TRIBUNAL REGIONAL FEDERAL DA 4ª REGIÃO
Rua Otávio Francisco Caruso da Rocha, 300 - Bairro Praia de Belas - CEP 90010-395 - Porto Alegre - RS - www.trf4.jus.br

ESTUDO TÉCNICO PRELIMINAR Nº 7393585/2024

INTRODUÇÃO

O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para atendimento da demanda constante no Documento de Oficialização da Demanda (doc. SEI 7348830), bem como demonstrar a viabilidade técnica e econômica da contratação.

1. ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO (ART. 14, RESOLUÇÃO CNJ 468/2022)

1.1. DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO (ART. 18, § 1º, I, DA LEI Nº 14.133/2021)

A Segurança da Informação tem se tornado cada vez mais importante para a imagem e para a continuidade das atividades finalísticas das instituições. Incidentes recentes ocorridos com órgãos do Poder Judiciário reforçam a necessidade de se buscar o aprimoramento dos controles de segurança de TI, procurar a identificação de vulnerabilidades de segurança cibernética e a urgência da atuação preventiva para tratar as brechas de segurança.

Dentre os diversos problemas de segurança cibernética existentes, um dos mais potencialmente danosos é o de exploração de contas privilegiadas. Tais contas são as que possuem permissão para acessar e modificar configurações de servidores, switches, roteadores, sistemas, bancos de dados e demais dispositivos do ambiente tecnológico. A utilização de credenciais com privilégios especiais é requisito de segurança básico para a manutenção das operações diárias das unidades de TI, seja por técnicos, contas de serviços ou aplicações.

Um relatório divulgado pela instituição de consultoria e pesquisa Forrester indicou que aproximadamente 80% das violações de segurança estavam relacionadas com o comprometimento de credenciais válidas [1]. O Gartner, renomado instituto de pesquisa, previsão e consultoria na área de TIC, afirma que as identidades são o novo perímetro de segurança, que um objetivo principal de todos os ataques avançados é obter credenciais privilegiadas e que o investimento em soluções para proteção das credenciais deve estar no topo de prioridade das organizações [2] [3].

Quando uma conta comprometida tem privilégios, o agente da ameaça pode conquistar o controle de ativos críticos da infraestrutura de TI, contornar ou desabilitar controles de segurança, realizar movimentos laterais para explorar outros serviços de TI, quebrar outras senhas, sequestrar informação confidencial ou sensível, criptografar dados, deletar cópias de segurança (backups) e assim acabar interrompendo o funcionamento de um órgão. A exploração de credenciais privilegiadas tem ocorrido na ampla maioria das invasões de grande impacto relatadas em organizações governamentais e privadas. Por esses motivos é que as credenciais altamente privilegiadas são as mais importantes de todas as credenciais a serem protegidas.

[1] https://www.seguridadar.com/bt/inf-pb-forrester-2018.pdf
[2] https://www.gartner.com/en/documents/3900996-top-10-security-projects-for-2019
[3] https://www.gartner.com/en/doc/760806-top-trends-in-cybersecurity

1.2. MOTIVAÇÃO DA CONTRATAÇÃO (ART. 50, § 1º, LEI N. 9.784/99)

Tendo em vista a esses desafios, a indústria de segurança da informação desenvolveu o conceito de solução de Privileged Access Management - PAM. As ferramentas PAM ajudam as organizações a fornecer acesso privilegiado seguro a ativos críticos e a atender aos requisitos de conformidade, gerenciamento e monitoramento de contas e acessos privilegiados. As ferramentas de PAM oferecem os seguintes recursos:

- Rastrear as ações executadas por usuários administradores.
- Impedir o compartilhamento de senhas.
- Descobrir e tratar contas com senhas que não são trocadas por muito tempo.
- Gerenciar de maneira centralizada as credenciais de acesso privilegiado.
- Registrar e auditar os acessos realizados por cada credencial privilegiada.
- Implementar trocas periódicas, programadas e automatizadas de senhas de acordo com necessidade do negócio.
- Proteger sessões estabelecidas na administração de ativos que utilizam credenciais privilegiadas.
- Descobrir contas privilegiadas em sistemas, dispositivos e aplicativos.
- Automaticamente randomizar, gerenciar e guardar senhas e outras credenciais para contas administrativas, de serviço e de aplicativos.
- Automatizar a aplicação de políticas de controle de acesso de contas privilegiadas ao ambiente tecnológico.

Buscando aplicar os devidos controles e reduzir o risco de eventos de grande impacto negativo, o CJF adquiriu uma solução de gerenciamento de acesso privilegiado (PAM, da sigla em inglês) e promoveu a adoção da solução em todo o Judiciário Federal, tendo este TRF4 formalizado a contratação em 2022 por meio do contrato nº 19/2022.

Considerando que a contratação realizada em 2022 não atendeu plenamente às necessidades dos órgãos da Justiça Federal, foi acordado ainda no ano de 2022 pelo Comitê Gestor de TI da Justiça Federal - SIJUS a realização de uma contratação conjunta em 2023, aprovado pelo Secretário-Geral do CJF, para reforçar a quantidade das licenças dos produtos adquiridos, bem como para complementar módulos e principalmente, estender o período de validade das licenças/prestação de serviços para a solução. Tal contratação foi inicialmente idealizada no proc. SEI 0001219-21.2023.4.90.8000 pelo CJF e atribuída a este Tribunal no Plano de Contratações Conjuntas da Justiça Federal.

Ante ao exposto, uma solução de gerenciamento de acesso privilegiado (PAM) adequadamente implementada e configurada é capaz de tratar os cenários de exploração de contas privilegiadas e de reduzir a possibilidade de incidentes de segurança, vazamento de dados ou crises cibernéticas causadas por sequestro de informações (ransomware) e se torna necessária a renovação e expansão de licenciamento de software e serviços das soluções de gerenciamento de acesso privilegiado (PAM) atualmente em uso pelos órgãos da Justiça Federal.

1.3. DEMONSTRATIVO DOS RESULTADOS PRETENDIDOS EM TERMOS DE ECONOMICIDADE E DE MELHOR APROVEITAMENTO DOS RECURSOS HUMANOS, MATERIAIS E FINANCEIROS DISPONÍVEIS (ART. 18, § 1º, IX, DA LEI N. 14.133/2021)

Os resultados a serem alcançados com esta contratação são:

- Rastrear as ações executadas por usuários administradores.
- Impedir o compartilhamento de senhas.
- Descobrir e tratar contas com senhas que não são trocadas a muito tempo.
- Gerenciar de maneira centralizada as credenciais de acesso privilegiado.
- Registrar e auditar os acessos realizados com credenciais privilegiadas.
- Implementar trocas periódicas, programadas e automatizadas de senhas de acordo com necessidade do negócio.

1.4. DEMONSTRAÇÃO DA PREVISÃO DA CONTRATAÇÃO NO PLANO DE CONTRATAÇÕES ANUAL (ART. 18, § 1º, II, DA LEI N. 14.133/2021)

A presente contratação está prevista no Item 13 (Senha Segura) do Plano de Contratações Compartilhadas Anual do Conselho da Justiça Federal para o ano de 2025.

1.5. ALINHAMENTO ENTRE A CONTRATAÇÃO E O PLANEJAMENTO ESTRATÉGICO

A contratação está alinhada com as seguintes diretrizes estratégicas aplicáveis à Justiça Federal:

- Estratégia Nacional do Poder Judiciário 2021-2026 – Resolução CNJ n. 325, de 30 de junho de 2020: Macro desafio do Poder Judiciário: fortalecimento da estratégia nacional de TIC e de proteção de dados.
- Estratégia Nacional de Segurança da Informação do Poder Judiciário – Resolução CNJ n. 396, de 7 de junho de 2021: Objetivos estratégicos: aumentar a resiliência às ameaças cibernéticas, permitir a manutenção e a continuidade dos serviços, ou o seu restabelecimento em menor tempo possível.
- Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário 2021 – 2026 – Resolução CNJ n. 370 de 28 de janeiro de 2021: Objetivo estratégico: aprimorar a Segurança da Informação a Gestão de Dados.
- Plano Estratégico de Tecnologia da Informação da Justiça Federal – Resolução CJF n. 685, de 15 de dezembro de 2020: Objetivo estratégico: promover e fortalecer a segurança da informação digital na Justiça Federal.

1.6. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES (ART. 18, § 1º, XI, DA LEI N. 14.133/2021)

- Contrato CJF nº 050/2021 - Aquisição de solução para Gerenciamento de Acesso Privilegiado (Privileged Access Management - PAM) para proteção dos ambientes computacionais do Conselho da Justiça Federal - CJF, contemplando o licenciamento perpétuo de software e o fornecimento de equipamento(s), serviços de instalação e configuração, transferência de conhecimento, suporte técnico mensal e garantia para 48 (quarenta e oito) meses.
- Contrato nº 0139/2022 - Aquisição de soluções de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados, endpoint e proteção e controle de acesso de usuários privilegiados (PAM), incluindo garantia, serviço de instalação e treinamento. Tribunal Regional Federal da 2ª Região.
- Contrato nº 07.002.10.2022 - Aquisição de soluções de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados, endpoint e proteção e controle de acesso de usuários privilegiados (PAM), incluindo garantia, serviço de instalação e treinamento. Tribunal Regional Federal da 3ª Região.

- Contrato nº 19/2022 - Aquisição de soluções de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados, endpoint e proteção e controle de acesso de usuários privilegiados (PAM), incluindo garantia, serviço de instalação e treinamento. Tribunal Regional Federal da 4ª Região.
- Contrato nº 78/2022 - Aquisição de soluções de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados, endpoint e proteção e controle de acesso de usuários privilegiados (PAM), incluindo garantia, serviço de instalação e treinamento. Tribunal Regional Federal da 5ª Região.

1.7. DEFINIÇÃO DOS REQUISITOS (ART. 18, § 1º, III, DA LEI N. 14.133/2021)

1.7.1. Requisitos de Negócio

1.7.1.1. Necessidade 1: Gerir as credenciais e acessos privilegiados dos órgãos participantes.

1.7.1.1.1. Funcionalidade 1: Identificar, controlar as autorizações, monitorar e auditar as ações realizadas por contas de administração em ativos de TI.

1.7.1.1.1.1. Ator Envolvido 1: Contratada.

1.7.1.1.1.2. Ator Envolvido 2: Área de segurança da informação ou segurança de TI.

1.7.1.1.1.3. Ator Envolvido 3: Área de infraestrutura de TI.

1.7.1.1.1.4. Ator Envolvido 4: Área de desenvolvimento de software.

1.7.1.2. Necessidade 2: Adequar o quantitativo de licenças adquiridas das soluções de gerenciamento de acesso privilegiado para as necessidades atuais dos órgãos participantes.

1.7.1.2.1. Funcionalidade 1: Avaliar a utilização das licenças já adquiridas e indicar a quantidade de licenças complementares necessárias.

1.7.1.2.1.1. Ator Envolvido 1: Contratada.

1.7.1.2.1.2. Ator Envolvido 2: Equipe de planejamento da contratação.

1.7.1.2.1.3. Ator Envolvido 3: Grupo de trabalho do CJF e TRFs.

1.7.1.3. Necessidade 3: Reduzir o custo administrativo para a gestão do contrato dos órgãos participantes.

1.7.1.3.1. Funcionalidade 1: Expandir o período de vigência do contrato para o período de 36 meses, conforme recomendação técnica do grupo de trabalho formado para essa contratação conjunta.

1.7.1.3.1.1. Ator Envolvido 1: Contratada.

1.7.1.3.1.2. Ator Envolvido 2: Gestores de TI.

1.7.1.3.1.3. Ator Envolvido 3: Equipe de planejamento da contratação.

1.7.1.3.1.4. Ator Envolvido 4: Grupo de trabalho do CJF e TRFs

1.7.2. Requisitos Técnicos

1.7.2.1. Necessidade 4: Ampliar as capacidades operacionais necessárias para manter a adequada gestão de privilégios do ambiente tecnológico dos órgãos participantes.

1.7.2.1.1. Funcionalidade 1: Gerenciar as execuções com privilégio de administrador nas estações de trabalho, permitindo autorizar ou negar a elevação de privilégios em aplicações específicas ou para usuários pré-definidos.

1.7.2.1.1.1. Ator Envolvido 1: Contratada.

1.7.2.1.1.2. Ator Envolvido 2: Área de segurança da informação ou segurança de TI.

1.7.2.1.1.3. Ator Envolvido 3: Área de infraestrutura de TI.

1.7.2.1.1.4. Ator Envolvido 4: Área de desenvolvimento de software.

1.7.2.1.2. Funcionalidade 2: Identificar e rotacionar automaticamente senhas de administração local em estações de trabalho.

1.7.2.1.2.1. Ator Envolvido 1: Contratada.

1.7.2.1.2.2. Ator Envolvido 2: Área de segurança da informação ou segurança de TI.

1.7.2.1.2.3. Ator Envolvido 3: Área de infraestrutura de TI.

1.7.2.1.2.4. Ator Envolvido 4: Área de desenvolvimento de software.

1.7.2.1.3. Funcionalidade 3: Controlar, monitorar e auditar os acessos remotos de terceiros, fornecedores ou prestadores de serviço aos ativos de tecnologia da informação de forma granular e segredada, sem a necessidade de interligação de redes ou estabelecimento de VPNs.

1.7.2.1.3.1. Ator Envolvido 1: Contratada.

1.7.2.1.3.2. Ator Envolvido 2: Área de segurança da informação ou segurança de TI.

1.7.2.1.3.3. Ator Envolvido 3: Área de infraestrutura de TI.

1.7.2.1.3.4. Ator Envolvido 4: Área de desenvolvimento de software.

1.7.2.1.4. Funcionalidade 4: Realizar registro individualizado das ações realizadas por contas de administração em servidores de rede e quando tais ações são realizadas e identificar de maneira preditiva os comportamentos anômalos.

1.7.2.1.4.1. Ator Envolvido 1: Contratada.

1.7.2.1.4.2. Ator Envolvido 2: Todos os usuários internos dos serviços de TI (magistrados, servidores, prestadores de serviço).

1.7.2.1.5. Funcionalidade 5: Utilizar solução para gerenciar e proteger automaticamente os segredos (secrets) de usuário e máquinas em ambiente de DevOps, tais como: senhas, tokens, chaves de API e certificados SSL.

1.7.2.1.5.1. Ator Envolvido 1: Contratada.

1.7.2.1.5.2. Ator Envolvido 2: Área de segurança da informação ou segurança de TI.

1.7.2.1.5.3. Ator Envolvido 3: Área de infraestrutura de TI.

1.7.2.1.5.4. Ator Envolvido 4: Área de desenvolvimento de software.

1.7.2.1.6. Funcionalidade 6: Operar em alta disponibilidade de forma a atender os requisitos de continuidade e tolerância a falhas para infraestruturas críticas de TI.

1.7.2.1.6.1. Ator Envolvido 1: Contratada.

1.7.2.1.6.2. Ator Envolvido 2: Área de segurança da informação ou segurança de TI.

1.7.2.1.6.3. Ator Envolvido 3: Área de infraestrutura de TI.

1.7.2.1.6.4. Ator Envolvido 4: Área de desenvolvimento de software.

1.7.3. Requisitos de Manutenção

1.7.3.1. Será prestado suporte técnico em regime ininterrupto (24x7) para o caso de falhas e interrupções do serviço, com direito a atualizações de versões da solução que incorporem correções de defeitos e melhorias implementadas pelo fabricante.

1.7.4. Requisitos de Capacitação

1.7.4.1. Deverá ocorrer a transferência de conhecimento, de forma remota online, das principais funcionalidades da solução para a equipe técnica do TRF4 e dos órgãos partícipes, em turmas de até 10 pessoas, para a administração e conhecimento das tecnologias da solução e com carga horária mínima de 20 horas.

1.7.5. Requisitos de Sustentabilidade Ambiental

1.7.5.1. A CONTRATADA será responsabilizada por qualquer prejuízo que venha causar ao TRF4 por ter suas atividades suspensas, paralisadas ou proibidas por falta de cumprimento de normas ligadas à solução elencada no presente Termo de Referência;

1.7.5.2. A CONTRATADA deverá se atentar às normas em vigor atinentes à sustentabilidade, entre elas:

1.7.5.2.1. 2ª edição do Manual de Sustentabilidade de compras e contratos do Conselho da Justiça Federal, instituído pela Portaria CJF n. 96, de 10 de fevereiro de 2023;

1.7.5.2.2. Guia de Contratações Sustentáveis Nacional;

1.7.5.2.3. Política de Sustentabilidade no âmbito do Poder Judiciário.

1.7.5.3. A CONTRATADA deverá respeitar a legislação vigente e as normas técnicas, elaboradas pela ABNT e pelo INMETRO para aferição e garantia de aplicação dos requisitos mínimos de qualidade e acessibilidade da solução elencada neste Termo de Referência.

1.7.6. Requisitos Legais

1.7.6.1. Requisito 1: Lei nº 14.133, de 1º de abril de 2021, que estabelece normas gerais de licitação e contratação para as Administrações Públicas diretas, autárquicas e fundacionais da União, dos Estados, do Distrito Federal e dos Municípios.

1.7.6.2. Requisito 2: Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais (LGPD).

1.7.6.3. Requisito 3: Resolução CNJ nº 468, de 15 de julho de 2022, que dispõe sobre diretrizes para as contratações de solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça.

1.7.6.4. Requisito 4: Resolução CNJ nº 400, de 16 de junho de 2021, que dispõe sobre a política de sustentabilidade no âmbito do Poder Judiciário.

1.7.6.5. Requisito 5: Resolução CNJ nº 396, de 7 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

1.7.6.6. Requisito 6: Resolução CNJ nº 370, de 28 de janeiro de 2021, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD).

1.7.6.7. Requisito 7: Resolução CNJ nº 347, de 13 de outubro de 2020, que dispõe sobre a Política de Governança das Contratações Públicas no Poder Judiciário.

1.7.6.8. Requisito 8: Resolução CJF nº 685, de 15 de dezembro de 2020, que dispõe sobre o Plano Estratégico de Tecnologia da Informação da Justiça Federal, período 2021-2026.

1.7.6.9. Requisito 9: Resolução CJF n. 6, de 7 de abril de 2008, alterada pela Resolução CF n. 687, de 15 de dezembro de 2020, que dispõe sobre a implantação da Política de Segurança da Informação do Conselho e da Justiça Federal de 1º e 2º graus.

1.8. LEVANTAMENTO DE MERCADO (ART. 18, § 1º, V, DA LEI Nº 14.133/2021)

1.8.1. IDENTIFICAÇÃO DAS SOLUÇÕES

SOLUÇÃO 1 - Manutenção da atual solução de Gerenciamento de Acesso Privilegiado (PAM).

SOLUÇÃO 2 - Aquisição de nova solução de Gerenciamento de Acesso Privilegiado (PAM).

SOLUÇÃO 3 - Contratação de empresa para prestação de serviços de Gerenciamento de Acesso Privilegiado (PAM) no modelo de software como serviço (SaaS).

1.8.2. ANÁLISE COMPARATIVA DAS SOLUÇÕES

SOLUÇÃO 1: Manutenção da atual solução de Gerenciamento de Acesso Privilegiado (PAM).

Alternativa contemplando a complementação de licenças, extensão de validade da garantia e do suporte técnico e adição de funcionalidades complementares para a solução de gestão de acesso privilegiado atualmente em uso na Justiça Federal.

Neste cenário poderiam ser renovados a garantia e suporte técnico da solução Senha Segura adquiridos pelos órgãos da Justiça Federal partícipes e a expansão da solução por meio da aquisição complementar de licenças. Neste caso, é oportuno que se permita também a possibilidade de aquisição de licenças adicionais necessárias para a execução de funções complementares, também relacionadas ao gerenciamento de credenciais e privilégios, tais como: a escalação de privilégios em estações de trabalho, gestão de segredos em ambiente de contêiner e de acesso remoto seguro de terceiros. Assim, a intenção de compra contemplaria licenças perpétuas adicionais para os itens em utilização, para funcionalidades adicionais e renovação de suporte técnico e garantia pelo período de 36 meses das licenças adquiridas. A eventual contratação se daria conforme as necessidades de cada órgão. Essa solução preserva o investimento realizado na aquisição da solução bem como o conhecimento técnico adquirido pelo quadro de servidores no uso da solução.

SOLUÇÃO 2: Aquisição de nova solução de Gerenciamento de Acesso Privilegiado (PAM).

Nesta alternativa seria registrada intenção de compra, em que seriam detalhadas todas as especificações técnicas da solução, em que seriam permitidas a substituição completa da solução de gestão de acesso privilegiado. Nessa solução também devem ser considerados os custos de instalação, configuração e treinamento.

SOLUÇÃO 3: Contratação de empresa para prestação de serviços de Gerenciamento de Acesso Privilegiado (PAM) no modelo de software como serviço (SaaS).

Esta alternativa considera a contratação de empresa para a prestação de serviços de gerenciamento de acesso na modalidade SaaS (Software como Serviço) para proteção dos ambientes computacionais dos órgãos da Justiça Federal. Na modalidade de software como serviço toda a infraestrutura (software e hardware) é disponibilizada pela empresa contratada.

1.8.3. QUADRO COMPARATIVO ENTRE AS SOLUÇÕES APRESENTADAS

Requisito	Solução	Sim	Não	Não se aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública	ID 1	X	-	-
A Solução encontra-se implantada em outro órgão ou entidade da Justiça Federal?	ID 1	X	-	-
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	ID 1	-	X	-
A Solução é composta por software livre ou software público? (quando se tratar de software)	ID 1	-	X	-
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	ID 1	-	-	X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	ID 1	-	-	X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	ID 1	-	-	X

1.8.4. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

1.8.4.1. Alternativa 2: Aquisição de nova solução de Gerenciamento de Acesso Privilegiado (PAM).

A aquisição de uma nova solução foi descartada por deliberação do encontro das seções judiciárias. A troca total do parque demanda um elevado tempo de implementação com a execução de tarefas complexas de migração de dados e integração com sistemas. Também apresenta uma elevada curva de aprendizado para utilização da solução assim como não preserva o investimento já realizado na aquisição da solução atualmente em uso na Justiça Federal.

1.8.4.2. Alternativa 3: Contratação de empresa para prestação de serviços de Gerenciamento de Acesso Privilegiado (PAM) no modelo de software como serviço (SaaS).

A opção foi descartada em função dos riscos de segurança da informação e de continuidade de negócio bem como pela aquisição anterior de solução com fornecimento de licenças perpétuas.

1.8.5. PESQUISA DE PREÇOS DE MERCADO

PARTNUMBER	DESCRIÇÃO	TOTAL	Proposta 1*	Proposta 2*	Proposta 3*

SS-COFRE	Usuários que farão acesso ao SenhaSegura, pelo período de 36 meses	586	R$ 2.506,50	R$ 2.435,00	R$ 3.090,00
RNV-SS-COFRE	Renovação usuários que farão acesso ao SenhaSegura, pelo período de 36 meses	374	R$ 1.416,60	R$ 1.550,00	R$ 1.500,00
SS-SRVPASWCHG	Servidores físicos ou virtuais para 36 meses	3580	R$ 817,60	R$ 820,00	R$ 800,00
RNV-SS-SRVPASWCHG	Renovação Servidores físicos ou virtuais para 36 meses	3275	R$ 48,60	R$ 45,00	R$ 50,00
SS-NETPASWCHG	Dispositivos de rede como firewalls, roteadores, balanceadores e afins para 36 meses	1160	R$ 791,40	R$ 795,00	R$ 880,00
RNV-SS-NETPASWCHG	Renovação Dispositivos de rede como firewalls, roteadores, balanceadores e afins para 36 meses	2285	R$ 34,00	R$ 33,00	R$ 35,00
SS-WINPASWCHG	Estações de trabalho ou workstation para troca de senha de admin ou root para 36 meses	8280	R$ 17,80	R$ 22,00	R$ 22,00
SS-SESWEB	Módulo que habilita a gravação de sessão e auditoria de comandos para 36 meses	544	R$ 2.438,60	R$ 2.575,00	R$ 2.498,00
RNV-SS-SESWEB	Renovação Módulo que habilita a gravação de sessão e auditoria de comandos para 36 meses	871	R$ 1.362,00	R$ 1.495,00	R$ 1.449,00
SS-A2A	Aplicações hardcode (API) para 36 meses	500	R$ 2.578,20	R$ 2.775,00	R$ 2.549,00
RNV-SS-A2A	Renovação Aplicações hardcode (API) para 36 meses	32	R$ 1.888,60	R$ 1.900,00	R$ 1.890,00
SS-JUMPSERVER	Acesso via Jump Server via SSH/RDP para 36 meses	3	R$ 65.745,80	R$ 55.999,00	R$ 65.880,00
RNV-SS-JUMPSERVER	Renovação Acesso via Jump Server via SSH/RDP para 36 meses	3	R$ 13.000,00	R$ 15.000,00	R$ 15.549,00
SS-SSG.GO-WIN	Estações de trabalho WINDOWS que utilizarão o gerenciamento de elevação de privilégios para 36 meses	8160	R$ 151,04	R$ 150,20	R$ 149,00
SS-SSG.GO-LIN	Estações de trabalho LINUX que utilizarão o gerenciamento de elevação de privilégios para 36 meses	420	R$ 207,64	R$ 195,50	R$ 229,00
SS-DSM-A2A	Aplicações em containers (DevOps) para 36 meses	445	R$ 4.400,56	R$ 4.450,00	R$ 4.590,00
RNV-SS-DSM-A2A	Renovação Aplicações em containers (DevOps)	14	R$ 7.153,22	R$ 7.125,00	R$ 7.590,00
SS-CERT-AUTO	Certifcados completo com automação para 36 meses	400	R$ 4.000,00	R$ 3.900,00	R$ 4.280,00
SS-DOMUM	Usuários terceiros ou externos que farão o acesso seguro sem a necessidade de VPN ao senhasegura para 36 meses	520	R$ 4.302,28	R$ 4.100,00	R$ 4.290,00
SS-HA/DR	Instância de contingência adicional além de produção para 36 meses	3	R$ 185.833,04	R$ 200.000,00	R$ 199.480,00
RNV-SS-HA/DR	Renovação Instância de contingência adicional além de produção	11	R$ 13.909,18	R$ 16.000,00	R$ 14.980,00
PS-IMP-STD-CB	Implantação PAM	11	R$ 80.000,00	R$ 120.000,00	R$ 69.980,00
PS-HR	Horas de professional services	1800	R$ 900,00	R$ 800,00	R$ 789,00
N/A	Suporte Tecnico Especializado	468	R$ 14.500,00	R$ 12.500,00	R$ 12.890,00
		TOTAL	R$ 27.538.336,58	R$ 27.099.334,00	R$ 27.272.033,00

1.9. JUSTIFICATIVA DA ESCOLHA DA ALTERNATIVA DE SOLUÇÃO A CONTRATAR

1.9.1. ALTERNATIVA/SOLUÇÃO ESCOLHIDA: MANUTENÇÃO DA ATUAL SOLUÇÃO DE GERENCIAMENTO DE ACESSO PRIVILEGIADO (PAM).

1.9.1.1. BENS/SERVIÇOS

1.9.1.1.1. Licenças;

1.9.1.1.2. Manutenção de licenças;

1.9.1.1.3. Serviços de implantação;

1.9.1.1.4. Serviços técnicos profissionais;

1.9.1.1.5. Serviços de suporte técnico.

1.9.1.2. CUSTO ESTIMADO

1.9.1.2.1. O valor total estimado para aquisição pelos órgãos partícipes é de R$ 25.962.168,30*.

* Estimativa baseada no menor custo individual apresentado para cada item.

1.9.1.3. JUSTIFICATIVA

1.9.1.3.1. Buscando aplicar os devidos controles e reduzir o risco de eventos de grande impacto negativo, o CJF adquiriu uma solução de gerenciamento de acesso privilegiado (PAM, da sigla em inglês) e promoveu a adoção da solução em todo o Judiciário Federal, tendo este TRF4 formalizado a contratação em 2022 por meio do contrato nº 19/2022.

A manutenção da solução Senha Segura apresenta vantagens consideráveis. Inicialmente, deve-se destacar a maturidade e estabilidade operacional da plataforma implementada. Desde sua instalação, o sistema passou por um ciclo de depuração e ajustes, resultando em um ambiente operacional estável e adaptado às particularidades da Justiça Federal. A substituição introduziria um novo ciclo de implantação, inerentemente sujeito a instabilidades e desafios de configuração.

A preservação das integrações e customizações específicas ao ambiente da Justiça Federal é um fator crucial. Soluções PAM demandam integrações complexas com sistemas legados, diretórios de identidade e infraestrutura de rede. O esforço despendido para

integrar e customizar a Solução PAM seria perdido, exigindo um novo e custoso processo com uma nova solução, com riscos de incompatibilidade e retrabalho.

Da mesma forma, a manutenção das políticas de acesso, dos fluxos de aprovação e os mecanismos de controle já implementados e refinados ao longo do tempo é essencial para evitar o retrabalho e a necessidade de reconstruir e validar todo o arcabouço de segurança de acessos privilegiados.

Também, a retenção do conhecimento técnico e da curva de aprendizado dos usuários também é um fator importante para a continuidade. As equipes técnicas e os usuários finais já possuem familiaridade com os processos, interfaces e funcionalidades da ferramenta existente. Uma nova plataforma implicaria na necessidade de capacitação na nova solução, com impacto na produtividade e potencial aumento de erros operacionais durante a fase de adaptação.

Do ponto de vista econômico, a manutenção da solução Senha Segura mostra-se mais vantajosa. O principal argumento reside na otimização do retorno sobre o investimento previamente realizado na aquisição da Solução. A substituição prematura da plataforma resultaria na subutilização do capital já empregado, interrompendo a amortização do investimento inicial. A contratação de uma nova solução PAM incorreria em despesas significativas com licenças, hardware, de serviços especializados de consultoria para implementação, customização e migração, que frequentemente superam os custos de manutenção da solução existente, de treinamento e de retenção do conhecimento.

Deve-se ressaltar ainda a eliminação dos custos e riscos associados à migração de dados. Projetos de migração de dados de sistemas críticos como PAM são notórios por sua complexidade, demandando horas de trabalho especializado e apresentando riscos de perda de dados ou inconsistências, com impactos financeiros diretos e indiretos.

Em suma, a manutenção da solução de Gerenciamento de Acesso Privilegiado Senha Segura pela Justiça Federal, do ponto de vista técnico, assegura a estabilidade operacional, preserva integrações e customizações essenciais, retém o conhecimento adquirido e garante a continuidade da segurança e conformidade. Economicamente, otimiza o investimento já realizado, evita custos substanciais de aquisição, migração e treinamento, e mitiga riscos financeiros associados à transição para uma nova plataforma.

1.10. DESCRIÇÃO DA SOLUÇÃO DE TI A SER CONTRATADA (ART. 18, § 1º, VII, DA LEI Nº 14.133/2021)

1.10.1. Solução para Gerenciamento de Acesso Privilegiado (*Privileged Access Management - PAM*) para proteção dos ambientes computacionais dos órgãos da Justiça Federal partícipes, contemplando licenciamento perpétuo de software e fornecimento de equipamento(s), serviços de instalação e configuração, suporte técnico mensal e garantia para 36 (trinta e seis) meses.

1.11. DA INDICAÇÃO DA MARCA

1.11.1. Conforme demonstrado neste estudo técnico preliminar, a manutenção da Solução para Gerenciamento de Acesso Privilegiado (*Privileged Access Management - PAM*) já implementada é a solução mais vantajosa para a Justiça Federal, tanto técnica quanto economicamente, de forma que a indicação da marca/fabricante é essencial para garantir a continuidade e compatibilidade com plataformas e padrões já adotados pela administração.

1.11. RELAÇÃO ENTRE A DEMANDA PREVISTA E A QUANTIDADE DE BENS E/OU SERVIÇOS A SEREM CONTRATADOS (ART. 18, § 1º, IV, DA LEI Nº 14.133/2021)

1.11.1. Renovação dos serviços de manutenção das licenças que compõem o atual parque da solução de gerenciamento de acesso privilegiado e dos serviços de suporte técnico:

PARTNUMBER	DESCRIÇÃO	CJF	TRF2	TRF3	TRF4	JFRS	JFSC	JFPR	TRF5	JFAL	JFPE	JFPB	JFRN	JFSE	TOTAL
RNV-SS-COFRE	Renovação usuários que farão acesso ao SenhaSegura, pelo período de 36 meses	0	40	80	43	31	40	60	22	12	24	8	7	7	374
RNV-SS-SRVPASWCHG	Renovação Servidores fisicos ou virtuais para 36 meses	0	350	500	650	410	400	315	260	60	130	70	70	60	3275
RNV-SS-NETPASWCHG	Renovação Dispositivos de rede como firewalls, roteadores, balanceadores e afins para 36 meses	0	500	500	120	170	100	295	200	30	190	60	60	60	2285
RNV-SS-SESWEB	Renovação Módulo que habilita a gravação de sessão e auditoria de comandos para 36 meses	0	40	40	45	31	400	315	0	0	0	0	0	0	871
RNV-SS-A2A	Renovação Aplicações hardcode (API) para 36 meses	0	2	10	0	0	0	0	5	0	0	5	5	5	32
RNV-SS-JUMPSERVER	Renovação Acesso via Jump Server via SSH/RDP para 36 meses	0	1	0	1	1	0	0	0	0	0	0	0	0	3
RNV-SS-DSM-A2A	Renovação Aplicações em containers (DevOps)	0	2	2	0	0	0	0	5	0	0	0	5	0	14
RNV-SS-HA/DR	Renovação Instância de contingência adicional além de produção	0	1	1	1	0	1	1	1	1	1	1	1	1	11
N/A	Suporte Tecnico Especializado	36	36	36	36	36	36	36	36	36	36	36	36	36	468

1.11.2. Aquisição de novas licenças para ampliação do parque, serviços de implantação e serviços técnicos profissionais:

PARTNUMBER	DESCRIÇÃO	CJF	TRF2	TRF3	TRF4	JFRS	JFSC	JFPR	TRF5	JFAL	JFPE	JFPB	JFRN	JFSE	TOTAL
SS-COFRE	Usuários que farão acesso ao SenhaSegura, pelo período de 36 meses	20	160	120	60	19	10	0	58	28	58	17	18	18	586

SS-SRVPASWCHG	Servidores físicos ou virtuais para 36 meses	350	1350	200	50	0	100	0	540	90	500	130	130	140	3580
SS-NETPASWCHG	Dispositivos de rede como firewalls, roteadores, balanceadores e afins para 36 meses	20	150	200	30	0	150	0	200	30	210	60	50	60	1160
SS-WINPASWCHG	Estações de trabalho ou workstation para troca de senha de admin ou root para 36 meses	0	200	8000	0	0	30	50	0	0	0	0	0	0	8280
SS-SESWEB	Módulo que habilita a gravação de sessão e auditoria de comandos para 36 meses	20	60	60	45	19	100	100	40	20	41	13	13	13	544
SS-A2A	Aplicações hardcode (API) para 36 meses	50	0	0	100	100	100	100	10	10	15	5	5	5	500
SS-JUMPSERVER	Acesso via Jump Server via SSH/RDP para 36 meses	0	0	0	1	0	1	1	0	0	0	0	0	0	3
SS-SSG.GO-WIN	Estações de trabalho WINDOWS que utilizarão o gerenciamento de elevação de privilégios para 36 meses	0	100	8000	0	0	30	30	0	0	0	0	0	0	8160
SS-SSG.GO-LIN	Estações de trabalho LINUX que utilizarão o gerenciamento de elevação de privilégios para 36 meses	0	100	300	0	0	10	10	0	0	0	0	0	0	420
SS-DSM-A2A	Aplicações em containers (DevOps) para 36 meses	65	0	0	0	100	100	100	30	10	20	10	5	5	445
SS-CERT-AUTO	Certifcados completo com automação para 36 meses	0	0	0	100	100	100	100	0	0	0	0	0	0	400
SS-DOMUM	Usuários terceiros ou externos que farão o acesso seguro sem a necessidade de VPN ao senhasegura para 36 meses	40	10	150	20	40	50	30	30	30	30	30	30	30	520
SS-HA/DR	Instância de contingência adicional além de produção para 36 meses	0	0	0	0	1	1	1	0	0	0	0	0	0	3
PS-IMP-STD-CB	Implantação PAM	1	1	1	1	1	0	0	1	1	1	1	1	1	11
PS-HR	Horas de professional services	0	200	200	100	100	300	300	100	100	100	100	100	100	1800

1.12. ESTIMATIVA PRELIMINAR DO CUSTO TOTAL DE CONTRATAÇÃO (ART. 18, § 1º, VI, DA LEI Nº 14.133/2021)

Custo total estimado por órgão partícipe	
Órgão	Valor Estimado
CNJ - Conselho Nacional de Justiça	R$ 1.490.766,40
TRF2 - Tribunal Regional Federal da 2ª Região	R$ 2.679.746,38
TRF3 - Tribunal Regional Federal da 3ª Região	R$ 3.696.479,18
TRF4 - Tribunal Regional Federal da 4ª Região	R$ 1.883.680,98
TRF5 - Tribunal Regional Federal da 5ª Região	R$ 1.816.883,18
JFAL - Justiça Federal em Alagoas	R$ 1.038.667,98
JFPB - Justiça Federal na Paraíba	R$ 1.043.026,38
JFPE - Justiça Federal em Pernambuco	R$ 1.715.560,38
JFPR - Justiça Federal no Paraná	R$ 2.939.508,22
JFRN - Justiça Federal no Rio Grande do Norte	R$ 1.049.752,98
JFRS - Justiça Federal no Rio Grande do Sul	R$ 2.249.464,04
JFSC - Justiça Federal em Santa Catarina	R$ 3.329.040,22
JFSE - Justiça Federal em Sergipe	R$ 1.029.591,98
TOTAL	R$ 25.962.168,30

1.13. NECESSIDADE DE ADEQUAÇÃO DO AMBIENTE DO ÓRGÃO PARA VIABILIZAR A EXECUÇÃO CONTRATUAL (ART. 18, § 1º, X, DA LEI Nº 14.133/2021)

1.13.1. Não há necessidade de adequação do ambiente tendo em vista que a solução já está em uso e operará nos ambientes computacionais existentes.

1.14. JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DO OBJETO (ART. 18, § 1º, VIII, DA LEI Nº 14.133/2021)

1.14.1. O objeto da contratação compreende o fornecimento de licenças e plano de manutenção e suporte técnico de software de gerenciamento de acesso privilegiado, bem como de serviços de implantação e serviços técnicos especializados na solução.

Inicialmente, deve-se destacar a inviabilidade econômica do parcelamento. É notório no mercado de TIC, especialmente em relação à comercialização de software, o modelo que oferece menores preços em razão do volume de aquisição. Além disso, deve-se considerar o aumento nos custos de gestão de diversas contratações. Dessa forma, a divisão em itens levaria à perda de economia de escala.

Da mesma forma, deve-se considerar o prejuízo ao conjunto da solução e da contratação. Considerando-se a necessidade de continuidade e de ampliação da solução, é essencial buscar assegurar a uniformização do licenciamento e a prestação concomitante de serviços de implantação para as novas funcionalidades, do suporte técnico e dos serviços profissionais especializados, de forma a evitar a fragmentação de responsabilidade entre fornecedores, uma vez que pode comprometer o funcionamento da solução como um todo.

1.15. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO (ART. 18, § 1º, XIII, DA LEI Nº 14.133/2021)

1.15.1. No âmbito deste Tribunal, as atividades judicante e administrativa são amparadas fortemente no uso de soluções de TI - equipamentos, softwares e sistemas de informação - que se tornaram vitais para o funcionamento e melhoria dos serviços prestados ao jurisdicionado. Como consequência, a proteção do ambiente tornou-se fator essencial para manutenção da disponibilidade e estabilidade dos serviços de TI e do funcionamento do Tribunal, bem como para manutenção da confidencialidade, integridade, disponibilidade e autenticidade dos dados.

O uso de soluções de TI no Poder Judiciário provocou uma mudança significativa nos processos internos de trabalho e contribuiu para aumentar a celeridade e produtividade na prestação jurisdicional, bem como assegurou o amplo acesso à Justiça. Atualmente são disponibilizados através da rede mundial de computadores, tanto para o público interno como externo, diversos sistemas e serviços acessíveis por dispositivos como computadores, *tablets* ou celulares.

Por conseguinte, a expansão da utilização da internet com a interconexão de instituições, corporações e pessoas, e o tráfego imenso de informações na rede provocou o interesse de pessoas mal-intencionadas visando à obtenção de vantagens financeiras, coleta de informações confidenciais, prática de vandalismo e golpes, realização de ataques ou a mera disseminação de mensagens indesejadas ou informação falsas.

Em movimento paralelo à expansão da utilização dos recursos tecnológicos, constata-se o aumento dramático de ataques a sistemas computacionais, com incidência acelerada desde a eclosão da pandemia, afetando instituições do Poder Judiciário, como Superior Tribunal de Justiça, Tribunal de Justiça do Rio Grande do Sul, Tribunal Regional Federal da 3ª Região e Justiça Federal de Pernambuco. Frente a essa crise cibernética, esta Corte tem adotado inúmeras providências, como reorganização da rede de computadores, aumento de soluções de segurança, adoção de segundo fator de autenticação (2FA) para os principais sistemas.

De fato, o emprego de 2FA consiste em estratégia de segurança das mais poderosas para evitar a má utilização de credenciais de usuários, principalmente os de elevados poderes nas infraestruturas computacionais. Para tanto, uma das estratégias para a implantação do segundo fator de autenticação consiste em adquirir uma solução de cofre de senhas, mecanismo pelo qual é possível implantar 2FA para acesso aos principais ativos computacionais, principalmente naqueles que constituem a infraestrutura computacional da corte. Para esses, torna-se necessário o monitoramento de acessos aos dados armazenados, gerenciamento e auditoria do repositório de usuários e ações proativas em casos de incidentes de segurança cibernética, ataque de *malwares* ou até identificação de acessos indevidos de usuários internos mal intencionados.

Por essa razão, torna-se essencial a adequada proteção dos ambientes computacionais do TRF4 com o gerenciamento das credenciais privilegiadas disponibilizadas no ambiente. Como credenciais de acesso privilegiadas entende-se contas que permitem acesso com maior nível de recursos aos ambientes tecnológicos que hospedam os sistemas computacionais da Justiça Federal.

Buscando aplicar os devidos controles e reduzir o risco de eventos de grande impacto negativo, o CJF adquiriu uma solução de gerenciamento de acesso privilegiado (PAM, da sigla em inglês) e promoveu a adoção da solução em todo o Judiciário Federal, tendo este TRF4 formalizado a contratação em 2022 por meio do contrato nº 19/2022.

De acordo com os estudos realizados a manutenção da atual solução de gerenciamento de acesso privilegiado mostra-se mais vantajosa para a Administração pelos seguintes motivos:

- Eficácia: A atual solução de gerenciamento de credenciais privilegiadas está implementada e em funcionamento na infraestrutura de TI dos órgãos partícipes, restando apenas o acréscimo de algumas funcionalidades para prover a plena capacidade operacional.

- Eficiência: A manutenção da atual solução dispensa o tempo de implementação necessário para a instalação de uma nova solução e o tempo de aprendizado para o uso da solução.

- Efetividade: A solução proposta atenderá às necessidades específicas do órgão, proporcionando uma infraestrutura de gerenciamento de acesso privilegiado robusto e confiável.

- Economicidade: Aproveitamento do investimento já realizado na aquisição da solução (hardware e software) e em capacitação, assim como dispensa os custos de migração.

1.15.2. Benefícios Esperados:

A implementação da solução proposta trará os seguintes benefícios:

- Estabelecer o controle de acesso aos ativos de informação, em cumprimento a Resolução TRF4 73/2021;
- Cumprir a Portaria CNJ 162/2021 - Estratégia Nacional de Segurança Cibernética do Poder Judiciário;
- Conformidade com a Lei Geral de Proteção de Dados;
- Redução de cenários de exploração de contas privilegiadas;
- Redução da possibilidade de crises cibernéticas causadas por sequestro informações (ransomware) por criminosos cibernéticos;
- Redução na utilização das mesmas senhas em várias contas de serviço;
- Manutenção de índices de satisfação dos clientes internos e externos com os serviços e sistema de TI;
- Atendimento de objetivos estratégicos da Justiça Federal da 4ª Região.

Assim, a equipe de planejamento da contratação declara viável a contratação de manutenção e ampliação da atual solução de gerenciamento de acesso privilegiado, estando alinhada com objetivos estratégicos da Justiça Federal e demonstrada a vantajosidade técnica e econômica da solução.

1.16. MARGEM DE PREFERÊNCIA

1.16.1. Não se aplica a Lei 8.248/1991, pois não há previsão em seu art. 16-A de serviços relacionados à solução de gerenciamento de acesso privilegiado. Consequentemente, afasta-se a aplicação do Decreto 7.174/2010, o qual regulamenta a lei supracitada.

1.16.2. Não se aplica o Decreto Nº 8.538/2015, pois o tratamento diferenciado e simplificado para as microempresas e as empresas de pequeno porte não é vantajoso para a administração pública e pode representar prejuízo ao conjunto ou ao complexo do objeto a ser contratado.

2. PLANO DE SUSTENTAÇÃO E TRANSIÇÃO CONTRATUAL

2.1. RECURSOS MATERIAIS E HUMANOS NECESSÁRIOS À EXECUÇÃO CONTRATUAL

2.1.1. Equipe de ficalização:

2.1.1.1. Gestor do contrato: dedicação estimada em aproximadamente 10h/mês.

2.1.1.2. Fiscal técnico: dedicação estimada em aproximadamente 15h/mês.

2.1.1.3. Fiscal administrativo: dedicação estimada em aproximadamente 5h/mês.

2.2. CONTINUIDADE DO FORNECIMENTO DA SOLUÇÃO DE TIC EM CASO DE EVENTUAL INTERRUPÇÃO CONTRATUAL

2.2.1. Em caso de interrupção no fornecimento da solução de TIC, o CONTRATANTE deverá realizar a contratação de um novo fornecedor.

2.2.2. Deverá ser exigida da fornecedora a apresentação de garantia de execução contratual para resguardar eventuais danos em caso de interrupção no fornecimento da solução de TIC.

2.3. ATIVIDADES DE TRANSIÇÃO CONTRATUAL E DE ENCERRAMENTO DO CONTRATO

2.3.1. Em até 3 (três) meses antes do término da vigência do contrato deverá ser realizada avaliação da solução de gerenciamento de acesso privilegiado e a verificação dos objetivos alcançados para fins de encaminhamento para manutenção da solução ou contratação de um novo produto.

2.3.2. Ao término da vigência do contrato, o CONTRATANTE deverá revogar os perfis de acesso concedidos à CONTRATADA necessários à execução dos serviços.

2.4. ESTRATÉGIA DE INDEPENDÊNCIA

2.4.1. Não se verifica na presente contratação uma relação de dependência à solução de gerenciamento de acesso privilegiado uma vez que há no mercado outros fabricantes que aptos a atenderem a demanda institucional. Para a presente contratação foi demonstrada nos estudos técnicos preliminares a manutenção da atual solução de forma a preservar os investimentos realizados e otimizar o custo total de propriedade da solução.

De toda forma, alguns requisitos são adotados para resguardar o funcionamento da solução e a dependência do fornecedor, tais como:

- Adoção do modelo de licenciamento perpétuo para assegurar que a solução continue funcional mesmo após o término da vigência do contrato.

- Garantia e suporte técnico do fabricante.

- Fiscalização diligente do contrato e da qualidade das entregas pela equipe técnica interna.

Documento assinado eletronicamente por **HENRIQUE MARCELINO CASSOL**, **Diretor de Tecnologia da Informação, em exercício**, em 05/06/2025, às 15:49, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **TAUAME AGUIAR PACCE**, **Diretor da Divisão de Infraestrutura e Segurança da Informação**, em 05/06/2025, às 15:59, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **JORGE LUIZ PIRES DE SOUZA**, **Diretor do Núcleo de Compras e Pesquisa de Preços**, em 05/06/2025, às 17:56, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://www.trf4.jus.br/trf4/processos/verifica.php informando o código verificador **7393585** e o código CRC **08BD7751**.