TERMO DE REFERÊNCIA

1. Definição do objeto

1.1. Contratação 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, de acordo com as especificações técnicas contidas neste Termo de Referência e anexos.

1.2. A contratação será dividida em itens, conforme tabela apresentada a seguir.

Item	Especificação	Unidade	Quantidade
1.	Solução para Gerenciamento de Acesso Privilegiado com licenciamento perpétuo de *software* e fornecimento de equipamento(s)	Solução	1
2.	Serviços de instalação e configuração	Serviço	1
3.	Serviço de suporte técnico mensal	Meses	48
4.	Transferência de conhecimento	Participante	6

1.3. Requisitos técnicos do objeto

1.3.1. Os requisitos técnicos são apresentados no ANEXO I - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO deste Termo de Referência.

1.4. Natureza do objeto a ser contratado

1.4.1. A natureza do objeto desta contratação possui caráter comum, pois enquadra-se no disposto no parágrafo único do art. 1º da Lei 10.520, de 17 de julho de 2002, a saber: “consideram-se bens e serviços comuns, para os fins e efeitos deste artigo, aqueles cujos padrões de desempenho e qualidade possam ser

objetivamente definidos pelo edital, por meio de especificações usuais no mercado".

1.4.2. No caso de contratações de TI, deve-se destacar o Acórdão 2.471/2008-TCU-Plenário, no qual ficou deliberado que (9.2.2) "devido à padronização existente no mercado, os bens e serviços de tecnologia da informação geralmente atendem a protocolos, métodos e técnicas pré-estabelecidos e conhecidos e a padrões de desempenho e qualidade que podem ser objetivamente definidos por meio de especificações usuais no mercado. Logo, via de regra, esses bens e serviços devem ser considerados comuns para fins de utilização da modalidade Pregão".

1.4.3. Assim, a solução para Gerenciamento de Acesso Privilegiado enquadra-se na definição de serviço comum, pois é descrito neste Termo de Referência de forma objetiva e bem definida, inclusive contendo cláusulas referentes a Acordos Mínimos de Serviço, os quais oferecem métricas reais para avaliação analítica da qualidade do serviço prestado pela CONTRATADA.

2. Fundamentação da contratação

2.1. Motivação da contratação

2.1.1. 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 órgão dos 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 premência da atuação preventiva para tratar as brechas de segurança.

2.1.2. 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. Este uso é rotineiro por técnicos, contas de serviços e aplicações. A utilização de credenciais com privilégios especiais para a administração do ambiente é requisito de segurança básico para a manutenção das operações diárias da Secretaria de TI.

2.1.3. No entanto, se tais credenciais não forem adequadamente protegidas, seria possível que um atacante externo ou um eventual prestador de serviço descontente, conquistar o controle de ativos da infraestrutura de TI do CJF, desabilitar controles de segurança, sequestrar informação confidencial ou sensível, criptografar dados, deletar cópias de segurança (*backups*) e assim interromper o funcionamento do órgão. A exploração de credenciais privilegiadas tem ocorrido na ampla maioria das invasões de grande impacto contra organizações governamentais e privadas.

2.1.4. Buscando aprimorar estes controles, a Comissão Local de Segurança da Informação do CJF buscou nortear questões relacionadas à proteção da informação no órgão por meio da normatização dos documentos acessórios da Política de Segurança da Informação da Justiça Federal. Na Política de Controle de Acesso Lógico (Portaria n. 279 de 19 de agosto de 2013) vedou-se a utilização de contas de acesso genéricas ou de uso compartilhado, restringiu-se o uso de contas privilegiadas e estabeleceu-se a necessidade de registro de todas as ações e acessos para fins de auditoria. Tais regras têm por objetivo permitir o rastreio dos acessos, individualizar as ações executadas nos sistemas para fins de auditoria e responsabilização, bem como a gestão adequada dos privilégios de acesso adequados.

2.1.5. Contudo, verifica-se que as áreas que administram o ambiente de infraestrutura de TI têm enfrentado dificuldades práticas para a implementação dos controles de acesso previstos na Política de Segurança da Informação, principalmente no que tange ao acesso privilegiado ao ambiente por parte de prestadores terceirizados. A utilização de contas privilegiadas genéricas e de uso compartilhado, aumentam significativamente a percepção de exposição a essas ameaças.

2.2. Objetivos a serem alcançados

2.2.1. Rastrear as ações executadas por usuários administradores.

2.2.2. Impedir o compartilhamento de senhas.

2.2.3. Descobrir e tratar contas com senhas que não são trocadas por muito tempo.

2.2.4. Gerenciar de maneira centralizada as credenciais de acesso privilegiado do CJF.

2.2.5. Registrar e auditar os acessos realizados com credenciais privilegiadas.

2.2.6. Implementar trocas periódicas, programadas e automatizadas de senhas de acordo com necessidade do negócio.

2.3. Benefícios diretos e indiretos

2.3.1. Dar cumprimento à Portaria CJF n. 279/2019 (Política de Controle Acesso Lógico);

2.3.2. Dar cumprimento aos Protocolos de Segurança Cibernética editados pelo CNJ.

2.3.3. Conformidade com a Lei Geral de Proteção de Dados - LGPD;

2.3.4. Conformidade com as melhores práticas da Segurança da informação;

2.3.5. Diminuição de cenários de exploração de contas privilegiadas;

2.3.6. Automatização na aplicação de políticas de controle de acesso de contas privilegiadas do ambiente de TI.

2.3.7. Redução do risco de uso de credenciais compartilhadas e por prestadores de serviços desligados;

2.3.8. Redução da possibilidade de crises cibernéticas causadas por sequestro informações (*ransomware*) por criminosos cibernéticos.

2.3.9. Redução na utilização das mesmas senhas em várias contas de serviço;

2.3.10. Controle operacional do uso de credenciais privilegiadas.

2.4. Alinhamento entre a contratação e o Plano Estratégico Institucional e/ou de TIC

2.4.1. Esta contratação está alinhada aos objetivos estratégicos traçados no Plano Estratégico de Tecnologia da Informação da Justiça Federal (PETI-JF 2021/2026) e metas definidas no Plano Diretor de Tecnologia da Informação do CJF (PDTI 2021-2023) conforme apresentado a seguir:

2.4.1.1. Conforme PETI-JF 2021/2026, essa contratação está alinhada ao Macrodesafio do Poder Judiciário “Fortalecimento da Estratégia Nacional de TIC e de Proteção de Dados”

2.4.1.2. Conforme PETI-JF 2021/2026, essa contratação está alinhada aos objetivos estratégicos da Justiça Federal de: “Promover e fortalecer a segurança da informação digital na Justiça Federal” e “Aperfeiçoar e Assegurar a efetividade dos serviços de TI para a Justiça Federal”;

2.4.1.3. Conforme PDTI-CJF 2021/2023, esta contratação está alinhada à iniciativa estratégica “INIC-2021-015 - Aprimorar a Segurança da Informação do CJF e da JF”;

2.4.2. Esta contratação está prevista no Plano de Contratação de Soluções de TI - 2021 do Conselho da Justiça Federal - CJF. Portaria Secretaria-Geral nº 524 de 23/11/2020, disponível na página de Governança de TI do Portal do CJF.

2.5. Referência aos Estudos Preliminares de STIC

2.5.1. Este Termo de Referência foi elaborado considerando o Documento de Oficialização da Demanda – DOD SEI n. 0178883 e os estudos técnicos preliminares - ETP acostados ao processo ao SEI n. 0004481-11.2020.4.90.8000.

2.6. Relação entre a demanda prevista e a quantidade de bens e/ou serviços a serem contratados

2.6.1. A solução abrange licenças e agentes para todo o parque computacional do CJF.

2.6.2. O quantitativo de usuários indicados na especificação técnica para a solução de gerenciamento de acesso considera o quadro de servidores da Secretaria de Tecnologia da Informação que acessam os servidores com contas privilegiadas.

2.6.3. O quantitativo previsto para os módulos de elevação de privilégio de servidores e estações de trabalho Windows e Linux) foram calculados com base no total desses dispositivos atualmente em utilização.

2.6.4. O serviço de instalação e configuração está previsto para ocorrer em uma única atividade assim que as licenças e agentes da solução estejam disponíveis conforme cronograma de entrega.

2.6.5. O serviço de suporte técnico mensal está dimensionado para atendimento durante toda a vigência do contrato.

2.6.6. A transferência de conhecimento está considerando o atendimento da equipe de administradores da área de segurança e de outras áreas relacionadas com a administração ferramenta dentro da STI.

2.7. Análise de mercado de Tecnologia da Informação e Comunicação

2.7.1. Inicialmente foram levantadas as necessidades de negócio para esta contratação no documento de Análise de Viabilidade da Contratação, a partir da motivação/justificativa descrita no Documento de Oficialização da Demanda - DOD (SEI 0178883).

2.7.2. Dentre as possibilidades de atendimento da demanda, considerados os riscos da contratação, restaram duas alternativas viáveis tecnicamente:

2.7.2.1. Aquisição de solução de mercado para Gerenciamento de Acesso Privilegiado (PAM) para proteção dos ambientes computacionais do Conselho da Justiça Federal – CJF, contemplando licenciamento perpétuo, serviços de instalação e configuração, transferência de conhecimento, suporte técnico mensal e garantia do fabricante.

2.7.2.2. Contratação de empresa para fornecer a solução para Gerenciamento de Acesso Privilegiado (PAM) na modalidade *Software as a Service* (*Software* como Serviço) - SaaS.

2.7.3. Sendo assim, dentre as opções que atendem ao escopo pretendido e considerando as características, riscos, vantagens e desvantagens técnicas identificadas, a alternativa que se apresenta como adequada nos termos fundamentados nos estudos técnicos preliminares é a Aquisição de solução para Gerenciamento de Acesso Privilegiado (PAM) para proteção dos ambientes computacionais do Conselho da Justiça Federal – CJF, contemplando licenciamento perpétuo, serviços de instalação e configuração, transferência de conhecimento, suporte técnico mensal e garantia do fabricante.

2.7.4. Para realização da estimativa de custo, a equipe de contratação levou em consideração fornecedores de solução de Gerenciamento Acesso privilegiado (Privileged Access Management – PAM) presentes no Quadrante Mágico Gartner de 2020, as quais sejam: BeyondTrust, Thycotic, CyberArk e SenhaSegura.

2.7.5. Com objetivo de dar publicidade ao processo, dar conhecimento das condições de contratação e receber propostas estimativas de preços, o Termo de Referência com suas especificações técnicas foi enviado para 62 endereços de e-mail, entre empresas indicadas pelos fornecedores e demais empresas que poderiam atender ao objeto a ser contratado.

2.7.6. Os integrantes técnicos também realizaram pesquisa para obtenção de contratos vigentes com vários órgãos da administração pública para este mesmo objeto. Dentre os órgãos pesquisados estão Supremo Tribunal Federal-STF e Superior Tribunal de Justiça-STJ.

2.7.7. Com base nas propostas recebidas e nos contratos com objeto e condições similares foi elaborado o mapa comparativo de preços estimados para esta contratação. A média dos valores obtidos de cada item estão indicadas na tabela abaixo relacionada.

	Especificação	Qtde	Preço Unitário (R$)	Preço Total (R$)
1	Solução para Gerenciamento de Acesso Privilegiado com licenciamento perpétuo de *software* e fornecimento de equipamento(s)	01	772.666,67	772.666,67
2	Serviços de instalação e configuração.	01	13.266,67	13.266,67
3	Serviço de suporte técnico mensal	48	4.241,67	203.600,00
4	Transferência de conhecimento	06	2.566,67	15.400,00
VALOR TOTAL				1.004.933,34

2.8. Conformidade técnica e legal do objeto

O presente Termo de Referência foi elaborado em conformidade com as seguintes normas:

2.8.1. Lei 8.666/1993, que regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências;

2.8.2. Lei 10.520/2002, que institui, no âmbito da União, Estados, Distrito Federal e Municípios, nos termos do art. 37, inciso XXI, da Constituição Federal,

modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns, e dá outras providências;

2.8.3. Decreto 3.555/2000, que aprova o regulamento para a modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns;

2.8.4. Decreto 8.186/2014, que estabelece a aplicação de margem de preferência em licitações realizadas no âmbito da administração pública federal para aquisição de licenciamento de uso de programas de computador e serviços correlatos, para fins do disposto no art. 3º da Lei nº 8.666, de 21 de junho de 1993;

2.8.5. Decreto 10.024/2019, que regulamenta a licitação, na modalidade pregão, na forma eletrônica, para a aquisição de bens e a contratação de serviços comuns, incluídos os serviços comuns de engenharia, e dispõe sobre o uso da dispensa eletrônica, no âmbito da administração pública federal;

2.8.6. Resolução CNJ 182/2013, que dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação pelos órgãos do Poder Judiciário;

2.8.7. Instrução Normativa ME 07/2018, altera a IN 05/2017, que dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública federal direta, autárquica e fundacional;

2.8.8. Resolução CJF 279/2013, que dispõe sobre o Modelo de Contratação de Solução de Tecnologia da Informação da Justiça Federal - MCTI-JF no âmbito do Conselho e da Justiça Federal de primeiro e segundo graus.

2.8.9. Resolução CNJ 360/2020, que determina a adoção do Protocolo de Gerenciamento de Crises Cibernéticas no âmbito do Poder Judiciário (PGCC/PJ).

2.8.10. Resolução CNJ 361/2020, que determina a adoção de Protocolo de Prevenção a Incidentes Cibernéticos no âmbito do Poder Judiciário (PPICiber/PJ)

2.8.11. Portaria CJF 279/2013, que dispõe sobre a aprovação da Política de Controle Acesso Lógico, que veda a utilização de identificação genérica e de uso compartilhado para acesso aos recursos de rede.

2.8.12. Portaria CJF 303/2018, que define as normas a serem seguidas no CJF, relativas à utilização de recursos de tecnologia da informação, de forma a minimizar os riscos à segurança da informação na instituição. Atualizada pela Portaria CJF-POR-2018/00303 de 20 de agosto de 2018.

2.8.13. Portaria CJF 524/2020, que dispõe sobre a aprovação do Plano de Contratação de Soluções de TI - 2021 do Conselho da Justiça Federal – CJF.

2.8.14. Portaria CJF 62/2021, que dispõe sobre as etapas do planejamento da contratação, para aquisição de bens e contratações de serviços sob o regime de execução indireta, no âmbito do Conselho da Justiça Federal.

2.9. Justificativa para o parcelamento ou não da solução de TIC

2.9.1. Não é viável o parcelamento da solução. Os módulos da solução são interdependentes e não funcionam de maneira isolada. A contratação em separado dos serviços de instalação, configuração e suporte técnico poderiam, em casos de falhas ou interrupção de funcionamento da solução, gerar situações nas quais ficaria comprometida a identificação de responsabilidade de cada CONTRATADA. Tais ocorrências de conflitos e transferências de responsabilidade resultariam em elevação dos riscos de implantação, administração, disponibilidade, operabilidade e possibilidade de perda de garantia dos equipamentos sem ganho técnico e econômico justificável.

2.9.2. Considerando a existência de produtos de fabricantes distintos que atendem ao escopo da contratação, em caso de parcelamento da solução, a possibilidade de diferentes licitantes sagrarem-se vencedores em itens distintos tornaria inviável tecnicamente a execução do objeto na forma pretendida, pois cada fornecedor disponibilizaria solução com arquitetura e componentes próprios incompatíveis entre si.

2.10. Justificativa para o período de vigência contratual

2.10.1. Considerando que a solução visa armazenar, gerenciar e manter as credenciais privilegiadas para acesso aos principais equipamentos servidores do parque computacional do CJF, a contratação em 48 meses se faz necessária para possibilitar que este serviço crítico seja prestado de maneira continuada. As potenciais interrupções contratuais causadas por eventual falta de interesse da CONTRATADA na renovação contratual, geralmente causadas por dificuldades na manutenção dos preços das licenças em virtude de elevação da cotação do dólar, e a necessidade de se fazer novas licitações em curto prazo de tempo, elevam sobremaneira o risco de interrupção contratual e de falta de suporte da solução. Tais fatores aumentam o risco de indisponibilidade dos sistemas e equipamentos cujas credenciais privilegiadas serão mantidas pela solução. Neste cenário, a paralisação do serviço, põe em risco a continuidade dos serviços e sistemas mantidos pela STI.

2.10.2. No aspecto financeiro, por se tratar de contratação de solução contemplando aquisição de licenças de direito de uso perpétuo, o período de licenciamento maior é mais vantajoso quando comparado ao período de 12 meses. O período maior de licenciamento possibilita um ganho de escala que comumente resulta em maiores descontos por parte dos fabricantes das soluções.

2.10.3. O contrato com período de vigência ampliado contribui também para que a contratação possa ser considerada mais atrativa pelo mercado, em razão da uma maior diluição do investimento realizado para o fornecimento de equipamentos da solução. Resultando na redução do preço final proposto pelas licitantes do certame, favorecendo ampliação da competitividade e economicidade da contratação.

2.10.4. Portanto, entende-se que a vigência por mais de um exercício financeiro é fundamental para se obter preços e condições mais vantajosos para a Administração.

3. Forma e critério de seleção de fornecedor

3.1. Modalidade e tipo de licitação

3.1.1. O objeto da presente contratação pode ser objetivamente especificado por meio de padrões usuais de mercado. Desta forma, entendemos que o objeto pode ser classificado como serviço comum, para fins do disposto no parágrafo único, art. 1º da Lei 10.520, de 17 de julho de 2002, podendo, portanto, ser contratado por meio de processo licitatório na modalidade pregão, preferencialmente na forma eletrônica. Os serviços aqui tratados possuem natureza de serviço comum para fins do disposto no art. 3º do Decreto nº 10.024/2019.

3.1.2. Desse modo, fica definida como forma de seleção do fornecedor LICITAÇÃO na modalidade PREGÃO ELETRÔNICO do tipo MENOR PREÇO.

3.2. Forma de adjudicação do objeto

3.2.1. A adjudicação se dará por menor preço global.

3.3. Critérios de seleção do fornecedor

3.3.1. A proposta deverá indicar em qual página e item da documentação está a comprovação do atendimento aos requisitos técnicos descritos no ANEXO I - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO. O CJF poderá diligenciar com a licitante, caso a proposta não indique a página e item, nos termos ora exigidos, sem que isso implique a desclassificação imediata da proposta apresentada.

3.3.2. A proposta deverá incluir, em versão eletrônica, todos os catálogos ou prospectos do fabricante ou da internet, preferencialmente em língua portuguesa (Brasil), podendo ser em idioma estrangeiro (inglês), correspondente aos produtos ofertados no ANEXO I - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO deste Termo de Referência, com descrição detalhada de cada item, tendo em vista que é comum soluções de Tecnologia da Informação serem desenvolvidas por empresas estrangeiras e material bilíngue.

3.4. Critérios técnicos

3.4.1. As empresas LICITANTES deverão apresentar atestado(s) de capacidade técnica, que comprovem que tenham fornecido e implementado a contento, para órgãos ou entidades públicas ou privadas, solução de gerenciamento de

acesso privilegiado, no mínimo, 20 usuários ou 300 dispositivos do módulo de cofre de senhas.

3.4.2. Deverão constar do(s) atestado(s) de capacidade técnica em destaque, os seguintes dados: identificação do emitente, especificação completa do fornecimento/ serviço executado, local e data de expedição, data de início e término do contrato

3.5. Margem de preferência

3.5.1. A licitação submete-se às regras relativas ao direito de preferência estabelecidas no Decreto n. 8.186/2014, por se tratar de contratação de aquisição de solução de software em sua maior parte;

3.5.1.1. O exercício do direito de preferência disposto no Decreto n.º Decreto n. 8186/2014 será concedido após o encerramento da fase de lances.

3.6. Vistoria

3.6.1. A licitante poderá vistoriar o local onde serão executados os serviços até o último dia útil anterior à data fixada para a abertura da sessão pública, com o objetivo de inteirar-se das condições e grau de dificuldade existentes, mediante prévio agendamento de horário, com antecedência mínima de 48 (quarenta e oito) horas, junto a Secretaria de Tecnologia da Informação (STI) do CJF, pelos telefones (61) 3022-7400 e (61) 3022-7403, de 14 às 18 horas, limitada a realização da vistoria a um interessado por vez.

3.6.2. Caso a licitante deseje realizar vistoria, esta deverá ser realizada no Conselho da Justiça Federal (CJF), no Setor de Clubes Esportivos Sul - SCES - Trecho III - Pólo 8 - Lote 9 - CEP 70200-003 - Brasília/DF.

3.6.3. Detalhes sobre o ambiente tecnológico do CJF serão apresentados durante a vistoria somente mediante assinatura de Termo de Confidencialidade (ANEXO VI), a ser preenchido e assinado pelo representante legal da empresa.

3.7. Prova de conceito

3.7.1. Poderá ser solicitada, a critério exclusivo do CJF, prova de conceito para avaliação técnica da solução à primeira empresa licitante classificada, antes da adjudicação, com objetivo de comprovação de atendimento às especificações e requisitos exigidos nas especificações Técnicas deste termo de Referência.

3.7.2. A Prova de Conceito consistirá na apresentação da solução e a averiguação prática das funcionalidades e características do produto e sua real compatibilidade com os requisitos exigidos, e será realizada conforme o

roteiro pré-estabelecido baseado no ANEXO I - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO deste Termo de Referência.

3.7.3. Participarão da prova de conceito o(s) representante(s) credenciado(s) da LICITANTE melhor classificada, a equipe de planejamento da contratação e, quando couber, representante da unidade de contratação do CJF, além de eventuais LICITANTES interessados em acompanhar as sessões de avaliação técnica da solução.

3.7.3.1. Os eventuais LICITANTES interessados em participar da prova de conceito deverão manifestar-se até o fim do dia útil seguinte à data de convocação da primeira classificada.

3.7.3.2. Na manifestação de que trata o item anterior, deverá ser informado o nome do representante da LICITANTE que acompanhará a prova de conceito, o número do seu CPF, a identificação da empresa representada e a assinatura de seu representante legal.

3.7.3.3. O representante indicado pela licitante interessada assinará Termo de Confidencialidade nos termos apresentados no Anexo IV, condição para sua participação.

3.7.3.4. Durante a prova de conceito, os licitantes interessados manter-se-ão em silêncio, sob pena de ficarem impedidos de acompanhar as sessões de avaliação técnica da solução. Havendo necessidade de questionamento, o interessado poderá submeter manifestação por escrito à comissão de licitação do CJF, o que ocorrerá somente após a conclusão da prova de conceito e em até 3 (três) dias úteis após o seu encerramento.

3.7.4. A partir da convocação, a licitante terá o prazo de até 5 (cinco) dias úteis para preparação do ambiente da prova de conceito, a qual será realizada preferencialmente nas dependências do CJF ou em local diverso definido pelo órgão, mediante justificativa.

3.7.4.1. A disponibilização dos *hardwares* e *softwares* necessários à realização da prova de conceito são de inteira responsabilidade da LICITANTE e deverão corresponder ao conjunto de elementos da mesma marca, modelo e especificações detalhados na proposta.

3.7.5. Após a preparação do ambiente, a equipe do CJF agendará o início da prova de conceito, que será realizada no prazo máximo de 10 (dez) dias úteis, cabendo prorrogação quando solicitado pela LICITANTE e mediante manifestação favorável do CJF.

3.7.6. Durante a prova de conceito a equipe do CJF submeterá questionamentos à licitante para verificação dos requisitos constantes do Termo de Referência.

3.7.7. É facultado à equipe do CJF a possibilidade de realização de diligências para aferir o cumprimento dos requisitos sob análise.

3.7.8. Ao final da prova de conceito o CJF emitirá relatório sucinto no prazo de 10 (dez) dias úteis descrevendo os testes realizados e a conclusão sobre a aprovação ou desclassificação da proposta.

3.7.9. Será desclassificada a proposta da licitante que:

3.7.9.1. não atender aos prazos referentes à realização da prova de conceito; ou

3.7.9.2. apresentar divergência entre as especificações da solução entregue para a prova de conceito em relação as especificações técnicas da proposta entregue pela LICITANTE; ou

3.7.9.3. apresentar versão de *software* diferente da publicada em site oficial do fabricante e disponível para *download* por qualquer cliente.

3.7.10. Será concedido prazo de 3 (três) dias úteis para apresentação de contraprova pela licitante desclassificada na prova de conceito.

3.7.11. Em caso de desclassificação na prova de conceito, assegurado o procedimento do item anterior, o Pregoeiro restabelecerá a etapa de lances.

4. Modelo de execução e de gestão do contrato

4.1. Vigência

4.1.1. A vigência do Contrato será de:

4.1.1.1. 03 (três) meses, contados da assinatura do contrato, para a execução, mediante a emissão da Ordem de Serviços, da entrega, instalação, configuração, transferência de conhecimento e recebimento definitivo dos itens que compõem a solução.

4.1.1.2. 48 (quarenta e oito) meses, contados da data de emissão do Termo de Recebimento Definitivo, referente aos serviços de garantia e suporte técnico da solução de segurança, relativo aos serviços de natureza contínua desta contratação.

4.2. Reajuste

4.2.1. O valor do suporte técnico mensal poderá ser reajustado decorrido 12 (doze) meses de vigência contratual, mediante negociação entre as partes, tendo como limite máximo a variação acumulada do Índice Nacional de Preços ao Consumidor Amplo/IPCA, calculado e divulgado pelo Instituto Brasileiro de Geografia e Estatística/IBGE.

4.2.2. As PARTES atentarão para que o percentual a ser aplicado não seja superior à variação acumulada no período compreendido entre a data da apresentação da proposta e aquela em que se verificar no mês anterior ao aniversário da celebração do contrato, conforme estabelece a Lei n. 8.666/1993, art. 40, inciso XI.

4.2.3. Os reajustes seguintes serão calculados considerando-se a variação acumulada dos 12 (doze) últimos meses, contados do mês anterior ao aniversário do contrato.

4.2.4. Caso o índice estabelecido para delimitar o reajustamento dos preços seja extinto ou, de qualquer forma, não possa mais ser utilizado para esse fim, as partes desde já concordam que em substituição seja adotado o que vier a ser determinado pela legislação então em vigor.

4.2.5. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice para delimitar o reajustamento dos preços.

4.2.6. Incumbe à CONTRATADA a apresentação do pedido de reajuste acompanhado da respectiva memória de cálculo, a qual, após análise e aprovação pelo CONTRATANTE, redundará na emissão do instrumento pertinente ao reajuste contratual.

4.3. Obrigações contratuais do CONTRATANTE e da CONTRATADA

4.3.1. **Deveres e responsabilidades do CONTRATANTE**

4.3.1.1. Acompanhar e fiscalizar a execução do objeto contratual.

4.3.1.2. Determinar responsável para o acompanhamento e fiscalização da execução do objeto contratual.

4.3.1.3. Informar a CONTRATADA de atos que possam interferir direta ou indiretamente nos serviços prestados.

4.3.1.4. Comunicar oficialmente à CONTRATADA quaisquer falhas e/ou anormalidades verificadas no cumprimento das obrigações contratuais.

4.3.1.5. Avaliar todos os serviços prestados pela CONTRATADA.

4.3.1.6. Responsabilizar-se pelos pagamentos dos serviços prestados pela CONTRATADA mediante a apresentação de Nota Fiscal.

4.3.1.7. Indicar os seus representantes para fins de contato e demais providências inerentes à execução do contrato.

4.3.1.8. Para os serviços inclusos no período de garantia do objeto e para a realização de suporte técnico, o CONTRATANTE permitirá o acesso dos técnicos habilitados e identificados da CONTRATADA às instalações onde se encontrarem os equipamentos. Esses técnicos ficarão sujeitos a todas as normas internas de segurança do CONTRATANTE, inclusive àqueles referentes à identificação, trânsito e permanência em suas dependências.

4.3.2. **Deveres e responsabilidades da CONTRATADA**

4.3.2.1. Fornecer os *softwares* e equipamentos da solução com todos os itens acessórios necessários à sua perfeita instalação, funcionamento e integração ao ambiente computacional do CONTRATANTE, incluindo cabos, conectores, interfaces, suportes, drivers de controle e programas de configuração.

4.3.2.2. Acatar as normas e diretrizes estabelecidas pelo CONTRATANTE para o fornecimento dos produtos e execução dos serviços objeto deste Termo de Referência.

4.3.2.3. Submeter à prévia aprovação do CONTRATANTE toda e qualquer alteração pretendida na prestação dos serviços.

4.3.2.4. Manter, durante a execução do contrato a ser firmado, as condições de habilitação e qualificação exigidas na licitação.

4.3.2.5. Sujeitar-se à fiscalização do CONTRATANTE, no tocante ao fornecimento e a prestação dos serviços, prestando todos os esclarecimentos solicitados e atendendo de imediato às reclamações fundamentadas, caso venham a ocorrer.

4.3.2.6. Prestar as atividades objeto da licitação, por meio de mão de obra especializada e devidamente certificada pelos fabricantes dos *softwares* e equipamentos da solução.

4.3.2.7. Indicar profissional que atuará, desde o início da execução do contrato até a conclusão da implantação, como Gerente de Projeto.

4.3.2.8. Propor os ajustes necessários à adequação, segurança e racionalização dos serviços prestados, respeitando o objeto deste Termo de Referência.

4.3.2.9. Responsabilizar-se por todos os ônus referentes aos serviços objeto deste Termo de Referência, inclusive salários de pessoal, alimentação, diárias, hospedagem, transporte e seguros, bem como tudo que as leis trabalhistas e previdenciárias preveem e demais exigências legais para o exercício da atividade objeto deste Termo de Referência.

4.3.2.10. Responsabilizar-se integralmente pela sua equipe técnica, primando pela qualidade, desempenho, eficiência e produtividade, visando à execução dos trabalhos durante todo o Contrato, dentro dos prazos estipulados, sob pena de ser considerada infração passível de aplicação das penalidades previstas, caso os prazos e condições não sejam cumpridos.

4.3.2.11. Ter pleno conhecimento de todas as condições e peculiaridades inerentes aos serviços a serem executados não podendo invocar posteriormente desconhecimento para cobrança de pagamentos adicionais ao CONTRATANTE ou a não prestação satisfatória dos serviços.

4.3.2.12. Guardar inteiro sigilo dos dados que tiver acesso, reconhecendo serem estes de propriedade exclusiva do CONTRATANTE.

4.3.2.13. Substituir imediatamente, a critério do CONTRATANTE, a qualquer tempo, e sem nenhum ônus adicional, qualquer profissional do seu corpo técnico cuja presença seja considerada indesejável ou inconveniente, em virtude de comportamento inadequado devidamente justificado.

4.3.2.14. Acatar, nas mesmas condições ofertadas, nos termos do art. 65, § 1º, da Lei nº 8.666/93, as solicitações do CONTRATANTE para acréscimos ou supressões que se fizerem necessárias à execução do objeto licitado.

4.3.2.15. Assumir a responsabilidade por danos causados diretamente à Administração ou a terceiros, decorrentes de sua culpa ou dolo na execução do objeto licitado, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pelo CONTRATANTE.

4.3.2.16. Sujeitar-se a mais ampla e irrestrita fiscalização, por parte da Equipe de Fiscalização e/ou Recebimento indicada pelo CONTRATANTE para acompanhamento da execução do contrato, prestando todos os esclarecimentos que lhes forem solicitados e atendendo às reclamações formuladas.

4.3.2.17. Comunicar a Equipe de Fiscalização e/ou Recebimento, por escrito, qualquer anormalidade que ponha em risco o fornecimento ou a execução dos serviços.

4.3.2.18. Corrigir as falhas detectadas pela Equipe de Fiscalização e/ou Recebimento indicada pelo CONTRATANTE.

4.3.2.19. Executar as atividades previstas no contrato em estrito cumprimento aos prazos previstos no ANEXO III – CRONOGRAMA DE IMPLANTAÇÃO, após a emissão de Ordem de Serviço pelo CONTRATANTE.

4.4. Papéis a serem desempenhados durante a execução contratual

4.4.1. Pela CONTRATANTE

4.4.1.1. Equipe de Fiscalização do Contrato.

4.4.1.2. Os produtos e serviços objetos desta contratação serão fiscalizados por servidor ou comissão de servidores do CONTRATANTE, doravante denominados Fiscalização, que terá autoridade para exercer toda e qualquer ação de orientação geral, controle e fiscalização da execução contratual.

4.4.1.3. À Fiscalização compete, entre outras atribuições:

4.4.1.3.1. Solicitar à Contratada e seus prepostos, ou obter da Administração, tempestivamente, todas as providências necessárias ao bom andamento do contrato e anexar aos autos do processo correspondente cópia dos documentos escritos que comprovem essas solicitações de providências.

4.4.1.3.2. Manter organizado e atualizado um sistema de controle em que se registrem as ocorrências ou os serviços descritos de forma analítica.

4.4.1.3.3. Acompanhar e atestar a prestação dos serviços contratados e indicar a ocorrência de inconformidade desses serviços ou não cumprimento do contrato.

4.4.1.3.4. Encaminhar à Secretaria de Administração os documentos para exame e deliberação sobre a possível aplicação de sanções administrativas.

4.4.1.4. A ação da Fiscalização não exonera a Contratada de suas responsabilidades contratuais.

4.4.2. Pela CONTRATADA

4.4.2.1. Representante legal: pessoa formalmente designada e devidamente autorizada a firmar contrato em nome da Contratada.

4.4.2.2. Preposto: nomeado pelo representante legal no início da execução contratual, nos termos do art. 68 da Lei nº 8.666/93, que atuará como representante da Contratada durante a execução contratual. Deve ser apresentado, por ocasião da reunião de planejamento.

4.4.2.3. Gerente de Projetos: líder e responsável pela entrega dos serviços de planejamento e implantação da solução, de modo a garantir a qualidade dos resultados e o atendimento aos requisitos e prazos estipulados no Edital. Deve ser apresentado, por ocasião da reunião de planejamento.

4.4.2.4. Responsável Técnico: funcionário da empresa responsável pela prospecção, elaboração e implantação da solução além de responder por questões técnicas atinentes à solução durante a execução contratual. Deve ser apresentado, por ocasião da reunião de planejamento.

4.5. Qualificação técnica dos profissionais da CONTRATADA

4.5.1. O Gerente de Projetos deve atender no mínimo aos seguintes requisitos:

4.5.1.1. Deve possuir escolaridade de nível superior completo;

4.5.1.2. Deve possuir certificação PMP – Project Management Professional do PMI – Project Management Institute ou possuir MBA – Master of Business Administration em Gerência de Projetos.

4.6. Dinâmica de execução contratual

4.6.1. **Plano de implantação**

4.6.1.1. A CONTRATADA deverá elaborar Plano de Implantação da solução contendo cronograma de execução das atividades, previsão de recursos, pessoas envolvidas e atividades a serem desenvolvidas pela CONTRATADA e indicar os principais riscos e forma de mitigação, contendo também os seguintes itens:

4.6.1.2. Descrição e detalhamento dos procedimentos para entrega, retirada das embalagens e conferência dos equipamentos, *softwares* e acessórios entregues.

4.6.1.3. Descrição e detalhamento das informações sobre as etapas de instalação física dos equipamentos incluindo distribuição dos equipamentos pelos *racks*, movimentação de equipamentos existentes, conexões elétricas e lógicas necessárias, definição de nomes dos equipamentos e de endereçamento de gerência IP.

4.6.1.4. Proposta de interconexão física e lógica dos componentes da solução aos ativos rede do CONTRATANTE, observando as melhores práticas de segurança e considerando os recursos disponíveis nos elementos da solução.

4.6.1.5. Planejamento da engenharia de tráfego da solução com base nas melhores práticas de segurança e considerando os recursos disponíveis nos elementos da solução.

4.6.1.6. Descrição e detalhamento das condições de *rollback* de cada mudança no ambiente do CONTRATANTE para a instalação da solução.

4.6.1.7. Descrição e detalhamento das atividades de teste de operação da solução e planos de testes para os diversos componentes da solução que comprovem o funcionamento das regras e configurações aplicadas, bem como dos recursos de tolerância a falhas dos *softwares* e equipamentos da solução.

4.6.1.8. Descrição e detalhamento da transferência de conhecimento nos termos do item 4.6.5

4.6.2. **Serviço de instalação e configuração**

4.6.2.1. As atividades de entrega, instalação e configuração dos *softwares* e equipamentos da solução deverão ocorrer na sede do CONTRATANTE e a execução deve ser realizada em horários que não coincidam com o expediente do CONTRATANTE.

4.6.2.2. O CONTRATANTE poderá autorizar a realização de atividades durante o horário de expediente se, ao seu exclusivo critério,

entender que não oferece risco ao funcionamento dos serviços e sistemas em produção.

4.6.2.3. O processo de entrega, instalação e configuração dos componentes da solução deverá ser acompanhado e supervisionado pela equipe técnica indicada pelo CONTRATANTE.

4.6.2.4. Entregar os equipamentos novos e 1º uso juntamente com todos os itens acessórios de *hardware* e de *software* necessários à perfeita instalação e funcionamento, incluindo cabos, conectores, interface, suportes, drivers de controle, programas de configuração, conforme especificações constantes no ANEXO I - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO deste Termo de Referência.

4.6.2.5. Entregar os equipamentos devidamente protegidos e embalados, originais lacrados, sem danos de transporte e manuseio.

4.6.2.6. Entregar os equipamentos e softwares, às suas expensas, bem como instalar e realizar todos os testes necessários à verificação do perfeito funcionamento dos produtos fornecidos.

4.6.2.7. Entregar toda a documentação técnica em meio eletrônico, completa e atualizada, contendo os manuais e guias de utilização.

4.6.2.8. Caso a implantação de qualquer elemento da solução cause interferência na correta operação da rede de dados do CONTRATANTE, a CONTRATADA deverá alocar profissionais com qualificação suficiente para corrigir o problema ou retornar ao ambiente à condição anterior à implantação.

4.6.2.9. A execução dos serviços de entrega, instalação e configuração dos *softwares* e equipamentos da solução deverá contemplar, no mínimo, os seguintes itens:

4.6.2.9.1. Instalação física e ativação dos componentes da solução.

4.6.2.9.2. Integração à rede do CONTRATANTE, sem interrupção no funcionamento normal dos serviços de TI. Caso exista a necessidade de interrupção de qualquer equipamento ou serviço em produção para a integração da solução, o prazo para realização e a duração da janela de manutenção deverão ser acordados com o CONTRATANTE.

4.6.2.9.3. Instalação e configuração dos softwares e funcionalidades exigidas na especificação técnica dos elementos que compõem a solução fornecida, bem como quaisquer outras disponíveis adicionalmente nos diversos componentes da solução mediante solicitação da equipe do CONTRATANTE.

4.6.2.9.4. Realização de testes de operação da solução que comprovem o funcionamento dos recursos de tolerância a falhas dos diversos componentes da solução, quando aplicável.

4.6.2.9.5. Atualização do Plano de Implantação com todas as informações que representem a topologia física e lógica e a configuração final aplicadas.

4.6.2.10. Os serviços e entregas serão executados no Conselho da Justiça Federal (CJF), no Setor de Clubes Esportivos Sul - SCES - Trecho III - Polo 8 - Lote 9 - CEP 70200-003 - Brasília/DF;

4.6.3. **Serviço de suporte técnico**

4.6.3.1. O serviço de suporte técnico para os softwares e equipamentos da solução deverá ser executado pela CONTRATADA ou diretamente pelo fabricante, durante o prazo de 48 (quarenta e oito) meses, contados a partir da data de emissão do Termo de Recebimento Definitivo dos serviços de entrega, instalação e configuração dos softwares e equipamentos da solução.

4.6.3.2. O serviço de suporte técnico da solução consiste em:

4.6.3.2.1. Atuar, mediante abertura pelo CONTRATANTE de chamado técnico de suporte, no local de instalação da solução, visando a solução de problemas que afetem de forma isolada ou conjunta, qualquer elemento da solução, permitindo o retorno à condição normal de operação.

4.6.3.2.2. Atuar, mediante abertura pelo CONTRATANTE de chamado técnico de suporte, por meio de contato telefônico ou outro recurso de comunicação, visando o esclarecimento de dúvidas em relação a qualquer elemento da solução.

4.6.3.2.3. Realizar visitas técnicas preventivas no local de instalação da solução (on-site), com frequência mensal, e com duração de pelo menos 1 (uma) hora a cada visita, visando assegurar o melhor desempenho da solução.

4.6.3.2.4. Substituir peças e componentes, cujos problemas sejam decorrentes do desgaste pelo uso normal dos equipamentos, por outras de configuração idêntica ou superior, originais e novas.

4.6.3.3. CONTRATANTE realizará a abertura de chamados técnicos de suporte por ligação telefônica, por e-mail ou via Internet, em período integral, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana.

4.6.3.4. A CONTRATADA deverá informar o procedimento para abertura de chamado técnico de suporte no documento Plano de Implantação.

4.6.3.5. Se a Central de Suporte estiver localizada fora de Brasília, a CONTRATADA deverá informar o DDG (discagem direta gratuita

0800). O acesso à área restrita de suporte em endereço eletrônico (WEB site) deverá estar disponível, também, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana.

4.6.3.6. Quando da abertura de chamado técnico de suporte pelo CONTRATANTE, a CONTRATADA deverá informar o número do chamado, para fins de controle.

4.6.3.7. A CONTRATADA deverá enviar mensalmente, ou disponibilizar acesso por meio de portal internet, relação consolidada dos chamados abertos no mês, mencionando: data e hora de abertura do chamado técnico, número do chamado técnico, problemas verificados, técnico responsável pelo atendimento.

4.6.3.8. A CONTRATADA deverá disponibilizar acesso a base de conhecimento do fabricante dos componentes da solução, contemplando toda a documentação técnica (guias de instalação/configuração atualizados, FAQ's, com pesquisa efetuada através de ferramentas de busca) e atualizações.

4.6.3.9. A CONTRATADA deverá realizar a cada ocorrência, como escopo das atividades de visitas técnicas preventivas, as tarefas de coleta e análise de logs dos produtos, realizar o levantamento de configurações aplicadas nos *softwares* e equipamentos da solução, buscando compará-las às melhores práticas e recomendações dos fabricantes, avaliar aspectos de segurança e desempenho da solução, finalizando com a elaboração de relatório técnico com as informações coletadas e as recomendações a serem aplicadas à solução.

4.6.3.10. As visitas técnicas preventivas deverão ser realizadas por técnico(s) plenamente qualificado(s), com certificação emitida pelos fabricantes dos *softwares* e equipamentos da solução ofertada, e deverão ser prestadas com acompanhamento da equipe técnica do CONTRATANTE.

4.6.3.11. A contagem de prazo para a realização das visitas técnicas preventivas será iniciada após emissão do Termo de Recebimento Definitivo, devendo ocorrer automaticamente em dia e hora previamente agendada com o CONTRATANTE e serão consideradas concluídas após o entrega do relatório técnico de atendimento e aceite pelo CONTRATANTE. A cada visita deverá ser gerado relatório técnico com sugestões e ajustes para a melhoria de desempenho, funcionalidade e segurança.

4.6.3.12. A CONTRATADA deverá prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos do CONTRATANTE, em relação à instalação, configuração e problemas detectados, atendendo de imediato as solicitações.

4.6.4. **Níveis mínimos do serviço de suporte técnico**

4.6.4.1. Quando da abertura de chamado técnico de suporte, os chamados deverão ser categorizados em 3 (três) níveis, da seguinte forma:

Criticidade	**Descrição**	**Prazo máximo para início de atendimento (contados a partir da abertura do chamado)**	**Prazo máximo para restauração de serviço (contados a partir da abertura do chamado)**
Severidade 1 (Alta)	Atuação ON-SITE em ocorrências que causem indisponibilidade ou restrição de funcionalidade da solução prejudicando a operação normal e que gerem impacto ao negócio.	Em até 1 (uma) hora deve ter um técnico da CONTRATADA ON-SITE.	Em até 3 (três) horas
Severidade 2 (Média)	Atuação REMOTA visando sanar problemas que criem restrições a operação normal da solução não gerando impacto ao negócio.	Em até 6 (seis) horas um técnico da CONTRATADA entra em contato.	Em até 12 doze) horas
Severidade 3 (Baixa)	Atuação REMOTA visando sanar problemas que não afetem a operação normal da solução ou dúvidas de operação e configuração.	Em até 12 (doze) horas um técnico da CONTRATADA entra em contato.	Em até 36 (trinta e seis horas)

4.6.5. **Transferência de conhecimento**

4.6.5.1. A CONTRATADA deverá realizar a transferência de conhecimento para a equipe técnica do CONTRATANTE por meio de treinamento nas tecnologias da solução para **6** participantes com carga horária total de no mínimo **20 (vinte)** horas.

4.6.5.2. O serviço de transferência de conhecimento será solicitado sob demanda, mediante de emissão de ordem de serviço específica

para este serviço conforme ANEXO III - CRONOGRAMA DE IMPLANTAÇÃO.

4.6.5.3. A transferência de conhecimento deverá iniciar no prazo máximo de **15 (quinze)** dias corridos após a emissão da ordem de serviço específica para esta etapa conforme ANEXO III - CRONOGRAMA DE IMPLANTAÇÃO.

4.6.5.4. A transferência de conhecimento deverá ser realizada em Brasília/DF na sede do CONTRATANTE ou em ambiente alternativo indicado pela CONTRATADA, desde que seja previamente justificado e autorizado pelo CONTRATANTE.

4.6.5.5. O programa para a transferência de conhecimento deverá abordar as principais funcionalidades de administração e operação da solução e ser previamente aprovado pelo CONTRATANTE, e eventuais mudanças de conteúdo solicitadas deverão constar no material didático.

4.6.5.6. O material didático do da transferência de conhecimento deverá ser disponibilizado em formato eletrônico, sem custo adicional para o CONTRATANTE, devendo ainda estar, preferencialmente, em língua portuguesa (Brasil), podendo ser em idioma estrangeiro (inglês), tendo em vista que é comum soluções de Tecnologia da Informação serem desenvolvidas por empresas estrangeiras e material bilíngue.

4.6.5.7. Deverá ser emitido certificado de participação ao final do curso a cada participante, detalhando programa e carga horária.

4.6.5.8. O cronograma efetivo da transferência de conhecimento será definido em conjunto com o CONTRATANTE, após a emissão da Ordem de Serviço na primeira reunião de planejamento.

4.6.5.9. Caso a transferência de conhecimento não seja satisfatória com relação à profundidade do conteúdo apresentado ou domínio dos temas por parte do instrutor, a CONTRATADA deverá complementar, sem ônus adicional, o repasse dos pontos considerados pelo CONTRATANTE como insatisfatórios.

4.6.5.10. A transferência de conhecimento deverá ser realizada por técnicos qualificados e certificados pelos fabricantes dos *softwares* e equipamentos da solução ofertada.

4.7. Cronograma de recebimento do objeto

4.7.1. A CONTRATADA deverá iniciar a execução das atividades de entrega, instalação e configuração dos *softwares* e equipamentos da solução a partir da emissão da Ordem de Serviço pelo CONTRATANTE, conforme ANEXO III - CRONOGRAMA DE IMPLANTAÇÃO.

4.7.2. A CONTRATADA e o CONTRATANTE deverão realizar, em até 3 (três) dias úteis após a emissão da Ordem de Serviço, reunião de planejamento presencial na sede do CONTRATANTE ou por meio de reunião à distância, a ser acordado com o CONTRATANTE, com o objetivo de apresentar a metodologia de trabalho, planejamento e coordenação das atividades de entrega da solução CONTRATADA, conforme ANEXO III - CRONOGRAMA DE IMPLANTAÇÃO.

4.7.3. A CONTRATADA deverá apresentar o Plano de Implantação, em até **10 (dez)** dias corridos da emissão da Ordem de Serviço, contendo a documentação detalhada das atividades de entrega, instalação, configuração e testes dos *softwares* e equipamentos da solução, conforme ANEXO III - CRONOGRAMA DE IMPLANTAÇÃO.

4.7.4. A CONTRATADA deverá entregar todos os equipamentos, *softwares* e acessórios da solução no prazo máximo de até **45 (quarenta e cinco)** dias corridos, a contar da data de emissão da Ordem de Serviço, conforme ANEXO III - CRONOGRAMA DE IMPLANTAÇÃO.

4.7.5. O CONTRATANTE fará a emissão do Termo de Recebimento Provisório (TRP1) da etapa da entrega dos *softwares* e equipamentos da solução, em até **5 (cinco)** dias úteis da comunicação da CONTRATADA, conforme descrito no cronograma do ANEXO III - CRONOGRAMA DE IMPLANTAÇÃO.

4.7.6. A CONTRATADA deverá realizar a instalação e configuração dos *softwares* e equipamentos da solução e entrega das licenças de uso no prazo máximo de **15 (quinze)** dias corridos, contados a partir da data de emissão do Termo de Recebimento Provisório (TRP1), conforme ANEXO III - CRONOGRAMA DE IMPLANTAÇÃO.

4.7.7. A conclusão das etapas instalação e configuração dos *softwares* e equipamentos da solução e entrega das licenças de uso deverá ser formalizada mediante comunicação escrita da CONTRATADA ao CONTRATANTE.

4.7.8. O CONTRATANTE fará a emissão do Termo de Recebimento Provisório (TRP2) da etapa de instalação e configuração dos *softwares* e equipamentos da solução em até **5 (cinco)** dias úteis da comunicação da CONTRATADA, conforme descrito no cronograma do ANEXO III - CRONOGRAMA DE IMPLANTAÇÃO.

4.7.9. O CONTRATANTE fará a emissão do Termo de Recebimento Definitivo (TRD) da entrega, instalação, configuração e licenciamento da solução em até **10 (dez)** dias úteis da emissão do Termo de Recebimento Provisório (TRP2), conforme descrito no cronograma do ANEXO III - CRONOGRAMA DE IMPLANTAÇÃO.

4.7.10. Na contagem dos prazos definidos, excluir-se-á o dia de início e incluir-se-á o dia do vencimento. Só se iniciam e vencem os prazos em dias úteis e de expediente no Conselho da Justiça Federal.

4.7.11. Serão considerados injustificados os atrasos não comunicados tempestivamente e indevidamente fundamentados, e a aceitação da justificativa ficará a critério do CONTRATANTE.

4.7.12. Havendo pedido de prorrogação do prazo de entrega, a eventual concessão ocorrerá somente nas hipóteses previstas no art. 57, §1°, da Lei nº 8.666/93, em caráter excepcional e sem efeito suspensivo, e deverá ser encaminhado por escrito, com antecedência mínima de 1 (um) dia útil do seu vencimento, anexando-se documento comprobatório do alegado pela CONTRATADA.

4.7.13. Eventual pedido de prorrogação deverá ser encaminhado ao CONTRATANTE preferencialmente na forma eletrônica.

4.7.14. Em casos excepcionais, autorizados pelo CONTRATANTE, o documento comprobatório do alegado poderá acompanhar a entrega do produto.

4.7.15. Juntamente com a documentação de entrega, instalação e configuração da solução, como requisito para a emissão do Termo de Recebimento Definitivo, a CONTRATADA deverá entregar a seguinte documentação:

4.7.15.1. Cessões de direito de uso perpétuo dos *softwares* fornecidos. Os termos de licenciamento de todos os *softwares* fornecidos, emitidos pelo fabricante, deverão ser entregues pela CONTRATADA e os mesmos serão pertencentes ao CONTRATANTE.

4.7.15.2. Conjunto de direitos de atualização de versão, pelo período de 48 (quarenta e oito) meses de garantia, de todos os *softwares* fornecidos. Abrangerá todos os *softwares* e licenças a serem fornecidos na solução. Os termos de licenciamento referentes aos direitos de atualização de versão, emitidos pelo fabricante, deverão ser entregues pela CONTRATADA e comporão direito pertencente ao patrimônio do CONTRATANTE.

4.8. Garantia do objeto

4.8.1. O prazo de garantia dos equipamentos e direito a atualização dos *softwares* que compõem a solução é de 48 (quarenta e oito) meses, contados a partir da emissão do Termo de Recebimento Definitivo dos serviços de entrega, instalação e configuração dos *softwares* e equipamentos da solução.

4.8.2. Todos os *softwares* e equipamentos fornecidos deverão suportar a última versão de *firmware* disponibilizada pelos fabricantes durante toda a vigência do contrato.

4.8.3. Caso algum *software* ou equipamento conste em lista de *end-of-support, end-of-engineering-support ou end-of-life* do fabricante, durante o período de vigência do contrato, a CONTRATADA deverá fornecer, configurar e promover a substituição por novo equivalente, que atenda as especificações técnicas descritas neste Termo e que não impacte na perda de funcionalidade da solução.

4.8.4. Os custos relativos ao serviço de garantia dos *softwares* e equipamentos da solução já devem estar incluídos no preço dos próprios itens.

4.8.5. O serviço de garantia técnica da solução consiste em reparar eventuais falhas de funcionamento dos equipamentos, dos *softwares* e na integração entre os componentes da solução, mediante a substituição de equipamentos e de versões dos *softwares* ou revisão de configurações, de acordo com as recomendações dos fabricantes, informações presentes nas páginas e manuais de suporte e normas técnicas específicas.

4.8.6. O direito a atualização dos *softwares* obriga a CONTRATADA a disponibilizar a atualização dos *softwares* fornecidos e que compõem a solução tão logo ocorra o lançamento de novos *softwares* em substituição aos fornecidos, ou mesmo não sendo uma substituição, se ficar caracterizada uma descontinuidade dos *softwares* fornecidos.

4.8.7. A reparação de falhas de funcionamento dos componentes da solução deverá ocorrer de acordo com os seguintes princípios:

4.8.7.1. Quanto aos equipamentos da solução:

4.8.7.1.1. Dispor de estoque de peças e equipamentos de reposição, visando à prestação dos serviços de reparação do funcionamento dos equipamentos durante todo o período de garantia.

4.8.7.1.2. Substituir, no prazo de **24 (vinte e quatro)** horas, partes e componentes dos equipamentos que apresentem defeito por outras de características idênticas ou superiores, originais e novas.

4.8.7.1.3. Nos casos em que não seja possível o reparo dentro do prazo estipulado acima, substituir no prazo máximo de **72 (setenta e duas)** horas, em caráter temporário ou definitivo, o equipamento defeituoso por outro de mesma marca e modelo, ou superior, e com as mesmas características técnicas, novo e de primeiro uso.

4.8.7.1.4. Substituir, no prazo de **120 (cento e vinte)** horas, qualquer equipamento, componente ou periférico por outro original e novo, na ocorrência dos seguintes casos:

- Se for constatada qualquer divergência com as especificações técnicas descritas na proposta técnica apresentada.
- Se no período de **15 (quinze)** dias corridos, contados após a abertura de chamado de Suporte Técnico, ocorrerem defeitos recorrentes que não permitam seu correto funcionamento, mesmo tendo havido substituição de partes e componentes.

4.8.7.1.5. Em todas as hipóteses de substituição previstas anteriormente, caso exista a impossibilidade técnica de substituição por modelo igual, novo e original, será permitida a substituição por outro com características técnicas idênticas ou superiores, plenamente compatível, também original e novo.

4.8.7.1.6. Devolver, em perfeito estado de funcionamento, no prazo máximo de **15 (quinze)** dias corridos, a contar da data de retirada dos equipamentos, os equipamentos que necessitem ser temporariamente retirados para reparo, ficando a remoção, o transporte e a substituição sob inteira responsabilidade da CONTRATADA.

4.8.7.1.7. Responsabilizar-se pelas ações executadas ou recomendadas por analistas e consultores do quadro da empresa, assim como pelos efeitos delas advindos na execução das atividades previstas neste Termo de Referência ou no uso dos acessos, privilégios ou informações obtidas em função das atividades por estes executadas.

4.8.7.1.8. Comunicar, por escrito, ao CONTRATANTE, sempre que constatar condições inadequadas de funcionamento ou má utilização a que estejam submetidos os equipamentos objeto deste Termo de Referência, fazendo constar a causa de inadequação e a ação devida para a correção

4.8.7.2. Quanto aos *softwares* da solução:

4.8.7.2.1. A CONTRATADA deverá promover o isolamento, identificação e caracterização de falhas nos *softwares* da solução consideradas “bug de software”.

4.8.7.2.2. Será considerado pelo CONTRATANTE como “bug de software” o comportamento ou característica dos *softwares* que se mostre diferentes daquele previsto na documentação do produto e seja considerado como prejudicial ao correto uso.

4.8.7.2.3. Será de exclusiva responsabilidade da CONTRATADA o encaminhamento da falha de *software* ao laboratório do fabricante, o acompanhamento da solução e a aplicação do respectivo *fix*, *patch* ou pacote de correção em dia e horário a ser definido pelo CONTRATANTE.

4.8.7.2.4. Responsabilizar-se pelas ações executadas ou recomendadas por analistas e consultores do quadro da empresa, assim como pelos efeitos delas advindos na execução das atividades previstas neste Termo de Referência ou no uso dos acessos, privilégios ou informações obtidas em função das atividades por estes executadas.

4.8.7.2.5. Comunicar, por escrito, ao CONTRATANTE, sempre que constatar condições inadequadas de funcionamento ou má utilização a que estejam submetidos os *softwares* objeto deste Termo de Referência, fazendo constar a causa de inadequação e a ação devida para a correção.

4.8.7.3. Quanto a integração dos componentes da solução:

4.8.7.3.1. A CONTRATADA deverá manter, durante a vigência da garantia, a correta integração entre os elementos de *hardware* e *software* que compõem a solução, nas mesmas condições de desempenho e confiabilidade que apresentavam no momento de emissão do Termo de Recebimento Definitivo.

4.8.7.3.2. Quando forem identificadas falhas de funcionamento na solução que não sejam atribuídas diretamente aos elementos de *hardware* ou de *software*, caberá à CONTRATADA a análise e o encaminhamento da solução, buscando restaurar o correto funcionamento do conjunto de elementos da solução.

4.8.7.3.3. Serão consideradas como falhas de funcionamento da integração dos componentes a redução significativa do desempenho ou a perda de funcionalidades técnicas disponibilizadas pelo conjunto da solução.

4.8.8. A atualização dos *softwares* fornecidos que compõem a solução, deverá ocorrer de acordo com os seguintes princípios:

4.8.8.1. O CONTRATANTE deverá ter direito irrestrito, durante a vigência da garantia, de atualizar as versões de todos os *softwares* que compõem a solução, mesmo que os fabricantes alterem suas políticas de licenciamento dos *softwares*.

4.8.8.2. O direito a atualização de versões dos *softwares* que compõem a solução não poderá gerar qualquer custo adicional para o CONTRATANTE.

4.8.8.3. Deverão ser criadas contas de acesso, em nome do CONTRATANTE, no site de suporte do fabricante dos *softwares* que compõem a solução.

4.8.8.4. O perfil das contas criadas em nome do CONTRATANTE deverá permitir de forma irrestrita o download de *drivers*, *firmwares*, *patches*, atualizações, novas versões, informações de suporte, acesso a base de conhecimento e manuais técnicos.

4.8.8.5. Sempre que solicitado, mediante chamado de Suporte Técnico, a CONTRATADA deverá orientar o CONTRATANTE quanto aos procedimentos técnicos para a instalação ou atualização de versões dos *softwares* que compõem a solução.

4.9. Pagamento

4.9.1. A CONTRATADA deverá emitir Notas Fiscais/Faturas relativas aos valores dos softwares e equipamentos da solução e garantia por 48 (quarenta e oito) meses, serviços de instalação e configuração e serviço de transferência de conhecimento após receber cópia do Termo de Recebimento Definitivo previsto no ANEXO III - CRONOGRAMA DE IMPLANTAÇÃO.

4.9.2. O pagamento do serviço de suporte técnico será efetuado mensalmente, sendo iniciado somente após o Recebimento Definitivo da solução, mediante envio da Nota Fiscal/Fatura pela CONTRATADA.

4.9.3. O pagamento será efetuado, por ordem bancária, mediante a apresentação de nota fiscal, correspondente ao fornecimento executado e aceito definitivamente, devendo ser emitida, obrigatoriamente, com número raiz do CNPJ qualificado no preâmbulo.

4.9.4. As notas fiscais deverão ser encaminhadas ao e-mail indicado pelo gestor do contrato.

4.9.5. No corpo da nota fiscal deverá ser especificado o objeto contratado e o período faturado no formato dia/mês/ano e os quantitativos dos itens, se for o caso.

4.9.6. O atesto do gestor do contrato ocorrerá em até **10** (**dez**) dias úteis contados do recebimento da nota fiscal, que será encaminhada à área financeira para pagamento nos seguintes prazos:

4.9.6.1. **5** (**cinco**) dias úteis contados da apresentação da nota fiscal, nos casos dos valores que não ultrapassem o limite de que trata o inciso II do artigo 24 da Lei n. 8.666/1993;

4.9.6.2. **10** (**dez**) dias úteis contados do atesto nos demais casos.

4.9.7. Os pagamentos serão efetuados em moeda corrente nacional, já aplicados os devidos descontos e glosas, sendo efetuada a retenção na fonte dos tributos e contribuições elencados na legislação aplicável.

4.9.8. O prazo de pagamento será interrompido nos casos em que haja necessidade de regularização do documento fiscal, o que será devidamente apontado pelo CONTRATANTE.

4.9.8.1. A contagem do prazo previsto para pagamento será iniciada a partir da respectiva regularização.

4.9.9. O depósito bancário produzirá os efeitos jurídicos da quitação da prestação devida.

4.9.10. Nenhum pagamento será efetuado enquanto pendente o cumprimento de qualquer obrigação imposta à CONTRATADA, inclusive em virtude de penalidade ou inadimplência.

4.9.11. No caso de eventual atraso no pagamento sem que a CONTRATADA tenha concorrido para tal, haverá incidência de atualização monetária, sobre o valor devido, *pro rata temporis*, ocorrida entre a data limite estipulada para pagamento e a da efetiva realização. Para esse fim, será utilizada a variação acumulada do IPCA, calculado e divulgado pelo Instituto Brasileiro de Geografia e Estatística/IBGE.

4.9.12. O mesmo critério de correção será adotado em relação à devolução dos valores recebidos indevidamente pela CONTRATADA, bem como em decorrência de atrasos no recolhimento de multas eventualmente aplicadas.

4.10. Glosas

4.10.1. O não cumprimento dos níveis de qualidade do Serviço de Suporte Técnico por ocorrência, independentemente das Sanções Administrativas previstas no Contrato, implicará em redutor sobre o valor mensal do serviço de suporte técnico (glosa), nos seguintes casos:

4.10.1.1. Glosa de **5% (cinco por cento)**, calculada sobre o valor mensal do serviço de suporte técnico, para cada hora de atraso, pela não resolução dos chamados com **severidade alta**, limitada até **06 (seis)** horas de atraso.

4.10.1.2. Glosa de **3% (três por cento)**, calculada sobre o valor mensal do serviço de suporte técnico, para cada hora de atraso, pela não resolução dos chamados com **severidade média**, limitada até **10 (dez)** horas de atraso.

4.10.1.3. Glosa de **1% (um por cento)**, calculada sobre o valor mensal do serviço de suporte técnico, para cada hora de atraso, pela não resolução dos chamados com **severidade baixa**, limitada até **30 (trinta)** horas de atraso.

4.10.1.4. Glosa de **2% (dois por cento)**, calculada sobre o valor mensal do serviço de suporte técnico, para cada hora de atraso, no início do atendimento dos chamados com **severidade alta**, limitada até **02 (duas)** horas de atraso, a partir desse prazo será aplicada a glosa por atraso na resolução do chamado.

4.10.1.5. Glosa de **1% (um por cento)**, calculada sobre o valor mensal do serviço de suporte técnico, para cada hora de atraso, no início do atendimento dos chamados com **severidade média**, limitada até **06 (seis)** horas de atraso, a partir desse prazo será aplicada a glosa por atraso na resolução do chamado.

4.10.1.6. Glosa de **0,5% (cinco décimos por cento)**, calculada sobre o valor mensal do serviço de suporte técnico, para cada hora de atraso, no início do atendimento dos chamados com **severidade baixa**, limitada até **24 (vinte e quatro)** horas de atraso, a partir desse prazo, será aplicada a glosa por atraso na resolução do chamado.

4.10.2. Nos casos em que os atrasos forem superiores aos limites previstos nos subitens anteriores, além da aplicação das glosas previstas, a cada nova ocorrência a CONTRATADA sofrerá primeiramente a Sanção Administrativa de advertência citada no item 4.11.1.1.

4.10.2.1. No caso de reincidência, aplicar-se-á a respectiva penalidade de mora prevista nos itens 4.11.1.8, 4.11.1.9, 4.11.1.10 e 4.11.1.11, a depender do caso.

4.10.3. Independentemente do descumprimento dos atrasos previstos nos subitens do item 4.10, o limite de glosas mensais será de até **30% (trinta por cento)** do valor mensal do serviço de suporte técnico.

4.10.4. .A aplicação da glosa servirá ainda como indicador de desempenho da CONTRATADA na execução dos serviços

4.10.5. O faturamento do serviço de suporte técnico deverá ser mensal, mediante apresentação de nota de cobrança consolidada para todos os *softwares* e equipamentos da solução, já descontadas as glosas eventualmente aplicadas em função do não atendimento dos níveis de qualidade definidos no contrato, determinando o valor total do serviço para o mês.

4.10.6. No caso de aplicação de glosa referente à demora na conclusão de chamados do mesmo nível de severidade, para qualquer componente da solução, durante **3 (três)** meses consecutivos, ou **5 (cinco)** meses intervalados durante os últimos 12 meses, serão aplicadas as sanções administrativas previstas no contrato.

4.10.7. No caso de discordância das glosas aplicadas, a CONTRATADA deverá apresentar o recurso que será analisado pela Área Administrativa.

4.10.8. Se a decisão da Administração for favorável ao recurso da CONTRATADA, a mesma emitirá a nota de cobrança adicional para que seja efetuado o pagamento referente ao valor glosado.

4.10.9. A nota de cobrança emitida pela CONTRATADA deverá ser atestada pelo Gestor do Contrato e encaminhada para a área financeira efetuar o pagamento, acompanhada da documentação comprobatória das glosas

4.11. Sanções

4.11.1. No caso de atraso injustificado ou inexecução total ou parcial do compromisso assumido com o CONTRATANTE, as sanções administrativas aplicadas à CONTRATADA serão:

4.11.1.1. Advertência por escrito, no caso previsto no subitem 4.10.2 e/ou quando do não cumprimento de quaisquer das obrigações contratuais;

4.11.1.2. Multa moratória no percentual correspondente a **0,05% (cinco centésimos por cento)**, calculada sobre o valor total da contratação, por dia de atraso na entrega do plano de implantação e da apresentação do preposto, gerente de projetos e responsável técnico, além do prazo máximo definido no ANEXO III - CRONOGRAMA DE IMPLANTAÇÃO, até o limite de **30 (trinta**) dias corridos, a partir do qual poderá ficar caracterizada a inexecução total ou parcial do contrato.

4.11.1.3. Multa moratória no percentual correspondente a **0,1% (um décimo por cento)**, calculada sobre o valor total da contratação, por dia de atraso na entrega de todos os equipamentos, *softwares* e equipamentos necessários da solução, além do prazo máximo definido no ANEXO III - CRONOGRAMA DE IMPLANTAÇÃO, até o limite de **30 (trinta)** dias corridos, a partir do qual poderá ficar caracterizada a inexecução total ou parcial do contrato.

4.11.1.4. Multa moratória no percentual correspondente a **0,1% (um décimo por cento)**, calculada sobre o valor total da contratação, por dia de atraso na conclusão da etapa de instalação e configuração da solução, além dos prazos máximos definidos no ANEXO III - CRONOGRAMA DE IMPLANTAÇÃO até o limite de **30 (trinta)** dias corridos, a partir do qual poderá ficar caracterizada a inexecução total ou parcial do contrato.

4.11.1.5. Multa moratória no percentual correspondente a **0,5% (meio por cento)**, calculada sobre o valor total do serviço de transferência de conhecimento, por dia de atraso na conclusão do serviço de transferência de conhecimento, além do prazo máximo definido informado ao CONTRATANTE, até o limite de **30 (trinta)** dias corridos, a partir do qual poderá ficar caracterizada a inexecução parcial do contrato.

4.11.1.6. Multa moratória no percentual correspondente a **0,2% (dois décimos por cento)**, por dia de atraso, até o limite de **30 (trinta)** dias corridos, calculada sobre o valor da garantia contratual, no caso de atraso injustificado na sua entrega, nos termos do item Garantia Contratual, a partir do qual poderá ficar caracterizada a inexecução parcial do contrato.

4.11.1.7. Multa moratória no percentual correspondente a **0,1% (um décimo por cento)**, calculada sobre o valor total da contratação, por dia de atraso no caso de descumprimento das obrigações referentes a reparação de falhas de funcionamento dos componentes da solução previstas no serviço de garantia da solução, até o limite de **30 (trinta)** dias corridos, a partir do qual poderá ficar caracterizada a inexecução total ou parcial do contrato.

4.11.1.8. Poderá ser aplicada multa moratória de **5% (cinco por cento)**, calculada sobre o valor mensal do serviço de suporte técnico, para cada hora de atraso, pela reincidência da não resolução dos chamados com **severidade alta**, limitada até **06 (seis)** horas de atraso.

4.11.1.9. Poderá ser aplicada multa moratória de **3% (três por cento)**, calculada sobre o valor mensal do serviço de suporte, para cada hora de atraso, pela reincidência da não resolução dos chamados com **severidade média**, limitada até **10 (dez)** horas de atraso.

4.11.1.10. Poderá ser aplicada multa moratória de **1% (um por cento)**, calculada sobre o valor mensal do serviço de suporte técnico, para cada hora de atraso, pela reincidência da não resolução dos chamados com **severidade baixa**, limitada até **30 (trinta)** horas de atraso.

4.11.1.11. Multa por mora no percentual correspondente a **5% (cinco por cento)**, calculada sobre o custo mensal fixo da contratação, por ocorrência, no caso de aplicação de glosa referente ao mesmo indicador de Nível Mínimo de Serviço, durante 3 (três) meses consecutivos, ou 5 (cinco) meses intervalados durante os últimos 12 (doze) meses. Após a 5ª (quinta) aplicação desta sanção ao longo da execução contratual, poderá ser considerado inexecução parcial ou total do contrato;

4.11.1.12. A inexecução parcial ou total deste instrumento, por parte da CONTRATADA, poderá ensejar a rescisão contratual ou a aplicação da **multa compensatória**, no percentual de **20% (vinte por cento)** sobre o valor da parcela inadimplida.

4.11.1.13. O disposto nos itens anteriores não prejudicará a aplicação de outras penalidades a que esteja sujeita a CONTRATADA, nos termos dos artigos 87 e 88 da Lei nº 8.666/1993.

4.11.1.14. Suspensão temporária de participar de licitações e impedimento de contratar com o Conselho da Justiça Federal;

4.11.1.15. Declaração de inidoneidade para licitar ou contratar com a Administração Pública.

4.11.2. A não manutenção das condições de habilitação da Contratada ao longo da execução do contrato, poderá ensejar a **RESCISÃO CONTRATUAL UNILATERAL** pelo Conselho da Justiça Federal após regular procedimento administrativo, resguardado à Contratada o direito ao contraditório e à ampla defesa. Na hipótese de rescisão motivada pelo disposto neste item, poderá ser aplicada a multa compensatória;

4.11.3. A reincidência da aplicação de multa ou advertência dará direito ao CONTRATANTE à rescisão contratual unilateral.

4.11.4. As multas porventura aplicadas serão descontadas da garantia ofertada ou cobradas diretamente da Contratada, amigável ou judicialmente, e poderão ser aplicadas cumulativamente às demais sanções previstas nesta cláusula.

4.11.5. A aplicação das sanções previstas nesta cláusula será realizada mediante processo administrativo específico, assegurado o contraditório e a ampla defesa, com a respectiva comunicação da penalidade à CONTRATADA.

4.11.6. As penalidades serão obrigatoriamente registradas no SICAF e sua aplicação será precedida da concessão da oportunidade de ampla defesa para o adjudicatário, na forma da lei.

4.11.7. Os prazos de adimplemento das obrigações contratadas admitem prorrogação nos casos e condições especificados no § 1º do art. 57 da Lei 8.666/93, em caráter excepcional, sem efeito suspensivo, devendo a solicitação ser encaminhada por escrito, com antecedência mínima de 1 (um) dia do seu vencimento, anexando-se documento comprobatório do alegado pela Contratada.

4.11.8. Eventual pedido de prorrogação deverá ser encaminhado ao CJF preferencialmente na forma eletrônica.

4.11.8.1. A critério da autoridade competente do CONTRATANTE, com fundamento nos princípios da proporcionalidade e razoabilidade, as penalidades poderão ser relevadas ou atenuadas, em razão de circunstâncias fundamentadas, mediante comprovação dos fatos e, desde que formuladas por escrito, no prazo máximo de **5 (cinco)** dias úteis, contados da data da notificação da CONTRATADA.

4.11.9. Serão considerados injustificados os atrasos não comunicados tempestivamente ou indevidamente fundamentados, e a aceitação da justificativa ficará a critério do Contratante.

4.12. Garantia contratual

4.12.1. Para segurança do Contratante quanto ao cumprimento das obrigações contratuais A CONTRATADA deverá apresentar garantia equivalente a **5% (cinco por cento)** do valor total do contrato, no prazo de até **20 (vinte)** dias úteis, a contar da assinatura do Contrato, em uma das seguintes modalidades:

4.12.1.1. Caução em dinheiro ou em títulos da dívida pública, emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda;

4.12.1.2. Seguro-garantia;

4.12.1.3. Fiança bancária.

4.12.2. O pedido de prorrogação deverá ser solicitado pela Contratada dentro do prazo inicialmente estabelecido, sob pena de ser-lhe imputada multa.

4.12.3. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de prejuízos advindos do não cumprimento do contrato, multas punitivas aplicadas à CONTRATADA, prejuízos diretos causados ao CONTRATANTE decorrentes de culpa ou dolo durante a execução do contrato e obrigações previdenciárias e trabalhistas não honradas pela CONTRATADA.

4.12.4. Caso a garantia prestada pela CONTRATADA seja nas modalidades seguro-garantia ou fiança bancária, ela deverá prever, expressamente, a cobertura indicada no parágrafo acima.

4.12.5. O número do contrato garantido e/ou assegurado deverá constar dos instrumentos de garantia ou seguro a serem apresentados pelo garantidor e/ou segurador.

4.12.6. A garantia prestada pela CONTRATADA deverá ter validade de três meses após o término da vigência contratual e somente será liberada ou restituída no prazo máximo de noventa dias, depois de expirado o prazo de vigência do Contrato ante a comprovação de que a empresa pagou todas as verbas rescisórias trabalhistas decorrentes da contratação. Caso esse pagamento não ocorra até o fim do segundo mês após o encerramento da vigência contratual, a garantia será utilizada para o pagamento dessas verbas trabalhistas diretamente pela Administração.

4.12.7. Quando a garantia for apresentada em dinheiro, ela será atualizada monetariamente, conforme os critérios estabelecidos pela instituição bancária em que for realizado o depósito.

4.12.8. Aditado o contrato, prorrogado o prazo de sua vigência ou alterado o seu valor, ou reduzido o valor da garantia em razão de aplicação de qualquer penalidade, a CONTRATADA fica obrigada a apresentar, no prazo de 20 (vinte) dias úteis, contados do evento que deu ensejo à alteração, garantia complementar ou substituta, no mesmo percentual e modalidades constantes desta Seção.

4.12.9. Em caso de prorrogação do prazo contratual, a garantia será liberada após a apresentação da nova garantia e da assinatura de termo aditivo ao Contrato.

4.12.10. É de inteira responsabilidade da Contratada a renovação da garantia prestada, quando couber, estando sua liberação condicionada ao término das obrigações contratuais com o CJF.

4.13. Propriedade intelectual

4.13.1. A CONTRATADA deverá:

4.13.1.1. Por se tratar de solução de TI de propriedade de terceiros com fornecimento de solução para Gerenciamento de Acesso Privilegiado com licenciamento perpétuo e de serviço de suporte técnico, não há requisitos a serem especificados quanto ao aspecto propriedade intelectual.

4.13.1.2. Realizar a transferência de conhecimento para o CONTRATANTE acerca das soluções implementadas durante a vigência do contrato;

4.13.1.3. Possibilitar a migração de dados das soluções integrantes do objeto contratual para padrão aberto com capacidade de ser reconhecida por *softwares* compatíveis com tal padrão, com vistas

a diminuir a dependência tecnológica em relação à CONTRATADA e em observância ao princípio da eficiência na Administração Pública consoante a deliberação relativa ao item 9.4.1.9 do Acórdão 1.937/2003-TCU-Plenário.

4.14. Confidencialidade de informações

4.14.1. A CONTRATADA compromete-se a manter em caráter confidencial, mesmo após a eventual rescisão do contrato, todas as informações relativas à:

4.14.1.1. Política de segurança adotada pelo CONTRATANTE e configurações de hardware e *software* decorrentes.

4.14.1.2. Qualquer dado pessoal ou dado pessoal sensível obtido na execução do contrato.

4.14.1.3. Processo de instalação, configuração e customizações de produtos, ferramentas e equipamentos em atendimento aos itens de segurança constantes do(s) objeto(s) instalado(s).

4.14.1.4. Qualquer informação do CONTRATANTE que venha tomar conhecimento em razão da execução dos serviços.

4.14.1.5. A CONTRATADA deverá concordar e assinar o Termo de Confidencialidade (ANEXO VI), entregando o documento assinado pelo representante legal da empresa, com firma reconhecida.

4.15. Impacto ambiental decorrente da contratação e critérios de sustentabilidade

4.15.1. A CONTRATADA será responsabilizada por qualquer prejuízo que venha causar ao CONTRATANTE em virtude de ter suas atividades suspensas, paralisadas ou proibidas por falta de cumprimento de normas ligadas ao produto objeto do presente Termo de Referência.

4.15.2. A CONTRATADA deverá, no tocante às tecnologias assistivas, quando couber, observar o disposto nos arts. 3º, 7º e 14 da Resolução CNJ n. 230, de 22 de junho de 2016.

4.15.3. 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, segurança e acessibilidade do produto elencado neste Termo de Referência.

ANEXO I - ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO

A solução para Gerenciamento de Acesso Privilegiado (*Privileged Access Management - PAM*) para proteção dos ambientes computacionais do Conselho da Justiça Federal - CJF, contemplando licenciamento perpétuo de *software* e fornecimento de equipamento(s), serviços de instalação e configuração, transferência de conhecimento, suporte técnico mensal e garantia para 48 (quarenta e oito) meses, contempla quatro módulos, conforme especificados adiante.

1. Módulo - Cofre de Senha

1.1. A solução deve ser licenciada de forma a atender os quantitativos mínimos descritos a seguir:

1.1.1. Quantidade de servidores Linux: 600;

1.1.2. Quantidade de servidores Microsoft Windows: 150;

1.1.3. Quantidade de estações de trabalho Microsoft Windows: 550;

1.1.4. Quantidade de estações de trabalho Linux: 30;

1.1.5. Quantidade de ativos de rede (switches, roteadores, firewalls, controladores, balanceadores, WAF e outros): 40;

1.1.6. Quantidade de instâncias de bancos de dados: 25;

1.1.7. Quantidade de usuários do cofre de senhas: 40;

1.1.8. Quantidade de aplicações com senha de banco de dados armazenada localmente: 15.

1.2. A solução deve suportar a implementação no parque computacional do CONTRATANTE relacionado no ANEXO II - RESUMO DO AMBIENTE DE TI.

1.3. A solução deve ser implantada localmente nas instalações do CONTRATANTE, com modelo de alta disponibilidade, continuidade de negócios e formas de recuperação de desastre.

1.4. A solução deve prover alta disponibilidade para as funcionalidades deste módulo com opção ativo/passivo ou ativo/ativo, com failover automático para todas as arquiteturas de implantação, com todas as licenças válidas e com garantia igual ao do objeto desta contratação e sem custos adicionais para o CONTRATANTE.

1.5. A solução deve contemplar a expansão, incremento ou melhoria dos métodos utilizados para alta disponibilidade sem qualquer custo adicional de licenciamento da solução para o CONTRATANTE.

1.6. Todos os controles de alta disponibilidade da solução devem ser feitos via interface gráfica, sem depender de comandos manuais, scripts ou adaptações.

1.7. A solução deve realizar gerência da sincronização de dados dos servidores/appliances da solução de forma nativa pela solução sem necessidade de intervenção manual.

1.8. A solução deve possuir a capacidade de operação de todas as funcionalidades a partir de nós (servidores) físicos e virtuais, permitindo arranjos do tipo: físico-físico ou físico-virtual, sendo que um dos nós ofertados pela CONTRATADA para a solução deve ser físico, obrigatoriamente.

1.9. A solução deve auxiliar no atendimento da Lei Geral de Proteção de Dados (LGPD) no que se refere a:

1.9.1. Determinação de como os dados deverão ser tratados, mantidos e protegidos e a quem responsabilizar em caso de descumprimento;

1.9.2. Proteção do acesso a dados pessoais;

1.9.3. Responsabilização pessoal e resposta a incidentes;

1.9.4. Aplicação de boas práticas de governança, através de regras que deverão respeitar os preceitos da lei, de maneira a mitigar os riscos inerentes ao tratamento de dados e implementar e demonstrar a efetividade das políticas de segurança relacionadas ao tratamento de dados.

1.10. A solução deverá operar de forma integrada, ou seja, os softwares, equipamentos e demais componentes fornecidos, bem como as configurações aplicadas pela CONTRATADA, deverão operar como um conjunto plenamente ajustado, de forma a garantir gerenciamento integrado, desempenho, disponibilidade e funcionalidades adequados aos requisitos do CONTRATANTE.

1.11. A solução deve prover mecanismos de atualização de segurança de forma automática e sob demanda por meio de interface gráfica intuitiva.

1.12. A solução deve disponibilizar console de configuração unificada para gerenciamento de contas e ativos agregados ao cofre de senhas.

1.13. A solução não deve depender da instalação de agentes para realizar a troca de senhas ou a gravação de sessão.

1.14. A solução deve ser capaz de descobrir credenciais privilegiadas utilizadas por serviços e processos automatizados.

1.15. A solução deve propagar as senhas geradas de forma aleatória onde quer que estas estejam referenciadas.

1.16. A solução deve ter a capacidade de gerenciar credenciais de sistemas localizados em múltiplas localidades geográficas ou domínios distintos.

1.17. A solução deve possuir interface única para gerenciamento de senhas e sessões, implementada em HTM5 ou cliente único compatível com sistema operacional Microsoft Windows 10 e superiores.

1.18. A solução deve possibilitar a integração com ferramentas de Service Desk e de Gestão Mudança com possibilidade de validação de critérios pré-definidos para liberação de acesso.

1.19. A solução deve gerenciar de forma segura senhas utilizadas por contas de serviço, evitando a utilização de senhas em texto claro por scripts ou rotinas dos equipamentos.

1.20. A solução deve garantir a aplicação exclusiva de privilégios adequados, provendo acesso às senhas das contas privilegiadas somente ao pessoal autorizado.

1.21. A solução não deve limitar o quantitativo de contas que podem ser gerenciadas em um dispositivo licenciado.

1.22. A solução, em um dispositivo licenciado, deve contemplar sua expansão, incremento ou melhoria sem qualquer custo adicional de licenciamento da solução para o CONTRATANTE.

1.23. A solução deve permitir a opção de implementar o gerenciamento de troca de senhas em redes separadas e dispositivos remotos.

1.24. Deve incorporar medidas de segurança, incluindo criptografia a fim de proteger a informação em trânsito entre os módulos distribuídos e entre as aplicações WEB dos usuários finais.

1.25. Deve permitir, através de interface gráfica, administração e configuração de integrações com dispositivos e/ou plataformas que não são disponibilizadas nativamente, sem a necessidade de serviços profissionais de terceiros.

1.26. A solução deve permitir que o administrador configure a comunicação com aplicações de terceiros utilizando scripts, linguagens de programação diversas e aceite protocolos variados incluindo, no mínimo, SSH e HTTP/HTTPS.

1.27. A solução deve ser disponibilizada com um SDK (*Software Development Kit*) ou API (*Application Programming Interface*) que pode ser configurado para permitir que aplicações possam:

1.27.1. Solicitar credenciais sob demanda ao invés de utilizar credenciais estáticas;

1.27.2. Atualizar informações de contas automaticamente no banco de dados de senhas;

1.27.3. Inscrever automaticamente em sistemas alvo sem aguardar por atualizações dinâmicas;

1.28. A solução deve proteger as senhas de credenciais compartilhadas que seriam normalmente armazenadas em planilhas e arquivos em texto claro.

1.29. Deve oferecer em sua aplicação diferentes visões e opções de acordo com as permissões dos usuários, mostrando, por exemplo, apenas as funcionalidades delegadas àquele usuário.

1.30. A solução deve permitir a configuração e emissão de alertas disparados automaticamente pelo sistema, por e-mail e SNMP, para eventos customizados pelo administrador do sistema e que contemplem, no mínimo, os dos seguintes casos:

1.30.1. Parada de serviços essenciais;

1.30.2. Alcance do limite de processamento da CPU;

1.30.3. Alcance do limite de processamento da memória;

1.30.4. Alcance do limite de capacidade do armazenamento de dados;

1.31. Caso a solução seja estruturada em componentes, nenhum deles deve conter senhas em texto claro para autenticação.

1.32. Deve permitir a formação de Grupos de Usuários e Dispositivos, bem como a atribuição de Privilégios de Acesso a esses Grupos, onde esses Privilégios de Acessos possam ser atribuídos por critérios como tipo de dispositivo, marca, modelo, fabricante, localidade ou grupo abertos definidos a critério do administrador na própria ferramenta.

1.33. A solução deve garantir que a senha gerada tenha a grafia diferente do nome da conta correspondente.

1.34. Permitir a determinação de quais símbolos estão excluídos ou exclusivamente permitidos na composição da senha.

1.35. A solução deve permitir que a senha seja segmentada em partes proporcionais ao número de segmentos definidos na política de segmentação da senha, seja por fracionamento da senha, seja mediante autorização por múltiplos aprovadores.

1.36. A solução deve permitir que sejam atribuídas autorizações granulares às execuções com nível administrativo em sistemas Microsoft Windows como, por exemplo, a execução de uma ou mais aplicações com nível administrativo, sem que esse privilégio seja global.

1.37. A solução deve garantir a configuração de mecanismo para que as senhas randomizadas sejam únicas para cada credencial.

1.38. A solução deve garantir a configuração de mecanismo para que determinados grupos de senhas randomizadas sejam as mesmas para cada credencial pertencente a este grupo.

1.39. A solução deve suportar em todos seus métodos de acesso, autenticação de duplo fator compatível com os métodos a seguir:

1.39.1. Algoritmo de One-time Password, compatível com os padrões HOTP: An HMAC-Based One-Time Password Algorithm (RFC 4226) e TOTP: Time-Based One-Time Password Algorithm (RFC 6238);

1.39.2. Certificado digital (x.509);

1.39.3. Aplicativos públicos de autenticação.

1.40. A solução deve ser compatível com pelo menos 02 (dois) dos seguintes métodos e padrões de criptografia:

1.40.1. AES com chaves de 256 bits;

1.40.2. FIPS 140-2;

1.40.3. Encriptação PKCS#11 ou superior por hardware utilizando dispositivos de HSM devidamente homologados pelo fabricante para a solução ofertada;

1.41. A solução deve disponibilizar a opção de autenticação utilizando os protocolos OpenID ou SAML 2.0.

1.42. A solução deve criptografar o banco de dados utilizado para o armazenamento das senhas e credenciais gerenciadas.

1.43. A solução deve possuir função de monitoramento e análise de comportamento para os sistemas e/ou dispositivos que contemplem, no mínimo, as especificações técnicas do parque computacional do CONTRATANTE.

1.44. A solução deve, a partir dos eventos coletados, montar perfis de comportamento dos usuários do sistema.

1.45. A solução deve alertar abusos e comportamentos fora dos padrões aprendidos ou mapeados.

1.46. A solução deve monitorar e exibir acessos e atividades realizadas no próprio sistema.

1.47. A solução deve detectar pelo menos os seguintes comportamentos anormais:

1.47.1. Acessos excessivos a contas privilegiadas. Quando um usuário acessa contas privilegiadas com mais frequência do que o normal, de acordo com seu perfil comportamental;

1.47.2. Alteração de senha suspeita. Quando é identificada uma solicitação para alteração ou redefinição de uma senha ignorando ação executada pela solução;

1.47.3. Acesso privilegiado a solução através de IP irregular/incomum ou desconhecido. Quando um usuário acessa contas privilegiadas de endereço IP e sub-rede incomum, de acordo com seu perfil comportamental. Caso a solução não possua alertas baseando- se em IP, deve ao menos limitar o acesso a credenciais através de redes desconhecias e possuir informação da origem do acesso em seus relatórios.

1.48. As detecções da solução não devem limitar-se a um tipo específico de comportamento anormal, possibilitando a correta demonstração de eventos complexos contemplando análise de comportamento de usuários.

1.49. A solução deve fornecer, por demanda do CONTRATANTE, funcionalidade para encerramento de sessões suspeitas por sistemas de terceiros em utilização no CONTRATANTE, tais como ferramentas de SIEM, *software* de gerenciamento de servidores, *software* de gerência de *Backup* e SGBD.

1.50. A solução deve permitir a configuração de eventos críticos a serem reportados automaticamente, baseados, no mínimo, em:

1.50.1. Comandos Linux;

1.50.2. Expressões regulares para comandos, no mínimo, em SSH;

1.51. A solução deve disponibilizar ao usuário acesso a console da solução, incluindo, no mínimo:

1.51.1. Acesso por interface WEB, sem necessidade de plug-in ou agente específico para o acesso;

1.51.2. Utilização de protocolos de comunicação totalmente criptografados, por exemplo TLS 1.2;

1.51.3. Suporte ao funcionamento dentro de redes que não estão diretamente conectadas à internet;

1.51.4. Suporte a injeção automática de credenciais, permitindo a autenticação ou elevação de privilégios para sistemas remotos, sem revelar credenciais e senhas de texto simples. Permitindo que os usuários selecionem a credencial a ser utilizada a partir de lista de credenciais que têm privilégios nos sistemas aprovados para acesso;

1.51.5. A injeção de senhas deve ser totalmente integrada com a solução de cofre de senhas corporativa, permitindo que seus usuários usem senhas com segurança durante as sessões de acesso;

1.51.6. Suportar os seguintes modos de acesso a desktops, servidores e outros sistemas remotos autônomos.

1.51.6.1. Integração com RDP (Remote Desktop Protocol) da Microsoft para realizar sessões utilizando protocolo RDP;

1.51.6.2. Acesso a dispositivos de rede habilitados para SSH/telnet;

1.51.6.3. Acesso a páginas WEB utilizando HTTP/HTTPS;

1.52. O equipamento da solução deve suportar retenção de gravações por 90 dias, considerando o no mínimo de 8 horas/dia, 5 dias por semana de gravações.

1.53. Deve armazenar os todos logs da solução por, no mínimo, 180 dias.

1.54. Todos os sistemas e recursos necessários para operação do módulo de cofre de senhas, incluindo seu banco de dados, deverão ser passíveis de plena utilização a partir de um único nó, em caso de contingência, seja ele virtual ou físico.

1.55. Não deve haver cobranças à parte no licenciamento de *software* para opção de ambiente de suporte ativo/passivo ou ativo/ativo ou arranjos de arquitetura. físico-físico, virtual-virtual e físico-virtual.

1.56. A solução deve poder ser monitorada via *software* de monitoramento utilizado pelo CONTRATANTE descrito no ANEXO II - RESUMO DO AMBIENTE DE TI.

1.57. A solução deve poder integrar-se sem custos adicionaiscom as soluções de Help Desk (ITSM) descritas no ANEXO II - RESUMO DO AMBIENTE DE TI.

1.58. A integração com a solução de Help Desk (ITSM) deve possibilitar a verificação e garantia de que todas as solicitações de *checkout* das senhas de credenciais privilegiadas sejam originadas de *tickets* válidos existentes na solução de Help Desk.

1.59. A solução deve integrar-se diretamente, sem codificação adicional ou adição de scripts, com soluções de SIEM, a fim de garantir o registro e a visualização, a partir da aplicação existente nesses sistemas, das seguintes ações, no mínimo:

1.59.1. Atividades administrativas relacionada a acesso as credenciais privilegiadas;

1.59.2. Atividades de recuperação, liberação e alterações de senhas;

1.59.3. Outras atividades de executadas pelos usuários na console web;

1.60. A solução deve utilizar um banco de dados com as melhores práticas de segurança, em ambiente “hardenizado”, com mecanismo de blindagem e criptografia do sistema operacional.

1.61. Tanto appliances virtuais quanto sistemas operacionais devem ser “hardenizados” e protegidos com firewall interno e detecção de intrusão.

1.62. Caso a solução utilize sistema operacional de terceiros, este deverá vir licenciado para a proteção interna do appliance e aplicação.

1.63. A solução deve utilizar uma arquitetura de banco de dados e aplicação que permita alta disponibilidade e mecanismos para a recuperação de desastres para todos os componentes da solução.

1.64. A solução deve permitir o *backup* e restore de seu banco de dados, bem como das configurações de *software* estabelecidas, com as seguintes capacidades:

1.64.1. Permitir a execução de tarefas de *backup* criptografado sem a necessidade de agentes de terceiros ou parada do ambiente ou comprometimento de qualquer funcionalidade; provendo assim o maior nível possível de segurança e integridade dos dados a serem copiados;

1.64.2. Permitir a execução de *backups* automatizados, permitindo a programação/agendamento de horários e configuração de locais para seu armazenamento local e remoto;

1.65. Caso a solução faça uso de mecanismos para controle e otimização da carga de trabalho interna, de modo a possibilitar o controle de parâmetros, melhorar ou ajustar o seu desempenho de acordo com as características do ambiente onde está localizado, estes mecanismos deverão ser providos pela solução.

1.66. A solução deve ser capaz de exportar a chave de criptografia ou credencial equivalente do local de armazenamento das credenciais (cofre), por meio de *backup* ou método análogo, para ser utilizada nos cenários de recuperação de desastres, de forma a conceder acesso à todas as senhas de identidades privilegiadas e dados gerenciados pela solução.

1.67. O acesso primário dos usuários à solução deve ser sempre a partir dos componentes instalados em sua rede local.

1.68. A solução deve suportar, sem necessidade de licenciamento adicional a gestão de senhas no código fonte em aplicações e scripts (AAPM) através de uma REST.

1.69. A solução deve suportar API REST, onde as aplicações consomem a senha com requisições a interface API REST, assim evitando que as senhas fiquem expostas no código fonte das aplicações.

1.70. A solução deve permitir o envio automático de logs para servidores Syslog de forma aderente ao disposto na RFC 5424 (the Syslog Protocol).

1.71. As solução deve permitir a definição de fluxos de aprovação (workflows) para obtenção de acesso às contas privilegiadas, com as seguintes características:

1.71.1. Personalização da configuração de fluxos para aprovação, de acordo com a criticidade e características da conta (como de acesso emergencial, de uso por terceiros), e aprovação de pelo menos um responsável;

1.71.2. Aprovação perante agendamento de ações administrativas, ou seja, a aprovação do acesso ocorrera em um dia, mas a liberação da senha ocorrerá de forma automática somente na data e horário previstos;

1.71.3. Substituição de senhas de identidades privilegiadas em uso por determinado serviço ou por tarefa agendada em todos os locais onde estejam sendo utilizadas;

1.71.4. Caso seja necessário, após alteração da senha de identidade privilegiada associada à um serviço, a solução deve ser capaz de reinicializar o mesmo.

1.72. A solução deve permitir o agrupamento lógico de sistemas a fim de simplificar a configuração de políticas apropriadas para diferentes tipos de sistemas alvo. Além de permitir a atualização de uma mesma conta em múltiplos sistemas-alvo com uma única tarefa de alteração de senhas.

1.73. A solução deve ser capaz de redefinir senhas individuais ou grupos de senhas sob demanda e deve ser capaz de realizar verificações agendadas e automáticas a fim de garantir que as senhas das contas gerenciadas pela solução no dispositivo de destino, correspondam às mesmas senhas armazenadas no banco de dados da solução.

1.74. A solução deve ser capaz de descobrir e alterar credenciais Microsoft Windows, incluindo contas nomeadas, administradores 'built-in' e convidados, exibindo em mapa de rede gráfico e interativo ou através de relatórios e interface de gerenciamento.

1.75. A solução deve ser capaz descobrir e alterar credenciais privilegiadas em ambientes Linux e Unix.

1.76. A solução deve identificar as contas privilegiadas com UID 0 (zero) em Linux e Unix e as contas privilegiadas através do uso do comando sudo.

1.77. A solução deve possibilitar a descoberta e alteração de contas privilegiadas usadas em serviços WEB de forma automática ou através de adaptações via

script integrados ao SDK ou API da solução. Ex: aplicações baseadas em Microsoft IIS.

1.78. A solução deve descobrir e alterar processos interdependentes e credenciais de serviço, incluindo credenciais em ambientes clusterizados.

1.79. A solução deve ser capaz de encontrar contas de usuários privilegiados que possam ser gerenciadas pela solução, permitindo que a conta descoberta seja gerenciada pela solução.

1.80. A solução deve ser capaz de substituir as senhas de identidades privilegiadas que estejam sendo utilizadas por determinado serviço em todos os locais onde estejam sendo utilizadas.

1.81. A solução deve ser capaz de realizar discovery automatizado de credencias em servidores e bancos de dados.

1.82. A descoberta automática de credenciais da solução deve ser realizada por buscas no Active Directory (AD) e/ou por ranges de endereços IP.

1.83. A solução deve descobrir e alterar credenciais do Active Directory (AD) e todos os outros serviços de diretório compatíveis com LDAP.

1.84. O gerenciamento de identidades privilegiadas deverá disponibilizar:

1.84.1. Mecanismo de retirada e devolução de contas e senhas compartilhadas;

1.84.2. Definição de tempo de validade: permitir o estabelecimento de tempo de validade para as senhas de identidades privilegiadas gerenciadas que forem requisitadas;

1.84.3. Troca automática da senha no sistema gerenciado, após a sua devolução ou após o vencimento do tempo de validade estabelecido;

1.84.4. Configuração de calendário de requisição de senhas de identidades privilegiadas com base em usuários ou grupos de usuários;

1.84.5. Troca de Senhas por Demanda: Permitir a troca de senhas nos Sistemas Gerenciados, de forma individual ou por grupos customizáveis, manualmente ou de forma automática, por agendamento.

1.85. No processo de definição da política de composição de senha, a solução deve ser capaz de:

1.85.1. Gerar senhas aleatórias com extensão de 128 (cento e vinte e oito) caracteres ou mais.

1.85.2. Utilizar caracteres alfabéticos (maiúsculos e minúsculos), numéricos e símbolos.

1.85.3. Especificar qual o tipo de caractere na composição das senhas a serem geradas;

1.85.4. Permitir a determinação de quais símbolos estão excluídos ou exclusivamente permitidos na composição da senha;

1.85.5. Garantir a configuração de mecanismo para que as senhas randomizadas sejam únicas para cada credencial;

1.85.6. Garantir a configuração de mecanismo para que determinados grupos de senhas randomizadas sejam as mesmas para cada credencial pertencente a este grupo;

1.85.7. Implementar controle de acesso baseado em papéis (roles), garantindo aderência ao princípio dos privilégios mínimos, e viabilizando a segregação de funções entre usuários de uma mesma aplicação gerenciada.

1.86. A solução não deverá permitir a abertura do cofre com chaves criptográficas geradas por seus respectivos fornecedores e/ou fabricantes.

1.87. Deve registrar cada acesso, incluindo os acessos via aplicação WEB para solicitações de senha, aprovações, *checkouts*, mudanças de delegação, relatórios e outras atividades. Devem ser registrados os acessos à console de gerenciamento tanto para configuração quanto para relatórios, bem como todas as atividades de alterações de senhas.

1.88. Todas as sessões acessadas no cofre digital devem ser gravadas, possibilitando a visualização destes vídeos na solução, com opção de armazenamento externo dos vídeos para que seja possível guardá-los por tempo indeterminado caso seja necessário.

1.89. As sessões acessadas por usuários poderão ser monitoradas pelo administrador da solução, o qual poderá bloquear e/ou interromper o acesso a qualquer tempo. Caso ocorra o bloqueio e/ou interrupção, estas ações exercidas pelo administrador também deverão ser gravadas.

1.90. A solução deve permitir a configuração de fluxo de aprovação de acordo com a criticidade e características da conta (como de acesso emergencial ou de terceiros), e aprovação de pelo menos um responsável.

1.91. A solução deve filtrar comandos executados ao longo das sessões gravadas, possibilitando pesquisar ações específicas nos vídeos gravados.

1.92. A pesquisa textual deve remeter ao momento exato em que o texto ou comando foi realizado no vídeo da gravação da sessão.

1.93. A solução deve permitir que os comandos executados em sistemas Linux e Unix monitorados sejam gravados em modo texto.

1.94. Deve ser possível colocar a sessão em quarentena ficando pendente de liberação e terminação pelo administrador ou permitir o monitoramento da sessão em tempo real permitindo sua terminação pelo administrador.

1.95. Deve possibilitar assistir o vídeo de uma sessão diretamente na solução, sem necessidade de converter em formato de vídeo ou realizar download.

1.96. Deve possibilitar sessões remotas através de programas instalados na estação de trabalho do cliente, a exemplo do Putty e RDP Client, sem obrigatoriedade de passar pela aplicação WEB ou baixar cliente adicional.

1.97. Deve permitir a inclusão de comentários em sessões gravadas, e marcar sessões como já revistas.

1.98. Conceder acesso aos sistemas utilizando "Remote Desktop" e "SSH" sem que os usuários vejam qualquer senha, garantindo que não haja necessidade de instalação de aplicações e/ou agentes nas estações dos usuários para realizar o acesso, devendo conceder acesso a:

1.98.1. Sistemas ou aplicações parametrizáveis, onde a aplicação deverá ser executada, por meio de página web, devidamente autenticada com usuário e senha pré-determinados ou recuperados da base de dados da solução, sem que haja login interativo por parte dos usuários no sistema operacional do servidor de destino, possibilitando habilitar gravação da sessão caso seja necessário. Exemplo: Executar o SQL Management Studio com credencial de SA (System Administrator) sem que o usuário conheça a senha e sem necessidade de login interativo prévio do usuário no sistema operacional do host de destino;

1.98.2. Sistemas baseados em Remote Desktop e SSH sem que os usuários vejam a senha. A senha vigente no momento (estática ou dinâmica) deverá ser provida para as aplicações ou conexões remotas devendo ser recuperadas de forma automática e transparente do banco de dados da solução.

1.98.3. As sessões acessadas podem ser monitoradas por meio de gravação de vídeos das mesmas, em formato padrão de execução da solução;

1.98.4. A solução deve permitir que um administrador possa bloquear e desbloquear, e terminar uma sessão ativa caso julgue necessário.

1.98.5. Monitorar comandos executados ao longo da sessão gravada, possibilitando pesquisar ações específicas no vídeo gravado.

1.98.6. A solução deve possuir a opção de terminar a sessão automaticamente em uma sessão SSH se o usuário digitar um comando não autorizado.

1.98.7. A solução deve permitir que as sessões SSH e RDP abertas através da solução sejam terminadas de forma automática ao expirar o tempo requisitado de sessão.

1.98.8. A solução deve suportar forçar o logoff dos usuários em sessões RDP terminadas pela solução ao final do tempo de requisição da sessão.

1.99. A solução deve fornecer relatórios de conformidade detalhados das operações realizadas pela solução, tais como:

1.99.1. Lista de sistemas gerenciados;

1.99.2. Senhas armazenadas;

1.99.3. Eventos de alteração de senha;

1.99.4. Auditoria de contas;

1.99.5. Auditoria de sistemas;

1.99.6. Auditoria de usuários;

1.99.7. Detalhes das próximas atualizações de senha programadas;

1.99.8. Sistemas que estão usando uma conta de serviço para iniciar um ou mais serviços;

1.100. A solução deve controlar o acesso aos relatórios se baseando nas permissões configuradas na solução.

1.101. A solução deve fornecer dados ad-hoc agendados, relatórios em tempo real dos usuários, contas, configuração da solução e informações sobre os processos da solução.

1.102. A solução deve apresentar relatórios com visibilidade hierárquica, contendo listas e filtros de ordenação de tal forma que os usuários possam detalhar as informações e os recursos que desejam acessar.

1.103. A solução deve fornecer relatórios de auditoria que disponibilizem detalhes das interações dos usuários com a solução, tais como:

1.103.1. Auditoria detalhada, com no mínimo, atividade de login e logoff dos usuários;

1.103.2. Alterações nas funções de delegação;

1.103.3. Adições, deleções, alterações de senhas gerenciadas pela solução;

1.103.4. Operações das senhas dos usuários, incluindo *check-in* e *checkout*, solicitações negadas e permitidas;

1.103.5. Os relatórios devem ser filtrados por período de tempo, tipo de operação, sistema, gerente e assim por diante.

1.104. A solução deve possibilitar a geração de relatórios, no mínimo, em um dos formatos a seguir:

1.104.1. Formato editável: HTML, CSV, XLSX ou XLS.

1.104.2. Formato não editável: PDF

2. Módulo - Elevação de Privilégios Servidores Linux

2.1. Deve ser capaz de garantir o controle, elevação de privilégios e bloqueio de comandos, mesmo que o acesso seja realizado diretamente no servidor de destino fazendo uso de agente instalado no sistema ou método análogo.

2.2. Deve deve implementar um modelo de delegação de privilégios mínimos, permitindo que os usuários executem qualquer comando em um nível de privilégio mais alto, desde que permitido pela política centralizada e removendo a necessidade de os usuários efetuarem logon como root.

2.3. Deve ser capaz de limitar o acesso a contas privilegiadas, permitindo que um usuário execute determinadas tarefas em um servidor Linux e Unix, sem dar acesso a contas privilegiadas, fazendo uso de agente instalado no sistema ou método análogo.

2.4. Deve prover um controle de comandos completo, possuindo a possibilidade de criar uma lista de comandos permitidos ou bloqueados (*whitelisting/blacklisting*), lista de comandos a serem alterados (criação de alias) ou prevenir que comandos sejam executados.

2.5. Deve prover meios de permitir que os usuários executem comandos específicos e conduzam sessões remotamente baseado em regras sem autenticar-se diretamente utilizando credenciais privilegiadas.

2.6. Deve permitir que os usuários executem comandos específicos e conduzam sessões remotamente com base em regras sem fazer logon como administrador ou root.

2.7. Deve oferecer suporte à políticas de acesso dinâmico utilizandofatores como hora, dia e local.

2.8. A política de acesso dinâmico permitirá que o administrador especifique:

2.8.1. Quais tarefas um usuário ou grupo de usuários pode executar.

2.8.2. De qual máquina o usuário pode iniciar uma solicitação para executar a tarefa.

2.8.3. Em quais máquinas uma tarefa pode ser executada;

2.9. Deve ser capaz de interceptar as chamadas da biblioteca relacionadas ao sistema de arquivos e permitir, proibir e auditar as chamadas. Deve permitir especificar ações (por exemplo, abrir/ler/ gravar/executar) que podem ou não ser executadas em um arquivo (usando padrões de arquivos no estilo de shell para corresponder aos arquivos) e também especificar um nível de auditoria;

2.10. Deve ser capaz de controlar, bloquear e auditar comandos executados em um script quando ele é elevado pela solução, mesmo como root;

2.11. Deve fornecer shells baseadas nas variantes Bourne e Korn de domínio público e fornecer os seguintes recursos:

2.11.1. Autorização transparente para cada comando, redirecionamento e comando interno;

2.11.2. Controle de scripts de shell;

2.11.3. Log de Entrada / Saída para toda a sessão de shell ou para comandos seletivos;

2.11.4. Registro de eventos para cada comando, redirecionamento e comando interno;

2.12. Deve fornecer capacidade de log flexível que permita controlar o que está sendo registrado, quando e onde.

2.13. Deve fornecer registro básico que registre as seguintes informações: data/hora do evento, status de aceitação e rejeição, eventos de ação de pressionamento de tecla, status da tarefa, comando que o usuário solicitou, comando executado, e o usuario que executou o comando, mesmo em casos de usuario executando comando como root.

2.14. Deve fornecer log de comandos pré-configurados ou de toda a sessão que podem ser guardados e permitindo sua reprodução como um vídeo de todos os comandos executados localmente no servidor.

2.15. Deve se integrar a ferramentas de SIEM para enviar dados do evento Aceitos e Rejeitados via Syslog.

2.16. Deve ser capaz de criptografar todo o tráfego de rede gerado, incluindo mensagens de controle, entrada que é digitada pelos usuários e saída gerada pelos comandos que são executados através dela.

2.17. Deve ser capaz de se integrar a ferramentas de HSM para usar os serviços de criptografia FIPS 140-2 Security Level 2 para obter conformidade com os requisitos e padrões de armazenamento de chaves mais rigorosos.

2.18. Deve suportar criptografia segura de log.

2.19. Deve possui uma forma de fazer integração ao Active Directory baseada em agente para vários sistemas Linux e Unix exibindo as classes e atributos de objetos.

2.20. Deve permitir que os usuários efetuem logon nos sistemas Linux e Unix usando seus nomes de usuário e senhas do Active Directory (AD), sem exigir infraestrutura adicional ou sincronização de senha.

2.21. Deve oferecer suporte à adesão nativa dos sistemas Linux e Unix ao Active Directory, sem a instalação de *software* no controlador de domínio ou a modificação do schema do Active Directory;

2.22. Deve permitir uma configuração consistente em toda a empresa, estendendo as ferramentas nativas de gerenciamento de Diretiva de Grupo (GPO) para incluir configurações específicas de diretiva de grupo para Linux e Unix.

2.23. Deve suportar várias florestas e domínios do AD;

2.24. Deve oferecer suporte ao acesso de compartilhamento de arquivos de rede remota para sistemas Linux e Unix;

2.25. Deve permitir a associação ao grupo AD para controlar centralmente o acesso ao servidor e à estação de trabalho. Fornecendo uma única política de senha definida no AD para todos os sistemas associados, incluindo o Kerberos SSO para SAP, Siebel e outros aplicativos corporativos importantes.

2.26. Deve oferecer suporte à autenticação Kerberos para máquinas Linux e Unix ingressadas no domínio AD.

2.27. Deve oferecer suporte à autenticação segura de cartão inteligente (smart cards), de modo que um sistema remoto executando o agente possa estabelecer um túnel seguro entre a estação de trabalho do usuário e o servidor de destino. O leitor de cartão inteligente do usuário pode ser conectado ao host de destino por meio desse túnel seguro, para que o sistema remoto atue como se o leitor de cartão inteligente estivesse fisicamente conectado diretamente à própria máquina;

2.28. Deve possuir a capacidade de ativar o logon único para qualquer aplicativo corporativo da plataforma Linux e Unix que suporte Kerberos ou LDAP, incluindo Samba, Apache, SSH, Websphere, JBoss, Tomcat, Oracle e MySQL.

2.29. Deve ser capaz de detectar o controlador de domínio e o servidor de catálogo global para autenticação;

2.30. Deve oferecer suporte à autenticação offline quando a conectividade de rede entre máquinas Linux e Unix e controladores de domínio não estiverem disponíveis.

2.31. A autenticação dos servidores Linux e Unix ao Active Directory NÃO deve depender de conexão ao cofre digital.

2.32. Deve oferecer suporte ao logon único (SSO) usando o cliente SSH, como o Putty, aos servidores Linux e Unix através de uma máquina Microsoft Windows parte do domínio do Active Directory.

2.33. Deve suportar a configuração de colocar uma mensagem no arquivo /etc/issue através do GPO para máquinas do Linux e Unix unidas ao domínio do AD.

2.34. Deve oferecer suporte à definição do prompt de senha personalizado por meio do GPO para máquinas do Linux e Unix unidas ao domínio do AD para distinguir o AD e a conta de usuário local.

2.35. A comunicação entre o sistema cliente e o Controlador de Domínio Active Directory deve ser assinada e criptografada.

2.36. Deve fornecer painéis e relatórios gerenciais.

3. Módulo - Elevação de Privilégios Servidores Microsoft Windows

3.1. Deve possuir agente local para Servidores Microsoft Windows que permita a remoção do privilégio administrativo dos usuários, permitindo a elevação de privilégios através de regras pré-definidas.

3.2. Deve possuir mecanismos para fazer a elevação de privilégios de aplicações autorizadas no Microsoft Windows, a fim de atribuir o direito de administrador somente as tarefas autorizadas para cada tipo de usuário (mesmo que o mesmo não tenha direitos de administrador) e implementar a segregação de funções.

3.3. Deve permitir a criação regras de privilégios, onde o privilégio de administrador é concedido para cada aplicativo/processo autorizado, de forma que cada usuário, mesmo com o privilégio de usuário convencional (usuário standard) possa instalar certos programas permitidos, possa executar os aplicativos legados que requerem o privilégio de administrador para funcionar, controles ActiveX, etc.

3.4. Deve permitir a remoção de direitos de administração local dos usuários e grupos de maneira segmentada.

3.5. Deve suportar que os aplicativos sejam agrupados logicamente em vez de criar uma regra para cada aplicativo. Estes grupos de aplicativos devem permitir sua reutilização em diferentes políticas.

3.6. Deve permitir criar uma lista branca (whitelist), onde seja possível configurar todos os aplicativos que podem ser executados e qualquer outra aplicação fora desta lista automaticamente seja bloqueada.

3.7. Caso a solução permita a execução dos aplicativos em lista branca (whitelist) sem escaneamento prévio por solução de segurança do CONTRATANTE, a solução deverá prover função de descoberta de malware em cada processo em execução, através da comparação automática do hash com fabricantes de antivírus (integração com virustotal) sem que o administrador precise executar a submissão manual.

3.8. Deve permitir, caso configurado, que um usuário faça o clique com o botão direito do mouse e possa executar uma aplicação com direitos de administrador, sem ter que saber a senha da conta local administrador (privilégio sob demanda, com justificativas)

3.9. Deve possuir uma integração com Controle de Conta de Usuário do Microsoft Windows (UAC), e conter relatórios do uso de prompts aos usuários feitos pelo UAC.

3.10. Todas as políticas dever ser mantidas em cache e serem aplicadas ao endpoint mesmo que o mesmo não esteja conectado à rede corporativa.

3.11. Deve permitir a execução automática dos aplicativos de lista branca (whitelist) implantados por ferramentas de implantação de *software* por administradores confiáveis, como o System Center Configuration Manager (SCCM).

3.12. Deve suportar a elevação segura de tipos de arquivos hospedados, como o Microsoft Management Consoles (MMC), sem depender de linha de comandos.

3.13. Deve suportar a elevação de scripts aprovados, incluindo scripts do tipo "*Batch Files*", scripts do Microsoft Windows e Microsoft PowerShell.

3.14. Deve permitir elevação de scripts e comandos individuais do Microsoft PowerShell ou bloqueio de execução da aplicação do CMD executados em uma máquina remota.

3.15. Deve possuir auditoria granular de todas as atividades remotas.

3.16. Deve fornecer proteção de grupos de privilégios (banco de dados SAM) em cada endpoint, o que significa que os usuários não podem adulterar ou modificar grupos privilegiados locais, como o grupo Administradores ou Power Users.

3.17. Deve evitar que anexos de e-mail maliciosos ou documentos baixados iniciem executáveis desconhecidos que possam infectar o sistema do cliente e criptografar dados dos usuários.

3.18. Deve impedir que processos ou executáveis desconhecidos executados a partir de um site devem ser impedidos de serem executados.

3.19. Deve impedir que quando o usuário abre uma sessão do navegador ou manipuladores de documentos, como o Microsoft Office ou o Adobe Reader, os processos desconhecidos não devem ter permissão para acessar e adulterar dados privados.

3.20. Deve forçar que conteúdo não confiável não deve poder fazer modificações no sistema operacional, no registro e nos aplicativos instalados.

3.21. Através de regras pré-definidas, deve forçar que quando um usuário abre um navegador ou um manipulador de documentos, somente os processos confiáveis e processos filho devem ser permitidos, e qualquer aplicativo potencialmente mal-intencionado será impedido de iniciar.

3.22. Deve permitir que mensagens customizadas sejam mostradas antes que uma aplicação seja executada ou bloqueada.

3.23. Deve suportar adição múltiplas mensagens, estas mensagens devem possibilitar edição e suportar múltiplas linguagens.

3.24. Deve consolidar os logs a soluções de SIEM para correlação e notificação de eventos.

3.25. Deve identificar o uso de aplicativos e a tentativa de uso, incluindo aplicativos bloqueados e restritos.

3.26. Deve relacionar os aplicativos instalados fornecendo informações sobre implantação e uso de políticas.

3.27. Deve fornecer painéis e relatórios gerenciais.

4. Módulo - Elevação de Privilégios em Estações de Trabalho (Desktops)

4.1. Deve possuir agente local para desktop Microsoft Windows e Linux que permita a remoção do privilégio administrativo dos usuários, permitindo a elevação de privilégios através de regras pré-definidas.

4.2. Deve possuir mecanismos para fazer a elevação de privilégios de aplicações autorizadas no Microsoft Windows, a fim de atribuir o direito de administrador somente as tarefas autorizadas para cada tipo de usuário (mesmo que o mesmo não tenha direitos de administrador) e implementar a segregação de funções.

4.3. Deve permitir a criação de regras de privilégios, onde o privilégio de administrador é concedido para cada aplicativo/processo autorizado, de forma que cada usuário, mesmo com o privilégio de usuário convencional (usuário standard) possa instalar certos programas permitidos, possa executar os aplicativos legados que requerem o privilégio de administrador para funcionar, controles ActiveX, etc.

4.4. Deve possuir uma integração com Controle de Conta de Usuário do Microsoft Windows (UAC), e conter relatórios do uso de prompts aos usuários feitos pelo UAC.

4.5. Deve permitir criar uma lista branca (whitelist), onde seja possível configurar todos os aplicativos que podem ser executados e qualquer outra aplicação fora desta lista automaticamente seja bloqueada.

4.6. Caso a solução permita a execução dos aplicativos em lista branca (whitelist) sem escaneamento prévio por solução de segurança do CONTRATANTE, a solução deverá prover função de descoberta de malware em cada processo em execução, através da comparação automática do hash com fabricantes de antivírus (integração com virustotal) sem que o administrador precise executar a submissão manual.

4.7. Deve manter as políticas em cache e aplicadas ao desktop mesmo que os desktop não esteja conectado à rede corporativa.

4.8. Deve permitir elevação de scripts e comandos individuais do Microsoft PowerShell ou bloqueio de execução da aplicação do CMD executados em uma máquina remota.

4.9. Deve fornecer proteção de grupos de usuários privilegiados em cada estação, o que significa que os usuários não podem adulterar ou modificar grupos privilegiados locais, como o grupo Administradores ou Power Users.

4.10. Deve permitiro mapeamento de compartilhamento de rede com usuário diferente do usuário logado na estação.

4.11. Deve fornecer painéis e relatórios gerenciais.

4.12. Deve possuir capacidade de identificar tentativa de modificação de grupos locais privilegiados nos desktops.

ANEXO II - RESUMO DO AMBIENTE DE TI

O quadro a seguir apresenta os sistemas operacionais, aplicativos, *softwares* de gerência, SGBDs, servidores de aplicação, servidores web e ferramentas em uso no CJF

Software	Nome / Versão	Descrição
Sistema Operacional	Microsoft Windows 2003, 2008, 2008 R2, 2012 e 2019 Server	Sistema Operacional de 32 bits e 64 bits
	Microsoft Windows 7 Pro e Windows 10	Sistema Operacional de 64 bits
	Suse Linux 9,10, 11, 12 e 15	Sistema Operacional de 32 bits e 64 bits
	IBM AIX 6.1	Sistema Operacional de 32 bits
	Oracle Linux 7	Sistema Operacional de 64 bits
	CentOS 7	Sistema Operacional de 32 bits e 64 bits
	Red Hat Linux 5, 6 e 7	Sistema Operacional de 32 bits e 64 bits
Ambiente de Virtualização, Orquestração e Automação de Nuvem	VCloud Suite Standard VMware vCenter VMware vSphere ESXi 6.5 U3 vRealize Automation VRealize Business Vrealize Log Insight vRealize Network Insight VRealize Operations Insight	Ferramenta de virtualização, orquestração e automação de nuvem.
Ambiente de Proteção de Dados (*Backup*)	Networker 9.1 Data Protection Advisor 6.4.0 Data Protection Central 19.1	Ferramenta de *Backup*
Base de Conhecimento	Service Now CA SDM	Ferramenta de documentação e base de conhecimento
Servidores de Aplicações (Middleware)	IIS 6.0 (Internet Information Services)	Servidor de Aplicações Microsoft ASP / HTML
	Apache 2.2.12	Servidor de Aplicações Apache / PHP
	Tomcat 5, 6 e 7	Servidor de Aplicações Java
	OAS 10g v10.1.35	Servidor de Aplicações Oracle

Software	Nome / Versão	Descrição
	Zope/Plone	Servidor de Aplicações Zope
	JBoss 4, 5.1.0, EAP 6 e EAP 7	Servidor de Aplicações Jboss Java
	Oracle APEX 19.1.00.15	Oracle Application Express
Ambiente de Automação DevOps	Jenkins 2.190.1	Automação de deploys
Ambiente de Containers	Docker Redhat Openshift Kubernets	Containers de aplicações
Gerenciamento de Containers	Redhat Openshift VMware PKS	Gerenciamento de containers de aplicações
Servidores Mensageria	Microsoft Teams	Serviço em Nuvem
Servidores Correio Eletrônico	Microsoft Windows Exchange Server 2013	Serviço de correio eletrônico Exchange
***Softwares* / Ferramentas de Gerência / Monitoração**	Zabbix 4.0.10	Software de Monitoramento do Ambiente
Gerenciador de Banco de Dados e ferramenta ETL	Postgres 8.3, 9.1.3, 9.4, 9.5 e 10	Sistema gerenciador de banco de dados Postgres
	MySql 5.0.26, 5.5.47	Sistema gerenciador de banco de dados MySql
	MariaDB 10.0.30	Sistema gerenciador de banco de dados MariaDB
	SqlServer 2014, 2016 e 2017	Sistema gerenciador de banco de dados SQLServer
	Ingres II 10.1	Sistema gerenciador de banco de dados Ingres
	BRS 8.0	Sistema gerenciador de banco de dados textual BRS
	Oracle 11g v11.2.0.4	Sistema gerenciador de banco de dados Oracle
	Oracle 12c v12.2.0.1.0	Sistema gerenciador de banco de dados Oracle

Software	Nome / Versão	Descrição
	Pentaho Data Integration 8.0	Ferramenta ETL
	Power BI	Microsoft Power BI
	ODI 10 / Sunopsis	Ferramentas ETL Oracle Data Integrator e Sunopsis
Servidores Web	Mailman 2.1.15	Servidor de Listas de Discussão
	IMAP 4.1.3	Servidor de POP IMAP Courier
	PostFix 2.9.4 e 3.3.1-5	Servidor de SMTP
	Open LDAP	Servidor de Diretórios
Solução de Auditoria de AD/File Server/E-mail	Varonis Data Manager	Varonis Data Manager
Ferramenta de Gerência	Suse Manager 4	Suse Manager

ANEXO III - CRONOGRAMA DE IMPLANTAÇÃO

Prazo Máximo (em dias)	Cronograma de Atividades da Prestação dos Serviços	Responsável
D	Emissão da Ordem de Serviço (D)	CONTRATANTE
D + 3*	Reunião de planejamento	CONTRATANTE e CONTRATADA
D + 10	Entrega do Plano de Implantação	CONTRATADA
D + 45	Entrega dos *softwares* e equipamentos da solução (E)	CONTRATADA
E + 5*	Emissão do **Termo de Recebimento Provisório (TRP1)** da etapa de entrega dos *softwares* e equipamentos da solução.	CONTRATANTE
TRP1 + 15	Instalação e configuração dos *softwares* e equipamentos da solução e entrega das licenças de uso (**I**)	CONTRATADA
I + 5*	Emissão o **Termo de Recebimento Provisório (TRP2)** da etapa de instalação e configuração dos *softwares* e equipamentos da solução e entrega das licenças de uso	CONTRATANTE
TRP2 + 10*	Emissão o **Termo de Recebimento Definitivo (TRD)** da etapa da entrega, instalação, configuração e licenciamento da solução.	CONTRATANTE
D-TC	Emissão da Ordem de Serviço para o serviço de Transferência de Conhecimento (D-TC)	CONTRATANTE
D-TC + 15	Limite para início do serviço de Transferência de Conhecimento	CONTRATADA

(*) Dias úteis

ANEXO IV - PLANILHA DE PREÇOS

ITEM	ESPECIFICAÇÃO	QTD	PREÇO UNITÁRIO (R$)	PREÇO TOTAL (R$)
1	Solução para Gerenciamento de Acesso Privilegiado com licenciamento perpétuo de *software* e fornecimento de equipamento(s)	01		
2	Serviços de instalação e configuração	01		
3	Serviço de suporte técnico mensal	48		
4	Transferência de conhecimento	06		
VALOR TOTAL				

ANEXO V - TERMO DE VISTORIA

Declaro que eu, _____,
portador(a) do CPF(MF) nº _____, representante da empresa
_____,
estabelecida no endereço _____
como seu(sua) representante legal para os fins da presente declaração, tomei conhecimento, com o objetivo de participação no Pregão N._____, de todas as informações necessárias à execução dos serviços licitados e que vistoriei os locais de instalação dos equipamentos e componentes.

Brasília, de de .

_____

ASSINATURA DO RESPONSÁVEL TÉCNICO/ REPRESENTANTE

_____

CARIMBO E ASSINATURA DO REPRESENTANTE DO CJF

ANEXO IV - TERMO DE CONFIDENCIALIDADE E SIGILO DA CONTRATADA

1. A empresa [RAZÃO/DENOMINAÇÃO SOCIAL], pessoa jurídica com sede em [ENDEREÇO], inscrita no CNPJ/MF com o n.º [N.º DE INSCRIÇÃO NO CNPJ/MF], neste ato representada na forma de seus atos constitutivos, doravante denominada simplesmente EMPRESA RECEPTORA, por tomar conhecimento de informações sobre o ambiente computacional do Conselho da Justiça Federal – CJF, aceita as regras, condições e obrigações constantes do presente Termo.

2. O objetivo deste Termo de Confidencialidade e Sigilo é prover a necessária e adequada proteção às informações restritas de propriedade exclusiva do CJF reveladas à EMPRESA RECEPTORA em função da prestação dos serviços objeto do contrato n.º XXX/XXX.

3. A expressão "informação restrita" abrangerá toda informação escrita, oral ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: técnicas, projetos, especificações, desenhos, cópias, diagramas, fórmulas, modelos, amostras, fluxogramas, croquis, fotografias, plantas, programas de computador, discos, disquetes, pen drives, fitas, contratos, planos de negócios, processos, projetos, conceitos de produto, especificações, amostras de ideia, clientes, nomes de revendedores e/ou distribuidores, preços e custos, definições e informações mercadológicas, invenções e ideias, outras informações técnicas, financeiras ou comerciais, entre outros.

4. A EMPRESA RECEPTORA compromete-se a não reproduzir nem dar conhecimento a terceiros, sem a anuência formal e expressa do CJF, das informações restritas reveladas.

5. A EMPRESA RECEPTORA compromete-se a não utilizar, bem como a não permitir que seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos utilizem, de forma diversa da prevista no contrato de prestação de serviços ao CJF, as informações restritas reveladas.

6. A EMPRESA RECEPTORA deverá cuidar para que as informações reveladas fiquem limitadas ao conhecimento dos diretores, consultores, prestadores de serviços, empregados e/ou prepostos que estejam diretamente envolvidos nas discussões, análises, reuniões e demais atividades relativas à prestação de serviços ao CJF, devendo cientificá-los da existência deste Termo e da natureza confidencial das informações restritas reveladas.

7. A EMPRESA RECEPTORA possuirá ou firmará acordos por escrito com seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos cujos termos sejam suficientes a garantir o cumprimento de todas as disposições do presente Termo.

8. A EMPRESA RECEPTORA obriga-se a informar imediatamente ao CJF qualquer violação das regras de sigilo estabelecidas neste Termo que tenha tomado conhecimento ou ocorrido por sua ação ou omissão, independentemente da existência de dolo.

9. A quebra do sigilo das informações restritas reveladas, devidamente comprovada, sem autorização expressa do CJF, possibilitará a imediata rescisão de qualquer contrato firmado entre o CJF e a EMPRESA RECEPTORA sem qualquer ônus para o CJF. Nesse caso, a EMPRESA RECEPTORA, estará sujeita, por ação ou omissão, além das multas definidas no Termo de Referência, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo CJF, inclusive os de ordem moral, bem como as de responsabilidades civil e criminal respectivas, as quais serão apuradas em regular processo judicial ou administrativo.

10. O presente Termo tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de acesso às informações restritas do CJF.

11. E, por aceitar todas as condições e as obrigações constantes do presente Termo, a EMPRESA RECEPTORA assina o presente termo através de seus representantes legais.

Brasília, de de 2021.

_____

ASSINATURA DO REPRESENTANTE DA CONTRATADA

_____

CARIMBO E ASSINATURA DO REPRESENTANTE DO CJF