo nas dependências do contratante o cadastro atualizado desses profissionais;* *2.29. Será obrigatório o uso de crachás por parte dos funcionários da contratada, de forma visível, durante o período que estiverem exercendo suas atividades nas*

				dependências do contratante. *ADENDO I - Minuta de Termo de Compromisso de Manutenção de Sigilo*

Manifestação da equipe de auditoria:

Após análise das amostras dos processos de contratações de TI, a fim de verificar a presença dos artefatos nos autos (DOD, ETP, TR e Termos de Sigilo), não foram vistos os termos de Sigilo. Em posterior manifestação da unidade auditada, foi apresentado quadro informativo que confirma os contratos que devem atender à requisitos de segurança da informação e apresentar os respectivos documentos de manutenção de confidencialidade e sigilo.

3) Achado 03: Sobre inventário de contas de usuário, controle de acesso lógico (criação e descomissionamento) e gestão ativa de privilégios/perfis/funções (revisão regular).

Achado: Constatação de 16 (dezesseis) usuários entre servidores e colaboradores desligados, porém, ainda com suas contas no Active Directory (AC) ativos até a execução desta auditoria.

Resposta do auditado:

Os usuários foram removidos e a STI irá providenciar a formalização de um processo/norma de gestão de acesso lógico.

Manifestação da equipe de auditoria:

Tendo em vista o achado constatado quanto à gestão de acesso lógico, corrigido após a verificação desta auditoria, destacamos a necessidade de formalização de procedimentos de controle, conforme mencionado pelo próprio auditado, de forma a atender às orientações dos controles 05 e 06 do Cis Controls.

4) Achado 04: Desligamento de colaboradores terceirizados

Achado: Ausência de comprovação mediante evidências do comunicado de desligamento de colaboradores terceirizados (Cestic).

Resposta do auditado:

Apresentamos no despacho CIS 0770205, as evidências de desligamento de colaboradores, sendo:

A lista de nomes de colaboradores desligados nos últimos dois anos, constando ainda o número dos chamados, encontra-se no documento 0769526

O espelho dos chamados encontra-se no documento 0769963

Não apresentamos somente o referido "comunicado de desligamento de colaboradores encaminhados por prepostos de empresa contratada", visto que não existe qualquer previsão contratual desse tipo de comunicação ser feita de forma escrita pelo preposto.
Há sim, na documentação de gestão, as informações de rescisão desses colaboradores. Essas

rescisões, por obrigação contratual, são encaminhadas ao Tribunal e representam a comunicação formal de desligamento.

Não identificamos qualquer normativo que obrigue a Administração fazer constar cláusula em que o preposto faça essa comunicação por escrito.

Manifestação da equipe de auditoria:

Vistos os esclarecimentos do auditado, bem como os documentos apresentados, esta equipe de auditoria destaca que o procedimento adotado para comunicação do desligamento de colaboradores não evidencia o cumprimento pela contratada da obrigação contratual de "*c) Informar e solicitar ao Fiscal Técnico do TRE, no prazo máximo de 24 (vinte e quatro) horas, o descredenciamento dos recursos desvinculados da prestação de serviços com o TRE/ES (CLÁUSULA QUARTA - DAS OBRIGAÇÕES DA CONTRATADA - PARÁGRAFO SÉTIMO, ALÍNEA C)",* e necessita de aperfeiçoamento no sentido de formalização deste ato. Ressalta-se ainda, que o Adendo I ao contrato, item 1.1, estabelece que "*A comunicação da Contratada com o setor técnico do TRE/ES dar-se-á* ***preferencialmente*** *através do endereço eletrônico* ***sso@tre-es.jus.br..."*** **(grifo nosso).**

5) Achado 05: Sobre inventário e classificação de provedores de serviço e política de gestão de provedores.

Achado: Inexistência de Política de Provedores de Serviços com referência sobre classificação, inventário, avaliação, monitoramento e descomissionamento de prestadores de serviços.

Resposta do auditado:

Não há. Sobre esse achado, trata-se de classificação e gestão de provedores de serviço que tratam sistemas críticos e dados sensíveis (incluindo os dados pessoais) de todo o Tribunal. A adequação em relação a este item extrapola esta STI. Entendemos que deva ser tratada no âmbito da Comissão de Segurança da Informação, quando a sistemas críticos e no âmbito do CGPD, quanto a dados pessoais sensíveis.

Manifestação da equipe de auditoria:

Diante das informações apresentadas pela unidade auditada, verificou-se a inexistência de Política de Provedores de Serviços que trate especialmente sobre classificação, inventário, avaliação, monitoramento e descomissionamento de prestadores de serviços no âmbito deste Tribunal, conforme orienta o controle 15 do Cis Controls.

6) Achado 06: Sobre o monitoramento quanto a aspectos de Segurança da Informação durante a execução contratual.

Achado: Inexistência de registros de checagens relativos à Segurança da Informação durante a execução contratual (registros de verificação do cumprimento de requisitos contratuais que contemplem Segurança da Informação, registros de ocorrências e de gestão de riscos em SI).

Resposta do auditado:

Esse achado extrapola esta STI. Conforme já informado no despacho CIS 0770205, sugerimos a atualização do manual de gestão contratual deste Tribunal, sob supervisão da Comissão de Segurança da Informação no que diz respeito aos aspectos de segurança da informação que devam constar.

Sobre gestão de riscos, existe em andamento uma contratação conduzida pelo sr. Encarregado de Dados deste TRE, no processo 0005342-85.2021.6.08.8000, cujo objeto é "Adquirir solução de software para manter inventário de dados pessoais, processos de trabalho que envolvam dados pessoais, análise de riscos de privacidade e de segurança da informação".

Manifestação da equipe de auditoria:

A partir das informações prestadas, identificou-se que não são realizadas checagens com foco em Segurança da Informação durante a execução contratual (registros de verificação do cumprimento de requisitos contratuais que contemplem Segurança da Informação, registros de ocorrências e de gestão de riscos em SI). Conforme destacado pelo auditado, o aperfeiçoamento desse processo passa pela revisão de procedimentos de gestão contratual, a fim de adequá-los a essa demanda.

7) Achado 07: Sobre o processo de acesso físico nas dependências da organização (TRE/ES).

Achado: Autorizações de entrada de prestadores de serviços externos concedidas por prestadores de serviços de TI que atuam internamente neste Tribunal.

Resposta do auditado:

A correção do problema já foi solicitada ao fiscal técnico do contrato. A SAO foi cientificada de que essas autorizações devem vir diretamente dos servidores.

Manifestação da equipe de auditoria

Diante dos esclarecimentos apresentados, esta equipe de auditoria interna reitera a necessidade de que se atente para a exigência de concessão de autorização de entrada de prestadores de serviços externos por servidores que atuam neste TRE/ES, em atenção à NSI 003 V 2.0 - AGO 2020 SEGURANÇA DA INFORMAÇÃO.

VI - CONCLUSÃO

Em última análise, após a aplicação dos procedimentos técnicos referentes às etapas para a realização desta auditoria, esta equipe da Seção de Auditoria de Gestão informa que, com base nos critérios adotados para verificação das situações encontradas relativas ao processo de Gestão de Segurança da Informação de TIC, deste Tribunal Regional - TRE/ES, referência 2022, foram constatadas inconsistências apontadas nos achados acima descritos, tendo por comprovação as evidências apresentadas que deram suporte para as conclusões objetivas desta avaliação.

Todavia, tais inconsistências verificadas não tiveram o condão de macular o processo, haja vista que as situações apuradas, isolada ou em conjunto, não se caracterizaram como irregularidade(s) capaz(es) de promover prejuízo ao Erário, razão pela qual permite esta equipe se manifestar pela **regularidade** desse processo.

A constatação dessas inconsistências proporciona a esta equipe de auditoria aproveitar a oportunidade para recomendar à Administração deste Tribunal, mediante as unidades responsáveis **(STI, SAO, Comissão de Segurança da Informação, CGPD)**, a promoção de melhorias no processo de gestão de Segurança da Informação de TIC deste TRE/ES.

Dessa forma, as conclusões específicas dos achados foram sintetizadas em recomendações de aperfeiçoamento do processo as quais se encontram, a seguir, na **"Proposta de Encaminhamento"** deste relatório de auditoria integrada.

VII - PROPOSTA DE ENCAMINHAMENTO

Pelo exposto, submete-se o presente relatório à consideração do Senhor Coordenador da Unidade de Auditoria Interna deste Tribunal para providências a seu cargo e posterior encaminhamento ao Excelentíssimo Senhor Presidente deste TRE/ES, com vistas à ciência e manifestação pelas unidades competentes **(STI, SAO, Comissão de Segurança da Informação e CGPD)**, em suas respectivas competências, com prazo de resposta para até 06 de setembro de 2022, no que se refere às seguintes recomendações:

1) Promover treinamento e capacitação em Segurança da Informação (SI) para todos os servidores que possam atuar como fiscais ou integrantes técnicos nas contratações que tratem do tema SI. **(item 1)**

2) Fazer constar nos autos dos processos de contratações que envolvam segurança da informação, os respectivos artefatos exigidos nos termos da Resolução TRE/ES 261/2018, especialmente os termos de sigilo quando cabíveis. **(item 2)**

3) Formalizar procedimentos de controle que contemplem a criação, descomissionamento e revisão regular de contas de acesso lógico. **(item 3)**

4) Estabelecer comunicação em tempo hábil, administrativa e formal, acerca de eventual desligamento de colaboradores terceirizados, entre a empresa contratada e este Tribunal, com vistas ao aperfeiçoamento deste controle. **(item 4)**

5) Estabelecer neste Tribunal Política de Provedores de Serviços com referência sobre classificação, inventário, avaliação, monitoramento e descomissionamento de prestadores de serviços. **(item 5)**

6) Adequar os normativos que tratam da gestão e fiscalização contratual, especialmente o Guia de Gestão e Fiscalização Contratual, para que estabeleçam a realização de checagens com foco em Segurança da Informação durante a execução contratual (verificação do cumprimento de requisitos contratuais relativos à Segurança da Informação, registros de ocorrências e de gestão de riscos em SI) e a manutenção dos registros de tal natureza nos autos. **(item 6)**

7) Atentar para que a autorização de entrada de prestadores de serviços externos seja concedida por servidores que atuam neste Tribunal. **(item 7)**

Em tempo, esta Seção de Auditoria solicita o encaminhamento deste Relatório Final para conhecimento do conteúdo pela Presidência deste Tribunal e posterior envio às unidades auditadas endereçadas **(STI, SAO, Comissão de Segurança da Informação e CGPD)** para providências dos responsáveis, na forma que dispõe o artigo 55 da Resolução CNJ 309/2020 alinhado às Normas de Auditoria do Tribunal de Contas da União (NAT's).

Documento assinado eletronicamente por **JOSE RENATO DE AZEVEDO**, **Chefe de Seção**, em 17/08/2022, às 17:19, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **PRISCILA SCHULTHAIS LEMOS**, **Técnico Judiciário**, em 17/08/2022, às 17:20, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **WELITON MARIANO NEVES**, **Técnico Judiciário**, em 17/08/2022, às 17:21, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **HELIO DE OLIVEIRA DUQUE**, **Técnico Judiciário**, em 17/08/2022, às 17:32, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tre-es.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0790500** e o código CRC **3FECE0F4**.