



TRIBUNAL REGIONAL ELEITORAL DE RORAIMA
AVENIDA JUSCELINO KUBITSCHEK 543 - Bairro SÃO PEDRO - CEP 69306685 - Boa Vista - RR
Coordenadoria de Auditoria

RELATÓRIO DE AUDITORIA

JUSTIÇA ELEITORAL
TRIBUNAL REGIONAL ELEITORAL DE RORAIMA
COORDENADORIA DE AUDITORIA
SEÇÃO DE AUDITORIA DE GOVERNANÇA

RELATÓRIO DE AUDITORIA n ° 01/2022

Preâmbulo

Processo n° : 0001125-45.2022.6.23.8000

Ato originário: PAA-2022 - Processo n° 0001917-33.2021.6.23.8000

Período abrangido pela auditoria: alguns testes levados a termo, tiveram abrangência dos últimos 2 (dois) anos.

Período de realização da auditoria: (Planejamento – de 09/05/2022 a 29/06/2022); (Execução de 30/06/2022 a 09/08/2022) e (Relatório de 10/08/2022 a 16/08/2022).

Unidade Auditada:

Secretaria/Assessoria: Secretaria de Tecnologia da Informação e Comunicação.

Coordenadoria: Coordenadoria de Infraestrutura e Soluções Corporativas -CISC; Coordenadoria de Infraestrutura e Cibersegurança-CIC

Seção: Seção de Infraestrutura e Comunicação -SIC (Atual Coordenadoria de Infraestrutura e Cibersegurança-CIC); Seção de Gestão de Serviços de TI - SGSTI (Atual Seção de Serviços aos Usuários) e Seção de Governança e Planejamento - SGP (Atual Seção de Governança e Gestão de Serviços).

Tipo de Auditoria: Auditoria Integrada da Justiça Eleitoral de 2022.

SUMÁRIO

I - INTRODUÇÃO**II - VISÃO GERAL DO OBJETO AUDITADO****III - OBJETIVO DA AUDITORIA****IV - ESCOPO****V - ACHADOS DE AUDITORIA****VI - CONCLUSÃO****VII - PROPOSTA DE ENCAMINHAMENTO****I - INTRODUÇÃO**

Em cumprimento ao cronograma estabelecido no Plano Anual de Auditoria - PAA - 2022, aprovado pela Presidência deste Tribunal, documento SEI nº [0708334](#), objeto do Procedimento SEI nº [0001917-33.2021.6.23.8000](#), foram realizados exames de auditoria, no âmbito da Justiça Eleitoral, no processo de gestão de segurança da informação.

Com vistas à determinação do escopo desta auditoria, o TSE elaborou o Plano de Trabalho de Auditoria ([0688854](#)) onde foram definidos a visão geral do objeto avaliado, o objetivo preliminar da auditoria, os parâmetros para escolha da equipe e determinação do tempo estimado da auditoria, as etapas da auditoria e o cronograma.

Foram realizadas reuniões de abertura ([0693466](#)) e de encerramento dos trabalhos ([0711428](#)) entre a equipe de auditoria e os gestores responsáveis pelas áreas auditadas.

Na reunião de abertura, foram apresentados os membros da equipe de auditoria, os objetivos do trabalho, o escopo e as questões de auditoria.

Na reunião de encerramento, foi apresentada a Matriz de Achados resultante dos testes aplicados. Na ocasião, foi possibilitado aos gestores manifestação sobre o exposto cujas respostas foram consideradas e incluídas neste relatório final.

II - VISÃO GERAL DO OBJETO AUDITADO

O objeto auditado, a cada dia, torna-se central na gestão das organizações, pois engloba a adoção de estratégias que devem se dar de modo organizado e planejado, com o propósito de proteger um ativo de importância singular: a informação. Nesse contexto, a cibersegurança é transversal, requerendo a implementação de diretrizes, políticas, práticas e protocolos, assim como a aderência a aspectos legais e a revisão de procedimentos técnicos.

De acordo com o ranking dos países alvo de ataques cibernéticos na América Latina, o Brasil é o principal alvo da região, sendo o 4º no ranking mundial de acordo com a 24ª edição do Internet Security Threat Report (ISTR), relatório de segurança da Symantec. Segundo o estudo, o Brasil ocupa a 3ª colocação em ataques referentes a spams e à Internet das coisas (IoT), o 4º em ransomware e o 9º em phishing.

Nos últimos anos, tem sido comum presenciar eventos de ataques cibernéticos a órgãos públicos, em especial a Tribunais, vide os ataques ao Superior Tribunal de Justiça – STJ (novembro/2020), Supremo Tribunal Federal – STF (maio/2021), TJ-RS (novembro/2020 e abril/2021) e TRF-3 (janeiro/2021 e março/2022).

Diante desse cenário de riscos e ameaças, a Justiça Eleitoral é um dos principais alvos de ataques cibernéticos, em especial devido a sua crítica missão de liderar e organizar as etapas do processo eleitoral brasileiro, representando instrumento essencial da democracia. Considerando a proximidade das eleições de 2022, que apresenta um provável cenário político bastante polarizado, além de declarações polêmicas que buscam ferir a imagem da Justiça Eleitoral, a temática da Segurança Cibernética no TSE se tornou ainda mais relevante.

Nesse sentido, o TSE aprovou a Estratégia Nacional de Cibersegurança, com o objetivo de direcionar “diversas ações em segurança cibernética necessárias para o ganho de maturidade em capacidade de identificação, proteção, detecção, resposta e recuperação de incidentes de segurança relacionados com a presença das instituições referenciadas no ciberespaço”. A iniciativa complementa os demais normativos recentes publicados no Poder Judiciário e no TSE, tal como a Portaria CNJ nº 162, de 10 de junho de 2021, que aprova Protocolos e Manuais criados pela Resolução CNJ nº 396/2021, bem como a Política de Segurança da Informação da JE, instituída pela Resolução TSE nº 23.644, de 1º de julho de 2021.

Frente ao exposto, os exames de auditoria, no presente caso, serão efetuados no âmbito da Secretaria de Tecnologia da Informação (STI), unidade responsável pela condução das principais tarefas dentro do Tribunal.

São objetivos do objeto avaliado, conforme os processos e controles de segurança em destaque:

- Gestão de identidade e de controle de acessos;
- Gerenciamento de crises cibernéticas;
- Investigação para ilícitos cibernéticos;
- Gerenciamento contínuo de vulnerabilidades e realização de testes de penetração;
- Proteções de e-mails, de navegadores e defesas antimalwares;
- Gerenciamento, monitoramento e defesa em infraestrutura de redes;
- Política de educação e cultura em segurança cibernética;
- Desenvolvimento seguro de sistemas; e
- Gerenciamento de provedores de serviços.

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, nos seguintes pontos:

- a. 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. A 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. Avaliar o alcance dos objetivos do processo quanto aos aspectos da eficiência, eficácia, economicidade e legalidade.

IV - ESCOPO

Como retratado no Plano de Trabalho desta auditoria integrada, 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 inter-relação 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

Os testes aplicados obedeceram aos testes mínimos previstos no Programa de Auditoria Consolidado da JE (Documento SEI nº [0701596](#)), elaborado por meio do cotejo das matrizes de testes levantadas por este TRE (Documento SEI nº [0697389](#) e [0711428](#)), com as informações correlatas de todos os tribunais regionais eleitorais.

Os achados a seguir foram identificados a partir da situação encontrada pela equipe e o critério estabelecido, e foram apresentados à Coordenadoria de Infraestrutura e Cibersegurança- CIC/STI, por meio da Matriz de Achados para ciência e manifestação:

Relação de Achados:

A1 - Não houve capacitação aos indicados técnicos da equipe.

Situação encontrada: Os servidores indicados como integrantes técnicos na composição das equipes de contratação não foram capacitados em SI nos últimos 2 anos, conforme informação contida no Despacho nº 12538 / 2022 - TRE-RR/PRES/DG/STIC/CIC/SCIC - Evento SEI 703514.

Critérios: Controle 14 do Controls CIS V- 8, (conscientização sobre segurança e treinamento de competências) e Art. 10, §3º da IN SGD/ME (Contratação de Soluções de TI) de nº 01/2019.

Efeitos/Consequência do Achado: Equipes de contratação compostas por integrantes técnicos sem capacitação na área de SI.

Possíveis causas: Ausência de políticas internas voltadas a treinamento da força de trabalho em SI.

Manifestação do Auditado: De acordo com o Despacho nº 14450 / 2022 - TRE-RR/PRES/DG/STIC/CIC, "*Com a reestruturação da comissão de segurança da informação e a criação da unidade de segurança cibernética que tem como um dos papéis apoiar tanto ao gestor de Segurança da Informação quanto à própria CSI, estão sendo encaminhadas tratativas no sentido de difundir a cultura de SI, bem como será realizado o planejamento da capacitação dos integrantes desta STIC e também integrantes das demais áreas envolvidas nos processos de contratações, tais como Secretaria de Administração, Assessoria de Contratos, Assessoria de Licitações, Assessoria Jurídica da Diretoria Geral e a própria Diretoria Geral.*"

Conclusão da Equipe de Auditoria: Monitorar a adoção ou o melhoramento de políticas voltadas à segurança da informação no âmbito do TRE/RR.

Proposta de Encaminhamento: Estabelecer e manter um programa de conscientização de segurança, através de treinamento da força de trabalho nas melhores práticas sobre segurança da informação.

A2 - Utilização incipiente de critérios de SI nos processo de contratação.

Situação encontrada: Na análise efetivada nas contratações de soluções de TIC, dos dois últimos anos, foi verificado que apenas 26% das contratações incluiu previsões de requisitos de SI (previsão de glosa ou sanções quanto à violações de SI, sigilo, termos de confidencialidade etc.).

Critérios: Item 7.1 da IN SGD/ME (Contratação de Soluções de TI) de nº 01/2019 e Item 15.4 do Controls CIS V- 8.

Efeitos/Consequência do Achado: Contratações de TIC sem a observância de critérios voltados à segurança da informação.

Manifestação do Auditado: De acordo com o Despacho nº 14450 / 2022 - TRE-RR/PRES/DG/STIC/CIC, "*O processo que resulta em uma contratação de solução de TIC envolve uma equipe contratação multidisciplinar com integrantes da STIC e da Assessoria de Licitações, com aprovação dos artefatos pelo Comitê de Governança de TIC e da Assessoria Jurídica da Diretoria Geral. Daí a necessidade primordial de capacitação dos setores chaves envolvidos no processo, situação esta que foge à alçada desta Unidade Administrativa, pois, há a necessidade de inserção de termos adicionais ao modelo de contratos utilizados e também a análise jurídica desses termos para que não haja qualquer vício ao processo.*"

Conclusão da Equipe de Auditoria: Monitorar a adoção ou o melhoramento de políticas voltadas à segurança da informação no âmbito do TRE/RR.

Proposta de Encaminhamento: Adotar controles visando a a elaboração de termos de referência ou projeto básico para contratação de Soluções de TIC com requisitos e obrigações de SI, considerando a legislação vigente e os riscos de segurança da informação.

A3 - O TRE/RR não possui inventário de provedores de serviço.

Situação encontrada: O TRE/RR ainda não adota política de gestão de provedores de serviços.

Situação Ideal/Critérios: Item 15.1 do Controls CIS V- 8.

Efeitos/Consequência do Achado: Risco de violação dos dados considerados críticos ou sensíveis.

Manifestação do Auditado: De acordo com o Despacho nº 14450 / 2022 - TRE-RR/PRES/DG/STIC/CIC, "*Quanto a este achado no relatório consideramos um ponto a ser melhorado. Na atual circunstância a STIC possui 08 (oito) contratos de prestação de serviços continuados, dos quais apenas 01 (um) provê serviços de terceirização.*"

Também está em processo de finalização o processo de licitação para a realização de 01 (um) contrato que substituirá 04 (quatro) dos oito atualmente existentes.

Mesmo sendo em quantidade muito reduzida, serão tomadas medidas para a implantação de um processo sistemático de inventário de provedores de serviço em atenção às boas práticas do processo de SI."

Conclusão da Equipe de Auditoria: Monitorar a adoção ou o melhoramento de políticas voltadas à segurança da informação no âmbito do TRE/RR.

Proposta de Encaminhamento: Estabelecer e manter um inventário de provedores de serviços que mantêm dados sensíveis ou são responsáveis por plataformas ou processos de TI críticos, incluindo classificação e designando um contato corporativo para cada provedor de serviços.

A4 - Não existe solução de TI ou outro procedimento para monitoramento de SI na execução contratual.

Situação encontrada: O TRE/RR ainda não possui solução de TI contratada ou em contratação para dar suporte ao processo de fiscalização e monitoramento da execução contratual.

Foram analisadas as contratações de soluções de TIC vigentes, e não foram observados critérios ou check-list para verificar a conformidade do contrato.

Situação Ideal/Critérios: Art. 8º, §1º da IN SGD/ME nº 01/2019 (Contratação de Soluções de TI) e Item 15.6 do Controls CIS V- 8.

Efeitos/Consequência do Achado: Possíveis falhas quanto aos quesitos de segurança da informação previstos na contratação.

Manifestação do Auditado: De acordo com o Despacho nº 14450 / 2022 - TRE-RR/PRES/DG/STIC/CIC, "*Quanto a este achado no relatório no relatório consideramos também um ponto a ser melhorado. O objetivo é traçar estratégia que viabilize o processo de monitoramento sem que haja alto custo de investimento e com a aplicação de mão de obra capacitada que faça parte do corpo de servidores deste TRE-RR.*"

Conclusão da Equipe de Auditoria: Monitorar a adoção ou o melhoramento de políticas voltadas à segurança da informação no âmbito do TRE/RR.

Proposta de Encaminhamento: Criar uma ferramenta de controle, por meio de check-list ou outro critério para avaliar o objeto ou serviço prestado durante a execução contratual, no tocante aos quesitos de segurança da informação.

A5 - Não existe assinatura dos termos de confidencialidade e sigilo, quando previstos na contratação.

Situação encontrada: A análise efetuada nos processos de contratação de soluções de TIC, nos últimos 2 anos, comprovaram que, embora alguns termos de referências e contratos tenham a previsão de exigência do termo de confidencialidade, quando da efetivação da contratação não foi exigida a apresentação do documento, portanto, considerou-se ausente de assinatura.

Situação Ideal/Critérios: Art. 8º, §1º da IN SGD/ME nº 01/2019 (Contratação de Soluções de TI) e Item 15.4 do Controls CIS V- 8.

Efeitos/Consequência do Achado: Execução contratual sem a exigência de instrumentos voltados à SI.

Manifestação do Auditado: De acordo com o Despacho nº 14450 / 2022 - TRE-RR/PRES/DG/STIC/CIC, "*Quanto a este achado no relatório consideramos também um ponto a ser melhorado. Na atual normatização a gestão contratual prevê a existência da fiscalização técnica e fiscalização administrativa, bem como os ditames necessários à assinatura contratual.*

Os termos de confidencialidade e sigilosidade são requisitos que devem ser observados quando da assinatura do contrato e devem constar nos artefatos de contratação como parte integrante da minuta do contrato a ser celebrado.

Dessa forma fica mais uma vez evidenciada a necessidade de capacitação de toda a equipe de contratação em Segurança da Informação de forma a garantir que o processo de contratação esteja em conformidade com os requisitos de Segurança da Informação."

Conclusão da Equipe de Auditoria: Monitorar a adoção ou o melhoramento de políticas voltadas à segurança da informação no âmbito do TRE/RR.

Proposta de Encaminhamento: Utilizar check-list para otimizar o acompanhamento da execução contratual, objetivando evitar eventuais descumprimentos dos quesitos de SI.

A6 - Utilização incipiente de critérios de SI nos processos de contratação de soluções de TIC.

Situação encontrada: Os exames foram efetivados em algumas contratações realizadas nos últimos dois anos e revelaram a efetivação de contratação de soluções de TIC sem a utilização de requisitos de SI, como nos processos 0001723-67.2020.6.23.8000 - acesso dedicado à internet; 0002876-38.2020.6.23.8000- serviço de suporte em nível 3; 0000786-86.2022.6.23.8000-aq. De solução de gerenciamento de acessos privilegiados e 0000781-64.2022.6.23.8000-Aquisição de subscrições de soluções anti-virus com EDR.

Situação Ideal/Critérios: Item 7.1 da IN SGD/ME (Contratação de Soluções de TI) de nº 01/2019 e Item 15.4 do Controls CIS V- 8.

Efeitos/Consequência do Achado: Possíveis fragilidades nas contratações, quanto ao aspecto da SI.

Manifestação do Auditado: De acordo com o Despacho nº 14450 / 2022 - TRE-RR/PRES/DG/STIC/CIC, "*Manifestação já realizada no achado de nº 2.*"

Conclusão da Equipe de Auditoria: Monitorar a adoção ou o melhoramento de políticas voltadas à segurança da informação no âmbito do TRE/RR.

Proposta de Encaminhamento: Adotar controles que possibilitem a adoção de normativos/políticas quanto à SI nos modelos de prestação de serviços, considerando a legislação vigente e os riscos de segurança da informação.

A7 - Não há registro formal da entrada e saída de prestadores de serviços no prédio do TRE/RR.

Situação encontrada: Despacho nº 12538/2022 - TRE-RR/PRES/DG/STIC/CIC/SCIC - Evento SEI 703514 e Despacho nº 13446/2022 - TRE-RR/PRES/DG/STIC/CIC -Evento SEI nº 706584 e Despacho nº 13209/2022 - TRE-RR/PRES/DG/SA/CAAE - evento SEI nº 0705910.

Situação Ideal/Critérios: Controle 15, do Controls CIS V- 8.

Efeitos/Consequência do Achado: Risco de incidente provocado por terceiros.

Manifestação do Auditado: De acordo com o Despacho nº 14450 / 2022 - TRE-RR/PRES/DG/STIC/CIC.

Quanto a este achado no relatório, está em análise na Comissão de Segurança da Informação a Minuta de Portaria - Gestão Ident. e Controle Acesso Físico e Lógico (SEI nº 0707860) que deverá regulamentar a implementação dos controles necessários ao atendimento.

Em conjunto com Coordenadoria de Polícia Judiciária (CPOL) deverão ser implementados os mecanismos necessários ao controle de acesso não só para o controle dos provedores de serviços, mas para toda a instituição."

Conclusão da Equipe de Auditoria: Monitorar a adoção ou o melhoramento de políticas voltadas à segurança da informação no âmbito do TRE/RR.

Proposta de Encaminhamento: Fortalecer os controles que resguardem o acesso físico de colaboradores às dependências do TRE/RR.

VI - CONCLUSÃO

Pelo exposto, em face dos resultados, observou-se que os controles internos instituídos no processo de gestão de identidade e de controle de acessos aos ativos do TRE/RR, como registro formal, via central de serviços, para concessão de contas e de privilégios a novos usuários, consultas junto a unidade de pessoal, a cada trimestre para efetivação da manutenção das contas, bem como adoção da política de expiração de senhas a cada 180 dias no Active Directory (AD); utilização de consultas semanais às portarias no DJE e de consultas trimestrais à unidade de pessoal para efetivar a exclusão do usuário que deixou o órgão, e a utilização da ferramenta MFA no acesso à VPN e ao correio eletrônico (contas de e-mail), garantem, de forma eficiente, a mitigação dos riscos deste processo.

Quanto aos controles adotados pelo TRE/RR no processo de gerenciamento de provedores de serviços e seus respectivos contratos, no tocante à segurança da informação, observou-se que estes são ainda incipientes, fazendo-se necessário a adoção uma política de conscientização de segurança da informação, de forma abrangente, envolvendo as unidades ligadas direta e indiretamente ao gerenciamento dos provedores de serviços externos, uma vez que os trabalhos revelaram deficiências desde a fase inicial da contratação (Achado 1); utilização tímida de critérios de SI, como previsão de glosa ou sanções quanto à violação de SI, exigência de termos de confidencialidade (Achado 2 e 6); não adoção de inventário dos provedores de serviço, em que pese o TRE/RR possuir um número bastante reduzido (Achado 3); inexistência de ferramenta formal para monitoramento de SI na execução contratual (Achados 5 e 6) e deixar de registrar, formalmente, a entrada e saída de prestadores de serviços no prédio do TRE/RR (Achado 7).

Assim, para o fortalecimento dos mecanismos de controles que mitigarão os riscos inerentes ao processo de gerenciamento de provedores de serviços, haverá a necessidade da participação de unidades que estão fora da estrutura da Secretaria de Tecnologia da Informação - STIC, conforme pontuado no Despacho nº 14450 / 2022 - TRE-RR/PRES/DG/STIC/CIC e Despacho nº 14773 / 2022 - TRE-RR/PRES/DG/STIC/CIC, documentos SEI nº [0709814](#) e [0710919](#).

VII - PROPOSTA DE ENCAMINHAMENTO

Diante do exposto, submetemos o presente relatório à consideração do Excelentíssimo Senhor Desembargador Presidente do TRE/RR, para conhecimento e autorização para encaminhamento à Secretaria de Auditoria do TSE, em observância ao cronograma da auditoria previsto no Anexo do Plano de Trabalho da Auditoria Integrada, documento SEI nº [0688492](#).

Após as providências acima, sugere-se o encaminhamento à Diretoria Geral, Secretaria de Tecnologia da Informação, Gestor de Segurança da Informação, Presidente da Comissão de Segurança da Informação, Secretário de Administração, Assessoria de Contratos e Assessor de Licitações para conhecimento e adoção das seguintes recomendações:

Recomendação	Achado nº	Unidade
Estabelecer e manter um programa de conscientização de segurança, através de treinamento da força de trabalho nas melhores práticas sobre segurança da informação.	A1	STIC
Adotar controles visando a a elaboração de termos de referência ou projeto básico para contratação de Soluções de TIC com requisitos e obrigações de SI, considerando a legislação vigente e os riscos de segurança da informação.	A2	STIC/SA
Estabelecer e manter um inventário de provedores de serviços que mantém dados sensíveis ou são responsáveis por plataformas ou processos de TI críticos, incluindo classificação e designando um contato corporativo para cada provedor de serviços.	A3	STIC
Criar uma ferramenta de controle, por meio de check-list ou outro critério para avaliar o objeto ou serviço prestado durante a execução contratual, no tocante aos quesitos de segurança da informação.	A4	STIC
Utilizar check-list para otimizar o acompanhamento da execução contratual, objetivando evitar eventuais descumprimentos aos quesitos de SI.	A5	STIC
Adotar controles que possibilitem a adoção de normativos/políticas quanto à SI nos modelos de prestação de serviços, considerando a legislação vigente e os riscos de segurança da informação.	A6	STIC/SA
Fortalecer os controles que resguardem o acesso físico de colaboradores às dependências do TRE/RR.	A7	STIC/SA

MARIA DO PERPÉTUO SOCORRO ROSAS TRAJANO Auditor 1 - matrícula 26200251 - Coordenação <i>(documento assinado eletronicamente)</i>	DENIS ALVES DA COSTA Auditor 2 - matrícula 26300421 - Membro da Equipe <i>(documento assinado eletronicamente)</i>
NELSON AMARO JUNIOR Auditor 3 - matrícula 26300492 - Membro da Equipe <i>(documento assinado eletronicamente)</i>	ALÍSIO STEINER SOARES DE MACEDO Auditor 4 - matrícula 26350102 - Supervisor <i>(documento assinado eletronicamente)</i>



Documento assinado eletronicamente por **DENIS ALVES DA COSTA, Chefe de Seção**, em 16/08/2022, às 11:14, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **ALÍSIO STEINER SOARES DE MACEDO, Coordenador de Auditoria**, em 16/08/2022, às 11:14, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **NELSON AMARO JUNIOR, Chefe de Seção**, em 16/08/2022, às 11:55, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **MARIA DO PERPÉTUO SOCORRO ROSAS TRAJANO, Analista Judiciário**, em 16/08/2022, às 12:19, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site <https://sei.tre-rr.jus.br/autenticidade> informando o código verificador **0712227** e o código CRC **99AD003B**.

0001125-45.2022.6.23.8000

0712227v76

Criado por **ALISIO**, versão 76 por **perpetuo** em 16/08/2022 11:10:11.