DMI - TERMO DE REFERÊNCIA - AMD 71/2023

Brasília, 02 de dezembro de 2025.

Documento elaborado de acordo com o ATO DA MESA DIRETORA Nº 71, DE 2023 que regulamenta as Contratações de Solução de Tecnologia da Informação no âmbito da Câmara Legislativa do Distrito Federal, o art. 44, §2º da Lei de Licitações e Contratos Administrativos (Lei federal nº 14.133, de 1º de abril de 2021), para definir o processo de gestão estratégica das contratações de soluções baseadas em software de uso disseminado, e dá outras providências.

1. OBJETO DA CONTRATAÇÃO (ART. 14)

Aquisição de solução de gerenciamento de contas e de acessos privilegiados (licença temporária), incluindo os serviços de instalação e configuração, operação assistida, capacitação, bem como garantia e suporte técnico por 36 (trinta e seis) meses.

LOTE ÚNICO			
ITEM	**ESPECIFICAÇÃO**	**MÉTRICA OU UNIDADE DE MEDIDA**	**QUANTIDADE**
1	Solução de gerenciamento de contas e de acessos privilegiados (PAM)	Licença Temporária	1
2	Serviço de instalação e configuração	Atividade	1
3	Serviço de operação assistida	Atividade	1
4	Serviço de capacitação	Atividade	1

1.1. Os bens e serviços objeto desta contratação são caracterizados como **comuns**, nos termos do art. 6º, inciso XXVII, da Lei nº 14.133/2021, por poderem ser adquiridos de forma padronizada, amplamente disponíveis no mercado, e comparáveis em termos de qualidade, características e preço, **sem necessidade de customizações específicas**.

1.2. O contrato terá vigência de **36 (trinta e seis) meses**, contados a partir da sua assinatura e com eficácia a partir da publicação no Portal Nacional de Contratações Públicas – PNCP, conforme o disposto no art. 105 da Lei nº 14.133, de 2021.

2. DESCRIÇÃO DA SOLUÇÃO DE TI (ART. 15)

2.1. A presente contratação tem por objeto a **aquisição de uma solução de gerenciamento de contas e acessos privilegiados (Privileged Access Management – PAM) com suporte técnico e garantia funcional por 36 meses a partir da assinatura do contrato**, abrangendo os seguintes serviços complementares:

2.1.1. **Instalação e configuração** da solução no ambiente da CONTRATANTE;

2.1.2. **Operação assistida**, com apoio técnico inicial para adaptação ao uso da ferramenta;

2.1.3. **Capacitação técnica**, com treinamento direcionado aos usuários e administradores do sistema;

2.2. A solução deve atender integralmente às necessidades de segurança da informação, controle de acessos privilegiados, rastreabilidade de sessões e integração com os sistemas e servidores atualmente utilizados pela CONTRATANTE.

2.3. QUANTITATIVO DE BENS E SERVIÇOS

LOTE ÚNICO			
ITEM	**ESPECIFICAÇÃO**	**MÉTRICA OU UNIDADE DE MEDIDA**	**QUANTIDADE**
1	Solução de gerenciamento de contas e de acessos privilegiados (PAM)	Licença	1
2	Serviço de instalação e configuração	Atividade	1
3	Serviço de operação assistida	Atividade	1
4	Serviço de capacitação	Atividade	1

3. JUSTIFICATIVA PARA CONTRATAÇÃO (ART. 16)

3.1. ALINHAMENTO ESTRATÉGICO (Art. 16, inc. I)

3.1.1. A segurança da informação compreende um conjunto de ações e estratégias para proteger sistemas, programas, equipamentos e redes de invasões. Seu objetivo central é proteger dados valiosos de possíveis violações ou ataques. Os pilares da segurança da informação incluem confidencialidade, integridade e disponibilidade. Além disso, suas funções envolvem prevenção, detecção e resposta a incidentes.

3.1.2. A segurança da informação é crucial para proteger informações sensíveis e evitar danos à organização e à imagem institucional. Houve um aumento contínuo de incidentes de segurança na infraestrutura da CLDF, especialmente após a pandemia e a adoção do trabalho remoto. O crescente aumento de incidentes se deve à complexidade do ambiente corporativo e ao uso crescente de técnicas de invasão. Contudo, a própria evolução dos sistemas de segurança, contra essas invasões, tendem a conter os incidentes de segurança. Em relação aos incidentes de segurança, destacam-se os acessos privilegiados não autorizados.

3.1.3. O Gerenciamento de Acesso Privilegiado (*Privileged Access Management* - PAM) é uma solução de segurança que protege identidades com acesso especial, além dos usuários normais. Ele controla e protege o uso de credenciais de alto privilégio, garantindo armazenamento seguro, segregação de acessos e rastreabilidade.

3.1.4. O PAM é essencial para prevenir o roubo de credenciais e garantir a conformidade. O princípio do menor privilégio é uma estratégia de segurança que se baseia na ideia de conceder autorizações apenas quando realmente necessárias. Essas soluções restringem os direitos de acesso

e permissões aos usuários, garantindo que um usuário legítimo tenha somente o acesso correto. Isso aumenta a visibilidade, o gerenciamento e o controle sobre as atividades administrativas. O gerenciamento de sessões permite que a comunicação entre usuários normais e ativos privilegiados seja intermediada por um proxy/gateway de conexão. Isso inclui a gravação de sessões e a auditoria de todas as operações realizadas com credenciais privilegiadas.

3.1.5. A contratação de uma solução de Gerenciamento de Acesso Privilegiado (PAM) com vigência de 36 meses representa uma medida estratégica alinhada às melhores práticas de segurança da informação e à continuidade operacional da Administração Pública. Em um cenário de crescente sofisticação de ameaças cibernéticas, a adoção de uma solução robusta e consolidada por um período mais longo garante:

- Estabilidade e maturidade na implementação: Soluções PAM exigem tempo para integração com os diversos sistemas da organização, treinamento de equipes e amadurecimento dos processos de controle de acesso. Um contrato de 36 meses permite consolidar essas etapas sem interrupções ou riscos de descontinuidade.
- Eficiência econômica e previsibilidade orçamentária: A contratação por prazo estendido permite negociar condições comerciais mais vantajosas, protegendo a Administração contra oscilações cambiais e inflacionárias. Isso reduz o custo total de propriedade (TCO) e evita gastos recorrentes com renovações ou novas licitações.
- Fortalecimento da postura de segurança: A permanência de uma solução PAM por três anos assegura a continuidade das políticas de segurança, auditoria e conformidade com normativas como LGPD e ISO 27001, sem a vulnerabilidade de transições tecnológicas frequentes.
- Fomento à inovação interna: Ao garantir uma base tecnológica estável, a Administração pode direcionar esforços para inovação nos processos internos, sem o ônus de reavaliar constantemente a infraestrutura de segurança.

3.1.6. Até o momento, a CLDF não possui uma solução dedicada para essa funcionalidade, provendo acessos privilegiados por meio de contas e permissões basicamente baseadas em grupos específicos no serviço de diretório ou em acesso local. Esse controle possui uma estratégia fraca, pois se baseia em uma autenticação semelhante à de um usuário padrão, de forma descentralizada e com baixa rastreabilidade, razão pela qual é necessário fazer a evolução para uma solução de gerenciamento de acesso privilegiado (PAM).

3.1.7. A contratação da solução de gerenciamento de contas e acessos privilegiados (PAM) está alinhada às estratégias institucionais da CONTRATANTE relacionadas à **governança de TI, segurança da informação e conformidade com normas de controle interno e auditoria**, além de atender às diretrizes da **Política de Segurança da Informação e Comunicação (POSIC)** da Casa.

3.1.8. Além disso, contribui diretamente para os objetivos estratégicos de **garantia da integridade, rastreabilidade e controle dos acessos administrativos**, conforme identificado no Estudo Técnico Preliminar - ETP (2356310), mitigando riscos operacionais e de segurança.

3.1.9. O objeto desta contratação está em consonância com o Plano Diretor de Tecnologia da Informação – PDTI 2024/2025 da CLDF, conforme abaixo:

MACRO OBJ-5 - Prover sustentação computacional				
OBJ-5.1 - Garantir sustentação e funcionamento do complexo computacional				
Necessidade	**Declarante**	**Função institucional (tipo de aplicação) (esforço estimado)**	**Relevância**	**Prioridade**

5.1.23 - Planejar, implantar, configurar, gerenciar e monitorar os serviços de infraestrutura de tecnologia da informação na administração dos sistemas gerenciadores de bancos de dados, do serviço de correio eletrônico, dos servidores de aplicação, do serviço de arquivos distribuídos, da conectividade e comunicação de dados, do serviço de cópias de segurança e recuperação de dados, do serviço de diretório e gerenciamento das diretivas de grupo inerentes à infraestrutura, do serviço de segurança e proteção de dados dos servidores de rede e estações de trabalho e do serviço de infraestrutura do ambiente de serviços de integração contínua e entrega contínua dos sistemas de software.	Diretoria de Modernização e Inovação - DMI	Representação Legiferação Fiscalização Administração (operação chave) (+++) ca,tg Visão: A a H	70	1

3.1.10. O objeto desta contratação está em consonância com o Plano Setorial 2025 da CLDF, conforme abaixo:

Nº Meta	META	Nº Ação	AÇÃO	Valor

30	Sustentação, manutenção e proteção da rede institucional de dados realizadas.	2	Adquirir solução de segurança para controle de credenciais privilegiadas locais e remotas. [SEINF]	R$ 2.500.000,00

3.2. RELAÇÃO ENTRE A NECESSIDADE DA CONTRATAÇÃO E O QUANTITATIVO A SER CONTRATADO (Art. 16, inc. II)

3.2.1. A contratação contempla **uma única solução de software**, com **licenciamento** e **serviços complementares** dimensionados conforme a infraestrutura e o corpo técnico da CONTRATANTE. O quantitativo definido neste Termo de Referência (TR) atende integralmente à demanda atual, sem excedentes, visto que a solução será centralizada e integrada aos sistemas e servidores existentes.

3.3. MEMÓRIA DE CÁLCULO DA DEFINIÇÃO DO QUANTITATIVO (Art. 16, inc. III)

3.3.1. A definição do quantitativo baseou-se nos seguintes critérios descritos no ETP (2356310):

3.3.1.1. **Inventário de servidores e sistemas** que demandam controle de acessos privilegiados;

3.3.1.2. Levantamento do número de usuários com contas administrativas e perfis sensíveis;

3.3.1.3. Capacidade de atendimento da solução por meio de uma única licença corporativa com recursos de expansão via módulos;

3.3.1.4. Serviços de instalação, operação assistida e capacitação dimensionados como **atividades únicas**, uma vez que a implementação ocorrerá em projeto piloto único e padronizado.

3.4. RESULTADO E BENEFÍCIOS A SEREM ALCANÇADOS (Art. 16, inc. IV)

3.4.1. A contratação visa alcançar os seguintes resultados:

3.4.1.1. Manter as atuais regras e políticas de segurança da rede CLDF, preservando as configurações existentes, sem grandes alterações, com o aproveitamento de recursos já existentes.

3.4.1.2. Gerenciamento, administração e monitoramento dos acessos aos ativos de TI da CLDF, com ferramentas que possa ser utilizadas pela equipe da SEINF, preservando o conhecimento existente com redução de treinamentos e esforço/mão de obra por parte dos operadores/administradores.

3.4.1.3. Manutenção da segurança e da disponibilidade dos acesso administrativos de TI da CLDF através de ajustes automáticos, para no caso de falhas físicas não haja parada nos acessos.

3.4.1.4. Facilidade de evolução. Melhor desempenho. Maior segurança e contingência para a infraestrutura de TI e consequentemente os serviços e aplicações disponibilizados por essa infraestrutura.

3.5. MOTIVAÇÃO PARA PERMITIR ADESÃO DE NÃO PARTICIPANTES (Art. 16, inc. V)

3.5.1. A presente contratação **não prevê adesão de órgãos não participantes**. A solução será

dimensionada exclusivamente para atender às demandas da CONTRATANTE, considerando características específicas de sua infraestrutura, ambiente tecnológico e política interna de segurança da informação.

3.5.2. JUSTIFICATIVA PARA CONTRATAÇÃO POR 36 MESES

3.5.2.1. A contratação da solução de gerenciamento de contas e acessos privilegiados por um período de **36 (trinta e seis) meses** justifica-se por fatores **econômicos, administrativos e operacionais**, que garantem maior previsibilidade orçamentária, mitigação de riscos cambiais e eficiência na gestão pública, conforme explicitado no ETP(2356310).

1. Sensibilidade ao câmbio e proteção contra flutuações internacionais

Soluções dessa natureza são, em geral, desenvolvidas e comercializadas por **empresas internacionais** ou seus representantes no Brasil. Os valores praticados, portanto, estão sujeitos à **variação cambial**, sobretudo do **dólar norte-americano**, impactando diretamente o custo das licenças e serviços vinculados.

Segundo o Banco Central do Brasil:

- Em **fevereiro de 2020**, a cotação média do dólar comercial foi de **R$ 4,31**;
- Em **fevereiro de 2025**, a cotação média subiu para **R$ 4,96**, representando um aumento de aproximadamente **15,1%** no período.

Ao optar por um contrato com vigência de 36 meses, a Administração protege-se contra **novas elevações cambiais**, assegurando **previsibilidade de custos e economia a longo prazo**.

2. Impacto da inflação (IPCA e IGP-M)

Além da variação cambial, os índices de inflação no período recente demonstram forte tendência de aumento de preços:

- O **IGP-M acumulado** de fevereiro de 2020 a janeiro de 2025 foi de **56,08%** (Fonte: FGV);
- O **IPCA acumulado** no mesmo período foi de **30,52%** (Fonte: IBGE/Bacen).

Diante desse cenário, a contratação por 36 meses **trava os preços** contratados por período superior, mitigando o impacto inflacionário e assegurando **vantajosidade econômica para a Administração**.

3. Facilidade de gestão e planejamento orçamentário

Renovações anuais demandariam a repetição de processos licitatórios ou adesões, gerando **ônus administrativos, retrabalho** e riscos de **descontinuidade operacional**. Com vigência de 36 meses:

- Reduz-se a frequência de tramitação de novos processos;
- Ganha-se em **eficiência administrativa** e **alocação mais eficiente dos recursos públicos**.

4. Continuidade operacional e redução de riscos

A solução a ser contratada é **estratégica para a segurança da informação** e continuidade das operações críticas da Casa. Uma vigência maior garante:

- **Disponibilidade contínua** dos recursos contratados;
- **Evita interrupções** em serviços sensíveis por falhas na renovação contratual;
- Proporciona estabilidade ao ambiente tecnológico e ao planejamento estratégico da CLDF.

5. Conclusão

Diante da **volatilidade econômica**, da **tendência inflacionária** e da **necessidade de continuidade operacional**, a contratação da solução por 36 meses representa a escolha mais **vantajosa, segura e eficiente para a Administração**, em conformidade com os princípios da economicidade, eficiência e interesse público previstos na Lei nº 14.133/2021.

4. ESPECIFICAÇÃO DOS REQUISITOS (ART. 17)

4.1. REQUISITOS DE NEGÓCIO (Art. 17, inc. I, a))

4.1.1. A solução deve permitir o **gerenciamento centralizado de contas privilegiadas**, com controle de acesso, autenticação segura e trilha de auditoria.

4.1.2. Deve possibilitar a **segregação de funções** e aplicação de perfis distintos por usuário, conforme papéis definidos pela CONTRATANTE.

4.1.3. Deve atender às **necessidades atuais da infraestrutura tecnológica**, integrando-se com os sistemas operacionais Windows e Linux da Casa.

4.1.4. A solução deve ser capaz de **registrar e auditar todas as sessões privilegiadas**, garantindo rastreabilidade e responsabilização.

4.2. REQUISITOS DE CAPACITAÇÃO (Art. 17, inc. I, b))

4.2.1. A CONTRATADA deverá ministrar **treinamento técnico e operacional**, com carga horária mínima de 8 horas, para os perfis de usuário administrador e usuário auditor.

4.2.2. O conteúdo deve abranger instalação, operação, relatórios, boas práticas de uso e análise de incidentes.

4.2.3. A capacitação deve ser acompanhada de **material didático em português** e incluir certificado de participação.

4.3. REQUISITOS LEGAIS (Art. 17, inc. I, c))

Ver Anexo I (item 7).

4.4. REQUISITOS DE MANUTENÇÃO (Art. 17, inc. I, d))

Ver Anexo I (item 4).

4.5. REQUISITOS TEMPORAIS (Art. 17, inc. I, e))

4.5.1. A implantação completa da solução deverá ocorrer no prazo máximo de **60 (sessenta) dias corridos** após a emissão da Ordem de Serviço.

4.5.2. O contrato terá vigência de **36 (trinta e seis) meses**, exclusivamente para serviços de suporte e manutenção.

4.6. REQUISITOS DE SEGURANÇA E PRIVACIDADE (Art. 17, inc. I, f))

Ver Anexo I (item 6).

4.7. REQUISITOS SOCIAIS, AMBIENTAIS E CULTURAIS (Art. 17, inc. I, g))

4.7.1. A solução deve ser **eletrônica, virtualizada e sem impacto ambiental direto**.

4.7.2. Não se aplicam requisitos sociais ou culturais específicos nesta contratação, por se tratar de software.

4.8. REQUISITOS DE ARQUITETURA TECNOLÓGICA (Art. 17, inc. II, a))

Ver Anexo I (item 1).

4.9. REQUISITOS DE PROJETO (Art. 17, inc. II, b))

4.9.1. Ver Anexo I (item 2).

4.10. REQUISITOS DE IMPLANTAÇÃO (Art. 17, inc. II, c))

Ver Anexo I (item 3).

4.11. REQUISITOS DE GARANTIA E MANUTENÇÃO (Art. 17, inc. II, d))

Ver Anexo I (item 4).

4.12. REQUISITOS DE CAPACITAÇÃO (Art. 17, inc. II, e))

Idem ao item 4.2.

4.13. REQUISITOS DE EXPERIÊNCIA PROFISSIONAL (Art. 17, inc. II, f))

4.13.1. A equipe técnica da CONTRATADA deverá comprovar **experiência prévia em implantação de soluções PAM** em órgãos públicos ou instituições de porte similar.

4.14. REQUISITOS DE FORMAÇÃO DA EQUIPE (Art. 17, inc. II, g))

Não se aplica.

4.15. REQUISITOS DE METODOLOGIA DE TRABALHO (Art. 17, inc. II, h))

4.15.1. A CONTRATADA deverá adotar **metodologia de projeto com entregas controladas por cronograma**, e acompanhamento por relatórios técnicos validados pela CONTRATANTE.

4.16. REQUISITOS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE (Art. 17, inc. II, i))

4.16.1. A solução e os serviços prestados deverão observar a **POSIC da Casa**, as diretrizes da **LGPD** e as normas do **GSI/PR** quanto à proteção de informações classificadas e sensíveis.

4.17. OUTROS REQUISITOS (Art. 17, inc. II, j))

4.17.1. A solução deverá ter suporte técnico em **português**, com atendimento realizado por equipe situada no Brasil ou com acesso remoto em horário comercial.

5. RESPONSABILIDADES (ART. 18)

5.1. OBRIGAÇÕES DA CONTRATANTE (Art. 18, inc. I)

5.1.1. A CONTRATANTE se obriga a:

5.1.1.1. Indicar formalmente um fiscal técnico do contrato e, quando necessário, um substituto;

5.1.1.2. Disponibilizar à CONTRATADA as informações e os acessos necessários à execução dos serviços, inclusive aos ambientes tecnológicos sob sua responsabilidade;

5.1.1.3. Avaliar e aprovar o plano de instalação e configuração da solução antes do início da implantação;

5.1.1.4. Acompanhar e validar os serviços executados pela CONTRATADA, incluindo instalação, testes, capacitação e operação assistida;

5.1.1.5. Homologar a solução após os testes de funcionamento e a entrega da documentação exigida;

5.1.1.6. Prestar os esclarecimentos e suporte necessário para a execução das atividades,

quando solicitado pela CONTRATADA;

5.1.1.7. Notificar formalmente a CONTRATADA sobre qualquer descumprimento contratual ou necessidade de correção de não conformidades.

5.1.2. Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato, quando aplicável, para acompanhar e fiscalizar a execução dos contratos;

5.1.3. Encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens ou equivalentes, de acordo com os critérios estabelecidos no Termo de Referência;

5.1.4. Receber o objeto fornecido pela CONTRATADA que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

5.1.5. Aplicar à CONTRATADA as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao Órgão Gerenciador da Ata de Registro de Preços, quando aplicável;

5.1.6. Liquidar o empenho e efetuar o pagamento à CONTRATADA, dentro dos prazos preestabelecidos em contrato;

5.1.7. Comunicar à CONTRATADA todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TI;

5.1.8. Definir produtividade ou capacidade mínima de fornecimento da solução de TI por parte da CONTRATADA, com base em pesquisas de mercado, quando aplicável;

5.1.9. Prever que os direitos de propriedade intelectual e direitos autorais da solução de TI sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à CLDF, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer.

5.2. OBRIGAÇÕES DA CONTRATADA (Art. 18, inc. II)

5.2.1. A CONTRATADA se obriga a:

5.2.1.1. Fornecer a solução de gerenciamento de contas e acessos privilegiados, em conformidade com as especificações técnicas do TR;

5.2.1.2. Realizar a **instalação, configuração, ativação, testes e validação funcional** da solução em ambiente indicado pela CONTRATANTE;

5.2.1.3. Apresentar à CONTRATANTE, previamente à instalação, o **plano de implantação**, contendo as etapas, prazos e métodos a serem adotados;

5.2.1.4. Ministrar **capacitação técnica** aos perfis definidos pela CONTRATANTE, com entrega de material didático e emissão de certificado;

5.2.1.5. Prestar **serviços de operação assistida** por período mínimo acordado, acompanhando o uso inicial da solução;

5.2.1.6. Disponibilizar **atendimento técnico de suporte** durante o prazo de 36 (trinta e seis) meses, conforme níveis de serviço (SLA) estabelecidos;

5.2.1.7. Entregar toda a **documentação exigida**, incluindo manuais, certificados de licença, plano de instalação, e relatório de testes de funcionamento;

5.2.1.8. Garantir a confidencialidade das informações acessadas em razão do contrato, em conformidade com a LGPD e a POSIC da Casa;

5.2.1.9. Refazer, sem ônus adicional, quaisquer serviços que forem recusados pela CONTRATANTE por não atenderem aos critérios de aceitação definidos no TR.

5.2.2. Indicar formalmente Preposto apto a representá-la junto à CONTRATANTE, que deverá

responder pela fiel execução do contrato;

5.2.3. Entregar o objeto e executar os serviços descritos no contrato nos prazos máximos nele determinados;

5.2.4. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual, sem qualquer ônus para a CONTRATANTE;

5.2.5. Reparar quaisquer danos diretamente causados à CONTRATANTE ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela CONTRATANTE;

5.2.6. Propiciar todos os meios necessários à fiscalização do contrato pela CONTRATANTE, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;

5.2.7. Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

5.2.8. Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TI;

5.2.9. Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TI durante a execução do contrato;

5.2.10. Ceder os direitos de propriedade intelectual e direitos autorais da solução de TI sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à CLDF;

5.2.11. Fazer a transição contratual, com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações;

5.2.12. Cumprir todos os requisitos descritos no contrato, responsabilizando-se pelas despesas de deslocamento de técnicos, diárias, hospedagem e demais gastos relacionados com a equipe técnica, sem qualquer custo adicional para a CONTRATANTE;

5.2.13. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, as partes do objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes dos materiais empregados ou da execução dos serviços;

5.2.14. Responder pelas despesas relativas a encargos trabalhistas, seguro de acidentes, impostos, contribuições previdenciárias e quaisquer outras que forem devidas e referentes aos serviços executados por seus empregados, uma vez inexistir, no caso, vínculo empregatício deles com a CONTRATANTE;

5.2.15. Fornecer todas as informações solicitadas pela CONTRATANTE, relativas ao cumprimento do objeto.

5.3. Aceitar acréscimos e supressões de até 25% (vinte e cinco por cento) do valor contratado, mantidas as mesmas condições contratuais estipuladas, sem que lhe caiba qualquer reclamação, com amparo no art. 125 da Lei nº 14.133, de 2021.

5.3.1. Toda e qualquer alteração, no que couber, deverá ser processada mediante a celebração de Termo Aditivo, com amparo no art. 124 da Lei nº 14.133, de 2021, vedada a modificação do objeto.

5.4. OBRIGAÇÕES DO ÓRGÃO GERENCIADOR (Art. 18, inc. III)

Não se aplica.

6. MODELO DE EXECUÇÃO (ART. 19)

6.1. ROTINAS DE EXECUÇÃO DO CONTRATO (Art. 19, inc. I)

6.1.1. Prazos, horários e local (Art. 19, inc. I, a))

6.1.2. O prazo para entrega e instalação da solução será de **60 (sessenta) dias corridos**, contados a partir da emissão da **Ordem de Serviço** pela CONTRATANTE.

6.1.3. Os serviços deverão ser prestados **preferencialmente em horário comercial** (das 08h às 18h), salvo acordo prévio entre as partes.

6.1.4. A entrega, instalação e demais atividades ocorrerão **em ambiente da própria CONTRATANTE**, podendo envolver acesso remoto ou presencial, conforme necessidade técnica e autorização da equipe de fiscalização.

6.1.4.1. A Câmara Legislativa do Distrito Federal encontra-se no endereço Praça Municipal, Quadra 2, Lote 5, Zona Cívico-Administrativa, Brasília – DF, CEP: 70.094-902.

6.1.5. Na contagem dos prazos previstos neste documento, 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 na Câmara Legislativa do Distrito Federal.

6.1.6. Documentação mínima (Art. 19, inc. I, b))

6.1.6.1. A CONTRATADA deverá entregar, no ato da entrega das licenças, a seguinte documentação:

6.1.6.1.1. Notas fiscais relativas à aquisição da solução, emitidas em conformidade com a legislação vigente;

6.1.6.1.2. Manuais técnicos e operacionais das licenças fornecidas, preferencialmente em formato digital e em português ou inglês;

6.1.6.1.3. Certificados de licenciamento e propriedade, emitidos pelo fabricante ou representante oficial, vinculando as licenças à CONTRATANTE;

6.1.6.1.4. Plano de instalação e configuração da solução, contendo escopo, cronograma, recursos envolvidos e requisitos técnicos mínimos. Este plano deverá ser aprovado previamente pela CONTRATANTE antes do início da instalação.

6.1.6.1.5. Comprovação de que os produtos ofertados estão em fase de comercialização ativa, não sendo aceitos produtos classificados como "end-of-life" ou "end-of-support".

6.1.6.2. A simples declaração do licitante **não será aceita** como comprovação dos documentos descritos no item 8.2.1. Todos os documentos devem ser apresentados de forma objetiva, verificável e rastreável.

6.1.6.3. Os documentos técnicos relativos à solução ofertada, tais como manuais, fichas técnicas, guias de implantação e descrições de funcionalidades, **devem estar disponíveis em domínio público**, sendo acessíveis em sites oficiais do fabricante. A CONTRATADA deverá apresentar os **links diretos (URL)** para acesso a tais informações.

6.1.6.4. Também deverão ser apresentados os seguintes documentos complementares:

6.1.6.4.1. Declaração de garantia e suporte técnico emitida pelo fabricante ou distribuidor oficial,

cobrindo todo o período de 36 (trinta e seis) meses de vigência contratual;

6.1.6.4.2. Declaração de aderência aos requisitos técnicos do ANEXO I, assinada por profissional da CONTRATADA habilitado tecnicamente;

6.1.6.4.3. Comprovação de que o fabricante da solução possui representação ou canal oficial de atendimento no Brasil, para suporte e eventual atualização da solução;

6.1.6.4.4. Termo de ciência e compromisso de sigilo, conforme modelos dos Anexos II e III deste Termo de Referência.

6.1.6.5. A não apresentação de qualquer dos documentos listados poderá implicar na rejeição do objeto e/ou aplicação das penalidades previstas contratualmente.

6.1.7. Papéis e responsabilidades (Art. 19, inc. I, c))

6.1.7.1. A **CONTRATANTE** será responsável pela supervisão, aprovação de planos, homologação da solução e acompanhamento da execução dos serviços;

6.1.7.2. A **CONTRATADA** será responsável pela entrega da solução, implantação técnica, execução dos serviços de capacitação e operação assistida, e prestação de suporte técnico durante os 36 (trinta e seis) meses de vigência contratual;

6.1.7.3. A **fiscalização técnica** designada pela CONTRATANTE atuará como interlocutor oficial, avaliando o cumprimento das metas e orientando ajustes quando necessário.

6.2. ESTIMATIVA DO VOLUME DE BENS OU SERVIÇOS (Art. 19, inc. II)

6.2.1. A contratação contempla **um único conjunto de bens e serviços**, conforme especificado na seção 1 deste Termo de Referência:

LOTE ÚNICO			
ITEM	**ESPECIFICAÇÃO**	**MÉTRICA OU UNIDADE DE MEDIDA**	**QUANTIDADE**
1	Solução de gerenciamento de contas e de acessos privilegiados (PAM)	Licença	1
2	Serviço de instalação e configuração	Atividade	1
3	Serviço de operação assistida	Atividade	1
4	Serviço de capacitação	Atividade	1

6.2.2. A contratação será realizada em **lote único e indivisível**, dada a natureza integrada da solução.

6.3. MECANISMOS FORMAIS DE COMUNICAÇÃO (Art. 19, inc. III)

6.3.1. Serão considerados mecanismos formais de comunicação entre a CONTRATANTE e a CONTRATADA:

6.3.1.1. Ordem de Fornecimento de Bens;

6.3.1.2. Ordem de Serviço;

6.3.1.3. Ata de Reunião;

6.3.1.4. Ofício;

6.3.1.5. Sistema de abertura de chamados;

6.3.1.6. E-mails;

6.3.1.7. Aplicativos de mensagens (ex.: WhatsApp e/ou Telegram), desde que previamente autorizados pela CONTRATANTE e com os devidos registros documentais.

6.4. FORMA DE PAGAMENTO (Art. 19, inc. IV)

6.4.1. O pagamento será efetuado **após o recebimento definitivo do objeto contratado**, condicionado à verificação da conformidade da entrega com os critérios técnicos estabelecidos, e à apresentação da **documentação mínima exigida**, conforme descrito neste Termo de Referência.

6.4.2. O pagamento será realizado mediante apresentação de **nota fiscal válida** e aprovação pela fiscalização do contrato, obedecendo aos prazos legais e à legislação vigente.

6.4.3. Os pagamentos serão efetuados pela CLDF, em moeda corrente nacional, mediante Ordem Bancária, em até 10 (dez) dias úteis, contados do recebimento definitivo do objeto, sendo efetuada a retenção na fonte dos tributos e contribuições elencados na legislação aplicável.

6.4.3.1. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

6.4.4. O setor competente para proceder o pagamento deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

6.4.4.1. o prazo de validade;

6.4.4.2. a data da emissão;

6.4.4.3. os dados do contrato e do órgão CLDF;

6.4.4.4. o período de prestação dos serviços;

6.4.4.5. o valor a pagar; e

6.4.4.6. eventual destaque do valor de retenções tributárias cabíveis.

6.4.5. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada das seguintes comprovações:

6.4.5.1. da regularidade fiscal, constatada através de consulta "on-line" ao Sistema de Cadastramento Unificado de Fornecedores – SICAF, ou na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021;

6.4.5.2. da regularidade trabalhista, constatada através da emissão da Certidão Negativa de Débitos Trabalhistas (CNDT); e

6.4.5.3. do cumprimento das obrigações trabalhistas e contribuições sociais, correspondentes à nota fiscal ou fatura a ser paga pela Câmara Legislativa do Distrito Federal – CLDF, se for o caso.

6.4.6. Nos casos de eventuais atrasos de pagamento por culpa comprovada da

CONTRATANTE, o valor devido deverá ser acrescido de encargos moratórios, apurados desde a data final do período de adimplemento até a data do efetivo pagamento.

6.4.7. A parcela devida será atualizada monetariamente, desde o vencimento da obrigação até a data do efetivo pagamento de acordo com a variação "pro rata tempore" do IPCA.

6.4.8. Nenhum pagamento será efetuado a contratada enquanto pendente de liquidação ou quando existir qualquer obrigação que lhe for imposta, em virtude de penalidade ou inadimplência, sem que isso gere direito ao pleito de reajustamento de preços ou correção monetária.

6.4.9. A critério da CLDF, poderá ser utilizado o valor contratualmente devido para cobrir dívidas de responsabilidade da Contratada relativas a multas que lhe tenham sido aplicadas em decorrência de irregular execução contratual.

7. MODELO DE GESTÃO (ART. 20)

7.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial;

7.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila;

7.3. As comunicações entre a CLDF e a CONTRATADA devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim;

7.4. A CLDF poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato;

7.5. Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, será realizada a Reunião Inicial de alinhamento com o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução do contrato;

7.6. A reunião ocorrerá em até 10 dias úteis da assinatura do Contrato, podendo ser prorrogada a critério da CONTRATANTE.

7.7. A pauta desta reunião observará, pelo menos:

7.7.1. Presença do representante legal da CONTRATADA, que apresentará o seu preposto;

7.7.2. Entrega, por parte da CONTRATADA, do Termo de Compromisso e dos Termos de Ciência;

7.7.3. Esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;

7.7.4. A Carta de apresentação do Preposto deverá conter no mínimo o nome completo e CPF do funcionário da empresa designado para acompanhar a execução do contrato e atuar como interlocutor principal junto à CONTRATANTE, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;

7.7.5. Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste Termo de Referência;

7.8. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos, observando-se, em especial, as rotinas a seguir:

7.8.1. O Fiscal Técnico do contrato, além de exercer as atividades elencadas no inciso II do art. 34 do AMD nº 71/2023 da CLDF, acompanhará a execução do contrato para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração.

7.8.2. O Fiscal Técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados;

7.8.3. Identificada qualquer inexatidão ou irregularidade, o Fiscal Técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção;

7.8.4. O Fiscal Técnico do contrato informará ao Gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso;

7.8.5. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o Fiscal Técnico do contrato comunicará o fato imediatamente ao Gestor do contrato;

7.8.6. O Fiscal Técnico do contrato comunicará ao Gestor do contrato, 180 dias antes do encerramento do contrato, o término do contrato sob sua responsabilidade, com vistas à prorrogação contratual;

7.8.7. O Fiscal Administrativo do contrato, além de exercer as atividades elencadas no inciso IV do art. 34 do AMD nº 71/2023 da CLDF, verificará a manutenção das condições de habilitação da CONTRATADA, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário;

7.8.8. Caso ocorram descumprimento das obrigações contratuais, o Fiscal Administrativo do contrato atuará tempestivamente na solução do problema, reportando ao Gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência;

7.8.9. O Gestor do contrato, além de exercer as atividades elencadas no inciso I do art. 34 do AMD nº 71/2023 da CLDF, coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração;

7.8.10. O Gestor do contrato acompanhará a manutenção das condições de habilitação da CONTRATADA, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais;

7.8.11. O Gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência;

7.8.12. O Gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais Técnico, Administrativo e Requisitante quanto ao cumprimento de obrigações assumidas pela CONTRATADA, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas;

7.8.13. O Gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso;

7.8.14. O Gestor do contrato, com auxílio dos fiscais, elaborará relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a

serem adotadas para o aprimoramento das atividades da Administração.

7.9. CRITÉRIOS DE ACEITAÇÃO (Art. 20, inc. I)

7.9.1. A aceitação da solução será condicionada à verificação técnica e documental dos itens fornecidos, com base nos seguintes critérios:

7.9.1.1. A licença da solução de gerenciamento de contas e acessos privilegiados deverá:

7.9.1.1.1. Ser nova, original, de primeiro uso, não recondicionada e devidamente registrada para uso exclusivo da CONTRATANTE;

7.9.1.1.2. Estar em fase de comercialização ativa pelo fabricante, não sendo aceitos produtos classificados como "end-of-life" ou "end-of-support";

7.9.1.1.3. Ser entregue em sua versão mais recente estável, compatível com os sistemas operacionais utilizados pela CONTRATANTE;

7.9.1.1.4. Estar acompanhada de termo de garantia e suporte técnico com vigência de 36 (trinta e seis) meses, período durante o qual deverá contar com atualizações corretivas, evolutivas e atendimento técnico conforme os níveis de serviço pactuados;

7.9.1.1.5. Estar acompanhada de toda a documentação técnica exigida, conforme item 8.2 deste Termo de Referência.

7.9.1.2. A entrega somente será considerada aceita após:

7.9.1.2.1. A instalação, ativação e testes da solução, comprovando o pleno funcionamento de todos os seus módulos;

7.9.1.2.2. A validação, pela equipe técnica da CONTRATANTE, de que a solução atende a todos os requisitos estabelecidos no ANEXO I;

7.9.1.2.3. A entrega do plano de instalação aprovado, relatórios de testes e demais documentos exigidos;

7.9.1.2.4. A inexistência de falhas críticas ou incompatibilidades com o ambiente de produção da CONTRATANTE.

7.9.1.3. O recebimento definitivo ocorrerá apenas após a conclusão satisfatória dos procedimentos de validação técnica e documental. Caso a entrega esteja em desconformidade com as especificações contratuais, a CONTRATANTE poderá:

7.9.1.3.1. Recusar a aceitação da entrega;

7.9.1.3.2. Solicitar a correção ou reapresentação dos itens, sem qualquer custo adicional;

7.9.1.3.3. Aplicar, quando cabível, as sanções contratuais previstas.

7.10. PROCEDIMENTOS DE TESTES E INSPEÇÃO (Art. 20, inc. II)

A verificação técnica da solução será composta por inspeção, validação funcional e conferência documental, conforme segue:

7.10.1. Metodologia de avaliação da qualidade (Art. 140 da lei nº 14.133/2021; AMD 71/2023, Art. 20, inc. II, a))

Será aplicada metodologia baseada em **verificação por evidência**, com validação funcional da solução e inspeção documental. A avaliação será binária (atende/não atende), observando os critérios mínimos de qualidade, adequação técnica, segurança e conformidade contratual.

7.10.1.1. Mecanismos de inspeção (Art. 20, inc. II, a), 1))

7.10.1.1.1. Inspeção visual e funcional do sistema instalado;
7.10.1.1.2. Verificação presencial ou remota do ambiente de produção;
7.10.1.1.3. Avaliação do comportamento da solução sob simulações de uso;
7.10.1.1.4. Conferência documental em checklist padronizado.

7.10.1.2. Ferramentas (Art. 20, inc. II, a), 2))

7.10.1.2.1. Interface de administração da própria solução;
7.10.1.2.2. Logs e relatórios gerados pelo sistema;
7.10.1.2.3. Ferramentas de diagnóstico fornecidas pelo fabricante;
7.10.1.2.4. Relatórios técnicos produzidos pela CONTRATADA.

7.10.1.3. Fontes de informação (Art. 20, inc. II, a), 3))

7.10.1.3.1. Documentação técnica e manuais oficiais;
7.10.1.3.2. Certificados de licenciamento e suporte;
7.10.1.3.3. Plano de instalação e configuração aprovado;
7.10.1.3.4. Relatórios de teste de funcionamento;
7.10.1.3.5. Relatórios emitidos pela equipe de fiscalização.

7.10.1.4. Lista de verificação (Art. 20, inc. II, a), 4))

A checklist incluirá os seguintes pontos:

1. Instalação e parametrização completa da solução;
2. Entrega e ativação da licença;
3. Acesso à interface de gerenciamento;
4. Funcionamento dos mecanismos de auditoria e controle de sessões;
5. Realização da capacitação técnica conforme previsto;
6. Entrega de toda a documentação exigida;
7. Homologação pela CONTRATANTE.

7.10.1.5. Previsão de inspeções e diligências (Art. 20, inc. II, a), 5))

7.10.1.5.1. Haverá **ao menos uma inspeção técnica** no momento da implantação;

7.10.1.5.2. Poderão ser realizadas diligências técnicas adicionais caso haja dúvidas quanto ao funcionamento da solução ou divergência documental;

7.10.1.5.3. A fiscalização poderá requisitar **demonstração das funcionalidades**, bem como simulações de uso.

7.10.2. Recursos humanos necessários (Art. 20, inc. II, b))

7.10.2.1. Equipe da CONTRATANTE com perfil técnico na área de segurança da informação e infraestrutura;

7.10.2.2. No mínimo um fiscal técnico designado oficialmente;

7.10.2.3. Profissionais da CONTRATADA com experiência comprovada na solução ofertada, conforme exigências do TR.

7.10.3. Níveis Mínimos de Serviço Exigidos

7.10.3.1. Os níveis mínimos de serviço são indicadores mensuráveis estabelecidos pela CONTRATANTE para aferir objetivamente os resultados pretendidos com a contratação. São considerados para a presente contratação os seguintes indicadores:

IAC – INDICADOR DE ATRASO NA CONCLUSÃO DOS CHAMADOS DE SUPORTE		
Tópico	**Descrição**	
Finalidade	Medir o tempo de atraso na prestação de suporte e garantia	
Meta a cumprir	**IAC <= 0**	A meta definida visa garantir a prestação de suporte e garantia dentro do prazo previsto.
Instrumento de medição	Chamado de suporte, relatório do chamado	
Forma de acompanhamento	A avaliação será feita conforme SLAs e prazos de atendimento constantes deste termo de referência e seus anexos. Para conclusão do chamado, será subtraída a data e hora da conclusão do chamado pela data e hora da abertura do chamado.	
Periodicidade	Para cada chamado de suporte e garantia realizado.	

Mecanismo de Cálculo (métrica)	**IAC = TEX – TEST** Onde: **IAC** – Indicador de Atraso na prestação de suporte e garantia **TEX** – Tempo de Execução Para resolução do chamado, será subtraída a data e hora da conclusão do chamado pela data e hora da abertura do chamado. **TEST** – Tempo Estimado para a execução do chamado – constante nos SLAs e prazos de atendimento do Termo de Referência; A data e hora de abertura será aquela constante na abertura do chamado, considerando-se o horário de envio de e-mail, ligação telefônica ou outra forma de abertura de chamado. A data e hora de conclusão do chamado deverá ser aquela reconhecida pelo Fiscal Técnico, conforme critérios constantes neste Termo de Referência. Para os casos em que o Fiscal Técnico rejeite o fechamento do chamado, o prazo de execução do chamado continua a correr, findando-se apenas quando a CONTRATADA efetivamente cumpra o chamado e haja aceitação por parte do Fiscal Técnico.
Observações	Obs1: Serão utilizadas horas corridas na contagem da execução, inclusive em feriados, fins de semana, horário noturno e demais situações.
Início de vigência	No momento da abertura do chamado ou da constatação da necessidade de troca de hardware.

Faixas de ajuste no pagamento (glosa).	Para valores do indicador **IAC**: Até 0: cumprimento adequado da obrigação Acima de 1: No caso de chamados de criticidade alta, assim compreendidos aqueles que causam interrupção em serviços de produção na CLDF, aplicar-se-á glosa de 0,1% por hora de atraso sobre o valor do contrato; No caso de chamados de criticidade média, assim compreendidos aqueles que causam interrupção em serviços não críticos na CLDF, ou que reduzem os níveis de serviço de segurança ou disponibilidade, tal como a aplicação de *patches* de segurança ou quando o incidente afetar itens de configuração redundantes, deixando o serviço de contar com redundância até a resolução, aplicar-se-á glosa de 0,03% por hora de atraso sobre o valor do contrato; No caso de chamados de criticidade baixa, assim compreendidos os casos não compreendidos nos itens acima, aplicar-se-á glosa de 0,005% por hora de atraso sobre o valor do contrato;

7.11. PROCEDIMENTOS DE RETENÇÃO, GLOSA E SANÇÕES NO PAGAMENTO (Art. 20, inc. III e V)

7.11.1. Nos casos de inadimplemento contratual, as penalidades pecuniárias seguirão os critérios estabelecidos no TR:

7.11.1.1. Atraso de 1 a 30 dias: multa de 0,5% a 2,5% sobre o valor da contratação ou da parcela inadimplida;

7.11.1.2. Atraso superior a 30 dias: multa de 2,5% a 5%.

7.11.2. As penalidades possuem natureza de sanção administrativa e não se confundem com glosa técnica. A aplicação poderá ocorrer independentemente de retenção de valores.

7.12. SANÇÕES ADMINISTRATIVAS (Arts. 155 a 163 da Lei nº 14.133, de 2021; AMD 71/2023, Art. 20, inc. IV)

7.12.1. A contratada estará sujeita às sanções administrativas previstas na Lei nº 14.133/2021, e às demais cominações previstas em regulamento específico que trata dos procedimentos de aplicação de sanções, resguardado o direito à ampla defesa e ao contraditório.

7.12.2. Independente das sanções legais cabíveis, a licitante/contratada ficará sujeita ainda ao ressarcimento das perdas e danos causados à Administração ou a terceiros, decorrentes de sua culpa ou dolo no descumprimento das obrigações licitatórias e/ou contratuais.

7.12.3. Comete infração administrativa, nos termos da Lei nº 14.133/2021, o contratado que:

a) der causa à inexecução parcial do contrato;

b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

c) der causa à inexecução total do contrato;

d) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;

f) praticar ato fraudulento na execução do contrato;

g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

h) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

7.12.4. Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:

7.12.4.1. Advertência, quando o contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, Lei nº 14.133/2021);

7.12.4.2. Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas "b", "c" e "d" do subitem acima deste Termo de Referência, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, Lei nº 14.133/2021);

7.12.4.3. Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas "e", "f", "g" e "h" do subitem acima deste Termo de Referência, bem como nas alíneas "b", "c" e "d", que justifiquem a imposição de penalidade mais grave (art. 156, §5º, Lei nº 14.133/2021).

7.12.4.4. Multa, que não poderá ser inferior a 0,5% nem superior a 30% do valor do contrato licitado ou celebrado com contratação direta (art. 156, §3º, Lei nº 14.133/ 2021)

7.12.5. A aplicação das sanções previstas não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante (art. 156, §9º, Lei nº 14.133/ 2021).

7.12.6. Todas as sanções previstas poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, Lei nº 14.133/2021).

7.12.7. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157, Lei nº 14.133/2021).

7.12.8. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pela Contratante ao Contratado, além da perda desse valor, a diferença poderá ser cobrada judicialmente (art. 156, §8º, Lei nº 14.133/2021).

7.12.9. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

7.12.10. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133/2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

7.12.11. Na aplicação das sanções serão considerados (art. 156, §1º, Lei nº 14.133/2021):

7.12.11.1. a natureza e a gravidade da infração cometida;

7.12.11.2. as peculiaridades do caso concreto;

7.12.11.3. as circunstâncias agravantes ou atenuantes;

7.12.11.4. os danos que dela provierem para o Contratante;

7.12.11.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

7.12.12. Os atos previstos como infrações administrativas na Lei nº 14.133/2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846/2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159).

7.12.13. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160, Lei nº 14.133/2021).

7.12.14. A Contratante deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e no Cadastro Nacional de Empresas Punidas (CNEP), instituídos no âmbito do Poder Executivo Federal. (art. 161, Lei nº 14.133/2021).

7.12.15. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/2021.

7.12.16. Os débitos do contratado para com a Administração contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pela referida autarquia decorrentes de um futuro contrato ou de outros contratos administrativos que o contratado possua com a mesma autarquia ora contratante.

7.13. ESTRUTURA DA COMISSÃO DE FISCALIZAÇÃO (Art. 20, inc. VI)

7.13.1. Será designado pela CONTRATANTE um **fiscal técnico do contrato**, com a possibilidade de designação de **fiscal substituto** e **fiscal administrativo**, conforme o caso.

7.13.2. A comissão ou equipe de fiscalização terá competência para:

7.13.2.1. Acompanhar a execução do contrato;

7.13.2.2. Avaliar conformidade técnica da solução;

7.13.2.3. Verificar o cumprimento das obrigações contratuais;

7.13.2.4. Elaborar os relatórios de recebimento provisório e definitivo.

8. ESTIMATIVA DE PREÇOS (AMD Nº 57, DE 2023; AMD 71/2023, ART. 21)

8.1. A estimativa de preços foi elaborada com base nas orientações da **Instrução Normativa nº 73/2020**, da extinta SEGES/ME, e nos critérios atuais da **Portaria SEGES/ME nº 57/2023**, observando os seguintes parâmetros:

8.1.1. **Consulta a soluções similares** disponíveis no mercado nacional por meio de cotações diretas com fornecedores e distribuidores oficiais;

8.1.2. **Contratações similares realizadas na Administração Pública**, especialmente registros no **Painel de Compras do Governo Federal (link)**;

8.1.3. **Catálogo de Soluções de TIC com Condições Padronizadas – SGD/ME**, versão vigente;

8.1.4. Pesquisas em **sites especializados, bases de dados governamentais e portais de compras públicas**, como Compras.gov.br.

Itens cotados:

ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	QUANTIDADE	VALOR ESTIMADO UNITÁRIO (R$)	VALOR TOTAL ESTIMADO (R$)
1	Solução de gerenciamento de contas e de acessos privilegiados (PAM)	Licença	1	R$ 2.154.855,85	R$ 2.154.855,85
2	Serviço de instalação e configuração	Atividade	1	R$ 126.216,00	R$ 126.216,00
3	Serviço de operação assistida	Atividade	1	R$ 27.000,00	R$ 27.000,00
4	Serviço de capacitação	Atividade	1	R$ 128.892,00	R$ 128.892,00
VALOR TOTAL					**R$ 2.436.963,85**

9. ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO (ART. 22)

9.1. DOTAÇÃO ORÇAMENTÁRIA

9.1.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento da CLDF.

9.1.2. Programa de Trabalho: 01.126.8204.2557.2627 - GESTÃO DA INFORMAÇÃO E DOS SISTEMA DE T.I. - CLDF.

9.1.3. Elemento de Despesa: 33.90.40 - Serviços de Tecnologia da Informação e Comunicação - Pessoa Jurídica.

9.2. ESTIMATIVA DO IMPACTO FINANCEIRO (Art. 22, inc. I)

9.2.1. O valor total estimado para a contratação é de até **R$ 2.436.963,85 (dois milhões, quatrocentos e trinta e seis mil novecentos e sessenta e três reais e oitenta e cinco centavos)**, conforme detalhado no item referente à **Estimativa de Preços** deste Termo de Referência e no Mapa de Preços (2220722). A despesa será realizada com recursos próprios da CONTRATANTE, previstos na dotação orçamentária apropriada, compatível com o Plano Plurianual (PPA), a Lei de Diretrizes Orçamentárias (LDO) e a Lei Orçamentária Anual (LOA).

9.2.2. A contratação **não implica em aumento de despesa continuada**, conforme disposto no art. 17 da Lei Complementar nº 101/2000 (Lei de Responsabilidade Fiscal – LRF), tampouco

compromete a sustentabilidade financeira da Administração.

9.3. CRONOGRAMA FÍSICO-FINANCEIRO (Art. 22, inc. II)

Eventos	Prazo Estimado	Valor
Entrega e implantação da solução de gerenciamento de contas e de acessos privilegiados	Em até **60 (sessenta) dias corridos** após a emissão da Ordem de Serviço (OS)	R$ 0,00
Recebimento provisório da solução	Em até **2 (dois) dias úteis** após a entrega e apresentação da documentação fiscal	R$ 0,00
Recebimento definitivo da solução	Em até **10 (dez) dias úteis** após o recebimento provisório, prorrogável por igual período mediante justificativa	R$ 2.436.963,85

10. REGIME DE EXECUÇÃO (ART. 23)

10.1. O regime de execução do contrato será de empreitada por preço global, de acordo com o art. 6º, inciso XXIX, da Lei nº 14.133/2021.

11. CRITÉRIOS PARA SELEÇÃO DO FORNECEDOR (ART. 24)

11.1. FORMA DE SELEÇÃO E CRITÉRIO DE JULGAMENTO DA PROPOSTA

11.1.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo menor preço global, considerando o objeto como lote único.

11.1.2. As licitantes deverão apresentar suas propostas conforme modelo constante no Anexo V.

11.1.3. Para fins de aceitação pela CLDF, todas as especificações técnicas descritas deverão ser comprovadas ponto-a-ponto através de catálogos, folders, manuais dos equipamentos ou declaração fornecida pelo próprio fabricante indicando corretamente, a página, o documento e o trecho de comprovação em arquivo digital editável (por exemplo, word e excel) que demonstre o atendimento de forma clara e objetiva de cada item/subitem da especificação técnica constante neste termo de referência.

I - A falta de informações técnicas ou a incompatibilidade destas com as características especificadas neste termo, implicará a desclassificação da proposta

11.1.4. Exemplo:

ESPECIFICAÇÃO DA CONTRATANTE	COMPROVAÇÃO
1. Deve permitir instalação...	Página 13 – Manual "Fabricante"

1.1. Deve ter suporte a...	Página 2 – Proposta comercial
2. Deve ser compatível com...	Conforme Link: http://linkdofabricante.com

11.2. QUALIFICAÇÃO TÉCNICA

11.2.1. Comprovação de aptidão para o fornecimento de bens similares de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de um ou mais atestado(s) de capacidade técnica, expedido(s) por pessoa jurídica de direito público ou privado, idônea, estabelecida em território nacional, que comprove o fornecimento de serviços, bem como a prestação de garantia e suporte técnico na quantidade de 50% do solicitado e em conformidade com as especificações descritas neste documento e anexos:

11.2.1.1. Entende-se por bens similares o fornecimento de solução com escopo mínimo de 125 dispositivos ou 750 usuários nominais para cofre de senha e gerenciamento de sessão, 125 dispositivos ou 750 usuários nominais para acesso remoto seguro e 125 dispositivos para elevação de privilégios.

11.2.1.2. Prestação de **garantia e suporte técnico;**

11.2.1.3. Execução conforme **especificações compatíveis** com as previstas neste Termo de Referência e seus anexos.

11.2.2. Os atestados poderão ser apresentados em nome da **matriz ou filial** da empresa licitante, desde que emitidos por pessoas jurídicas distintas da própria licitante e que tenham relação direta com o fornecimento declarado.

11.2.3. A Administração poderá solicitar **complementos documentais** para verificação da legitimidade dos atestados apresentados, tais como:

11.2.3.1. Cópia do contrato relacionado;

11.2.3.2. Identificação da contratante (razão social, endereço e CNPJ);

11.2.3.3. Indicação do local de execução do objeto;

11.2.3.4. Declaração de que o serviço foi prestado de forma satisfatória.

12. ÍNDICE DE CORREÇÃO MONETÁRIA (ART. 25)

12.1. Dentro do prazo de vigência da contratação, os preços contratados poderão sofrer reajuste após o interregno de um ano, contado da data do orçamento estimado, aplicando-se a variação acumulada do Índice de Custos de Tecnologia da Informação - ICTI.

13. DA VISTORIA

13.1. Para conhecimento das características do objeto e a adequada elaboração de sua proposta, recomenda-se que o interessado realize vistoria nos locais de execução dos serviços, acompanhado por servidor desta Câmara Legislativa, devendo o agendamento ser efetuado previamente pelo telefone (61) 3348-8321.

13.2. A realização da vistoria não se consubstancia em condição para a participação na licitação, entretanto, será exigida no edital a DECLARAÇÃO do licitante que tem pleno conhecimento

das condições necessárias para a realização do serviço, conhecendo todas as informações e condições locais para o cumprimento das obrigações do objeto deste instrumento, não sendo admitidas, em hipótese alguma, alegações posteriores no sentido da inviabilidade de cumprir com as obrigações, face ao desconhecimento dos serviços e de dificuldades técnicas não previstas.

14. GARANTIA CONTRATUAL

14.1. Será exigida a garantia da contratação no percentual de 5% do valor contratual em até 5 (cinco) dias úteis após sua assinatura, na forma do art. 98 da Lei nº 14.133/2021.

14.2. O prazo estabelecido no subitem acima não se aplica nos casos em que a CONTRATADA optar pela modalidade seguro garantia. Nesse caso, a prestação da garantia deverá ocorrer no prazo de 1 (um) mês contado da data de homologação da licitação e anterior à assinatura do contrato, em conformidade com o estabelecido no § 3º do art. 96 da Lei 14.133/21.

15. SUBCONTRATAÇÃO

15.1. Não é admitida a subcontratação do objeto contratual, conforme justificativa constante do Estudo Técnico Preliminar (2356310).

16. ASSINATURAS

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO				
Integrante	**Nome**	**Matrícula**	**Lotação**	**Ramal**
Requisitante	**FÁBIO VIRGÍLIO DE SOUZA NEVES**	24554	SEINF	8321
Técnico	**AIMBERE GIANNACCINI**	18327	SEINF	8321
Administrativo	**CARLOS HENRIQUE DA SILVA JUNIOR**	24418	DAF	8558

ÁREA TÉCNICA DE TI			
NOME DA ÁREA TÉCNICA DE TI	**NOME DO CHEFE OU SUBSTITUTO**	**Matrícula**	**Ramal**
SEINF	**PEDRO CUNHA REGO CELESTIN**	22858	8344

17. APROVAÇÃO E DECLARAÇÃO DE CONFORMIDADE

Aprovo este Termo de Referência e atesto sua conformidade às disposições do AMD nº 71 de 2023 da CLDF, bem como à Lei 14.133/2021.

WALÉRIO OLIVEIRA CAMPORÊS

Diretor da DMI

ANEXO I – REQUISITOS DA CONTRATAÇÃO

REQUISITOS DA CONTRATAÇÃO

1. REQUISITOS DE ARQUITETURA TECNOLÓGICA

De modo resumido, a solução deverá ser composta por módulo de gerenciamento de contas e de sessões privilegiados (Privileged Account and Session Management – PASM) e módulo de gerenciamento de elevação e delegação de privilégios (Privilege Elevation and Delegation Management – PEDM)

1.1. **Módulo de gerenciamento de contas e de sessões privilegiados:**

1.1.1. Prover credenciais e acessos privilegiados para, pelo menos, 250 (duzentos e cinquenta) dispositivos e 1.000 (um mil) aplicações, para consumo de API;

1.1.2. Ser licenciado para, pelo menos, 1.500 (um mil e quinhentos) usuários privilegiados nominais;

1.1.3. Suportar a integração com os sistemas operacionais a seguir, sendo possível a utilização de APIs para a compatibilidade:

1.1.3.1. Microsoft Windows Server 2016 e superiores;

1.1.3.2. Rocky Linux 9.0 e superiores;

1.1.3.3. Ubuntu Linux 18 e superiores;

1.1.3.4. CentOS Linux 6.1 e superiores;

1.1.3.5. Ambientes de virtualização VMWare ESXi 8.0 e superiores;

1.1.3.6. Sistemas gerenciadores de banco de dados Microsoft SQL Server 2022, MySQL, PostgreSQL e MariaDB;

1.1.3.7. Ferramentas de busca e análise de dados ElasticSearch;

1.1.3.8. Equipamentos de rede e de segurança do fabricante Fortinet, 7.2 e superiores;

1.1.3.9. Controladores de storage Dell e PureStorage;

1.1.3.10. Aplicações Microsoft Windows, incluindo contas de serviço, tarefas agendadas e pools de conexão do IIS;

1.1.3.11. Aplicações Web, incluindo JBoss, Tomcat, Oracle Application Server, Apache e IIS;
1.1.3.13.

1.1.3.12. Aplicações em nuvem, incluindo Microsoft Azure, Amazon AWS, Google Cloud e Office 365.

1.1.4. Ser composto por cofre de senhas, elemento responsável pela geração, revogação, versionamento, armazenamento e controle das credenciais de acesso, e por gateway ou proxy de sessão, elemento responsável pelo provimento do acesso privilegiado, monitoramento e controle de sessão;

1.1.5. Ser provisionado para instalação em ambientes de virtualização VMWare, Microsoft Azure, Google Cloud e Amazon AWS, sendo o contratante responsável pelo provimento dos recursos de armazenamento, processamento, memória e rede na forma de IaaS no modelo BYOL (no caso de ambientes em nuvem). Nesse sentido, não será permitido o provimento de solução com uso de hardwares dedicados (appliances);

1.1.6. Operar em regime de alta disponibilidade e tolerância a falhas no ambiente virtualizado, de modo que, em caso de falha em algum servidor, o serviço continue disponível e com a mesma capacidade. Nesse contexto, deverá ser capaz de operar em modo ativo-passivo, replicando as configurações entre todos os elementos que compõe a solução, incluindo cofres de senhas e gateways/proxies de sessão e banco de dados. A arquitetura será discutida e acordada no projeto de implantação da solução, conforme exigências da Contratada;

1.1.7. Incluir o licenciamento dos sistemas operacionais próprios ou de terceiros necessários para a funcionamento da solução durante a vigência do contrato, incluindo eventuais licenças de sistemas de gerenciamento de banco de dados;

1.1.8. Ser implantado com os recursos mínimos e suficientes para o provimento do serviço, incluindo a criptografia do sistema operacional e do sistema de gerenciamento de banco de dados (hardening);

1.1.9. Incluir, caso necessário, o licenciamento necessário de Microsoft Remote Desktop Server, para acesso comum a servidores e/ou aplicativos (Remote App);

1.1.10. Realizar o gerenciamento de credenciais, em que credencial é qualquer senha, chave criptográfica ou token capaz de ser guardado de maneira segura, garantindo os seguintes aspectos:

1.1.10.1. Rotatividade de credenciais, permitindo a geração de senhas aleatórias para ativos e grupo de ativos;

1.1.10.2. Revogação de credenciais sob demanda ou por meio de política definida;

1.1.10.3. Especificação do tipo de caracteres para a composição de senhas, incluindo caracteres alfabéticos maiúsculos, minúsculos, numéricos, especiais e símbolos, por ativos ou grupo de ativos;

1.1.10.4. Definição de tempo de validade de credencias;

1.1.10.5. Criptografia de credencias com protocolos padrões da indústria, incluindo AES 256;

1.1.10.6. Capacidade de reinicialização de serviços e dependências, no caso de mudança de uma credencial de serviço;

1.1.10.7. Segmentação de senhas, por fracionamento da senha e por autorização de múltiplos aprovadores;

1.1.10.8. Injeção automática de credenciais, de modo que a autenticação se realize sem que o usuário tenha conhecimento ou precise conhecer a senha;

1.1.10.9. Exportação da chave de criptografia ou da credencial equivalente do cofre de senhas, para uso em caso de recuperação de desastres ou de migração de solução.

1.1.11. Possuir funcionalidade de discovery, capaz de buscar e registrar novos ativos alvo, garantindo as seguintes condições:

1.1.11.1. Capacidade de realizar buscas no Active Directory e em blocos de endereços IP,

podendo ser realizada por demanda, agendada e rotina periódica;

1.1.11.2. Levantamento automático de contas administrativas em cada ativo;

1.1.11.3. Levantamento automático de ativos e de suas respectivas identidades em grupos, de acordo com parâmetros previamente configurados;

1.1.11.4. Classificação automática de contas locais e de domínio;

1.1.11.5. Identificação de contas de serviços e de tarefas em ambientes Microsoft Windows;

1.1.11.6. Identificação de contas locais e que possuam chaves SSH em ambientes Unix/Linux.

1.1.12. Não conter restrição em relação ao quantitativo de contas que podem ser gerenciadas em um dispositivo licenciado;

1.1.13. Ser capaz de monitorar sessões, gravar sessões, capturar telas, coletar, armazenar e indexar logs de teclas pressionadas em teclado (keystrokes) em acessos privilegiados, garantindo os seguintes requisitos:

1.1.13.1. Alerta ao usuário privilegiado que a sessão está sendo gravada;

1.1.13.2. Monitoramento por meio de gravação de vídeos, em formato padrão de execução da solução;

1.1.13.3. Monitoramento ao vivo, permitindo ao usuário supervisor, previamente configurado, realizar ações de lock/unlock, suspender e terminar a conexão;

1.1.13.4. Pesquisa forense de eventos de segurança em todas as sessões gravadas, incluindo comandos digitados, copiar e colar arquivos e execução de softwares;

1.1.14. Integrar-se à soluções de *Security Information and Event Management* - SIEM. Essa integração deverá garantir o fornecimento das seguintes informações, para visualização, consolidação, correlação e alerta de eventos de segurança:

1.1.14.1. Acessos a credenciais privilegiadas, incluindo solicitação, liberação e revogação;

1.1.14.2. Autenticação e revogação de acessos.

1.1.15. Controlar e monitorar sessões usando protocolos padrões e acesso remoto, incluindo RDP, HTTP/HTTPS e SSH;

1.1.16. Ser capaz de recuperar senhas guardadas na solução, em caso de inviabilidade de conexão por meio de sessão auditada, para acesso direto ao ativo;

1.1.17. Integrar-se com soluções de autenticação de duplo fator através do protocolo RADIUS, Single Sign on via SAML ou OIDC e Time-Based One-time Password (TOTP);

1.1.18. Garantir que os usuários da solução tenham visualização somente dos recursos que tem capacidade de requerer acesso;

1.1.19. Permitir o agrupamento lógico de sistemas alvo de modo a simplificar a configuração de políticas de acesso;

1.1.20. Possuir recurso que permita a integração de terceiros utilizando scripts, macros, comandos, chamadas executáveis e protocolos de rede, incluindo SSH, API REST e HTTP/HTTPS;

1.1.21. Possuir recurso que permita a integração de terceiros utilizando scripts, macros, comandos, chamadas executáveis e protocolos de rede, incluindo SSH, API REST e HTTP/HTTPS;

1.1.22. Garantir requisitos de segurança na guarda de credencias, incluindo criptografia no tráfego de informações, suportando, no mínimo, TLS 1.2;

1.1.23. Gerenciar senhas privilegiadas de aplicações, de modo a evitar que sejam senhas estáticas em códigos-fonte (hardcoded), garantindo os seguintes aspectos:

1.1.23.1. Solicitação de credenciais via REST sob demanda ao invés de credenciais estáticas;

1.1.23.2. Atualização automática de contas no banco de dados de senhas;

1.1.23.3. Inscrição automática de sistemas alvo sem aguardar por atualizações dinâmicas;

1.1.23.4. Integração ao cofre da solução, utilizando a mesma interface Web;

1.1.23.5. Configurações de segurança que garantam o acesso apenas por aplicações permitidas, suportando no mínimo o endereço de origem das requisições, nome de usuário, autenticação por certificados e/ou caminho da aplicação.

1.1.24. Permitir a criação de fluxos customizáveis de aprovação de acesso privilegiado, garantindo os seguintes aspectos:

1.1.24.1. Configuração de acessos pré-aprovados;

1.1.24.2. Interface para solicitar e aprovar acessos, com exposição do motivo;

1.1.24.3. Notificação em casos de acessos não aprovados para solicitantes.

1.1.25. Prover interface Web para administração da solução, permitindo a autenticação por meio de usuário e senha local, Active Directory, LDAP e métodos de multifatores (MFA);

1.1.26. Possuir mecanismo de backup e restore de todos os dados e configuração da solução, incluindo recurso de exportação para um servidor remoto, de maneira automática ou agendamento;

1.1.27. Prover relatórios de auditoria que disponibilizem informações das interações dos usuários, tais como atividades de login, adição e remoção de senhas privilegiadas, endereço IP de máquina de origem e do destino alvo, atividades administrativas de delegação e revogação de acesso e eventos agendados. Os relatórios devem ser filtrados por período, tipo de operação, sistema e usuários;

1.1.28. Prover relatórios de conformidade que disponibilizem operações, incluindo lista de sistemas gerenciados, eventos de alteração de senha, auditoria de contas e alertas de segurança

1.2. **Módulo de gerenciamento de elevação e delegação de privilégios**

1.2.1. Incluir o fornecimento de agentes locais para 50 (cinquenta) servidores Microsoft Windows e 200 (duzentos) servidores Unix/Linux;

1.2.2. Para servidores Microsoft Windows, permitir a elevação de privilégios de aplicações autorizadas em regras pré-definidas, a fim de atribuir o direito de administrador somente às tarefas permitidas para cada tipo de usuário, sem a necessidade de utilização de contas com direitos administrativos locais ou de domínio, atendendo aos seguintes requisitos:

1.2.2.1. Suportar os sistemas operacionais Microsoft Windows Server 2012 e superiores;

1.2.2.2. Permitir a criação de regras para cada aplicativo ou processo autorizado, de forma que cada usuário, mesmo com o privilégio de usuário convencional, possa exercer funções administrativas controladas;

1.2.2.3. Permitir a elevação de privilégios de acordo com a origem, permitindo estabelecer restrições como discos, caminhos de rede, nome de arquivos e nome de pastas;

1.2.2.4. Permitir a execução de executáveis que requerem elevação através de User Account Control (UAC) e de aplicativos que pertençam a um proprietário confiável (System, Administradores ou Trusted Installer).

1.2.2.5. Permitir a desinstalação de aplicativos;

1.2.2.6. Suportar a utilização de variáveis de sistema e de usuário;

1.2.2.7. Permitir o controle de ações em serviços do Windows, garantindo a criação de regras como parar, iniciar, pausar e resumir serviços, bem como a criação de regras baseadas no nome e nome de exibição do serviço, suportando a possibilidade de uso de expressões regulares;

1.2.2.8. Permitir a elevação de privilégios de aplicativos contidos na loja do Windows, classificando por versão da aplicação, nome do pacote e editor (publisher);

1.2.2.9. Possuir regras avançadas que permitam que os usuários não se aproveitem das elevações de privilégio executadas pela ferramenta para ações secundárias ou não autorizadas, suportando processos filho que são iniciados a partir de um aplicativo elevado;

1.2.2.10. Restringir a alteração ou modificação de grupos privilegiados locais, como administradores ou power users;

1.2.2.11. Permitir a elevação sobre demanda de aplicativos classificados por regra, isso é, permitir que a opção padrão de "executar como administrador" seja automaticamente elevada a aplicativos previamente configurados, sem qualquer interação ou autenticação necessária ao usuário final;

1.2.2.12. Permitir que as opções de "run as" e "executar como Administrador" sejam omitidas ao usuário final, permitindo a elevação sobre demandas através de uma mensagem customizada oferecida pela ferramenta;

1.2.2.13. Conter relatórios que permitam a correta demonstração do uso de prompts executados pelos usuários;

1.2.2.14. Permitir que mensagens customizadas sejam mostradas antes que uma aplicação seja executada ou bloqueada. Essas mensagens deverão conter níveis de permissionamento para execução, como a possibilidade de re-autenticação, códigos de desafio e resposta para liberação de privilégios sob demanda ou opções para que o usuário selecione ou especifique o motivo da execução;

1.2.2.15. Permitir a criação de aplicativos permitidos;

1.2.2.16. Permitir a atribuição granular para execução de aplicações com nível de privilégio administrativo, sem que esse privilégio seja global na máquina;

1.2.2.17. Permitir a criação de políticas reutilizáveis, contendo os seguintes tipos de aplicações ou tipos de arquivos: executáveis, scripts, aplicações nativas Windows, bibliotecas dinâmicas (DLL), instaladores, controles ActiveX e objetos COM;

1.2.2.18. Implementar o suporte ao nome exato da aplicação, arquivo ou script, para objetos reutilizáveis da solução;

1.2.2.19. Permitir a criação de tokens personalizados a serem atribuídos a um aplicativo para modificar os privilégios dessa atividade. Estes tokens personalizados deverão permitir especificar as associações de grupo, nível de integridade e direitos de acesso a processos do Windows;

1.2.2.20. Permitir elevação de scripts e comandos individuais do cliente PowerShell executados em uma máquina remota;

1.2.2.21. Suportar a elevação de scripts aprovados, incluindo scripts do tipo batchs, scripts do Windows e PowerShell. Nessa funcionalidade, os scripts e comandos do PowerShell devem ser colocados em uma lista de permissões para bloquear o uso de scripts, comandos e cmdlets não autorizados, sem a necessidade de políticas específicas do PowerShell ou clientes próprios para esta execução;

1.2.2.22. Realizar varreduras fazendo uso das funcionalidades instaladas no sistema operacional alvo para catalogar arquivos existentes nas máquinas;

1.2.2.23. Identificar o uso de aplicativos e a tentativa de uso, incluindo aplicativos bloqueados e restritos, elevações sobre demanda, elevações com justificativa ou canceladas pelo usuário final;

1.2.2.24. Manter todas as políticas em cache a serem aplicadas ao servidor de destino, ainda que não esteja conectado à rede corporativa.

1.2.3. Para servidores Unix/Linux, garantir o controle, elevação de privilégios e bloqueio de

comandos, mesmo que o acesso seja realizado diretamente no servidor de destino, sem passar pelo cofre de senhas, fazendo uso de agente instalado no sistema ou método análogo, atendendo aos seguintes requisitos:

1.2.3.1. Implementar modelo de delegação de privilégios mínimos, removendo a necessidade de os usuários efetuarem logon como root, permitindo que a conta do usuário root tenha controles de segurança mais restritos;

1.2.3.2. Prover controle de comandos, possuindo a possibilidade de criar lista de comandos permitidos (allowlist) e bloqueados (blocklist), assim como lista de comandos alterados (alias);

1.2.3.3. Ser não-intrusiva e não requerer reconfiguração do kernel ou reinicialização do sistema;

1.2.3.4. Permitir que os usuários executem comandos específicos e conduzam sessões remotamente sem autenticar-se diretamente, utilizando credenciais privilegiadas;

1.2.3.5. Integrar-se com o Pluggable Authentication Module (PAM) para verificação de segurança secundária, como senha e MFA, ao elevar um comando;

1.2.3.6. Oferecer suporte à política de acessos dinâmicos que utiliza fatores como hora, dia e local para tomar decisões de elevação de privilégio;

1.2.3.7. Ser capaz de interceptar as chamadas da biblioteca relacionadas ao sistema de arquivos. Nesse sentido, deverá controlar as atividades no ativo de destino como criação e exclusão de arquivos e diretórios, mudança de nome de arquivos e diretórios, abertura de arquivos para escrita, comandos chown e chmod e ligações entre arquivos;

1.2.3.8. Ser capaz de controlar, bloquear e auditar comandos executados em scripts;

1.2.3.9. Oferecer suporte ao recurso de File Integrity Monitoring (FIM) que audita e relata alterações nos arquivos críticos de políticas, sistemas, aplicativos e dados;

1.2.3.10. Realizar o controle mediante interceptação do comando antes que ele seja executado, permitir a liberação de comandos privilegiados a usuários comuns, permitir que os comandos executados em sistemas monitorados sejam gravados em modo texto no repositório seguro de credenciais e permitir o agrupamento de comandos, bem como a utilização de coringas para uma definição de parâmetros;

1.2.3.11. Possuir funcionalidade que permita definir variáveis de ambiente no momento da execução de um comando, independente da definição realizada pelo usuário ou do perfil, incluindo as variáveis PATH, ENV, BASH_ENV, GLOBIGNORE e SHELLOPTS;

1.2.3.12. Disponibilizar a funcionalidade de restrição de shell, que impossibilite que scripts executem comandos não permitidos pelas regras definidas na solução;

1.2.3.13. Permitir a criação de ponte ao Active Directory baseada em agentes, permitindo a autenticação com usuários do Active Directory em sistemas Unix/Linux;

1.2.3.14. Oferecer suporte à adesão nativa dos sistemas Unix/Linux ao Active Directory, sem a instalação de software no controlador de domínio ou a modificação do schema do Active Directory;

1.2.3.15. Oferecer suporte ao acesso de compartilhamento de arquivos de rede remota para sistemas Unix/Linux;

1.2.3.16. Oferecer suporte à autenticação Kerberos para máquinas Unix/Linux ingressadas no domínio, não dependendo da solução de cofre de senhas para esta integração;

1.2.3.17. Suportar autenticação offline quando a conectividade de rede entre máquinas Unix/Linux e controladores de domínio não estiverem disponíveis;

1.2.3.18. Não depender de conexão ao cofre digital para autenticar os servidores Linux/Unix ao Active Director

1.3. **Módulo de acesso seguro:**

1.3.1. A solução deverá incluir o fornecimento de módulo de acesso remoto seguro, que permita a intermediação de conexões privilegiadas entre usuários e ativos críticos da infraestrutura de TI da CONTRATANTE, com funcionalidades de proxy, gravação de sessões, controle de comandos e autenticação reforçada.

1.3.2. O módulo deverá ser licenciado de forma a atender cumulativamente aos seguintes requisitos mínimos de capacidade:

1.3.2.1. Permitir acesso seguro a pelo menos 250 (duzentos e cinquenta) ativos corporativos (servidores, dispositivos de rede, sistemas críticos, etc.);

1.3.2.2. Suportar até 1.500 (mil e quinhentos) credenciais, simultâneos ou cadastrados, conforme o modelo de licenciamento adotado pela solução.

1.3.2.3. A exigência de atendimento a ambos os requisitos é **cumulativa**, sendo necessário que a solução fornecida tenha capacidade técnica e de licenciamento adequada para suportar **simultaneamente** o número de ativos e o número de usuários especificados.

1.3.3. Suportar o acesso externo a rede sem qualquer necessidade de utilização de VPN ou método similar de acesso;

1.3.4. Permitir o acesso remoto, no mínimo, aos seguintes sistemas operacionais:

1.3.4.1. Microsoft Windows 10 e superiores.;

1.3.4.2. Servidores Windows Server 2012 e superiores;

1.3.4.3. Linux Red Hat Enterprise 6.0 e superiores.

1.3.5. Utilizar protocolos de comunicação fazendo uso de criptografia TLS 1.2 ou superior;

1.3.6. Suportar o funcionamento a redes que não estão conectadas diretamente a internet e a redes seguras;

1.3.7. Suportar o acesso sem necessidade de permissão prévia para o acesso a desktops e servidores;

1.3.8. Possibilitar o acesso a dispositivos de rede via SSH, como roteadores e switches;

1.3.9. Disponibilizar aos usuários, no mínimo, as seguintes formas de acesso a console da solução:

1.3.9.1. Console local, instalada no desktop do usuário, suportando os sistemas operacionais Microsoft Windows e Unix/Linux;

1.3.9.2. Console de acesso Web, sem a necessidade de instalação de plugins ou agentes.

1.3.10. Suportar provedores externos de identidades para autenticação, incluindo, no mínimo, servidores LDAP, Active Directory, RADIUS e Kerberos, bem como atribuir privilégios com base na hierarquia e nas configurações de grupo já especificadas nos respectivos servidores;

1.3.11. Integrar-se com soluções de autenticação de duplo fator através de protocolo RADIUS, Single Sign-on via SAML ou OIDC e Time-Based One-Time Password (TOTP);

1.3.12. Suportar o uso de um certificado assinado por uma autoridade certificadora válida;

1.3.13. Permitir o agendamento para liberação do acesso remoto, incluindo notificação por e-mail aos destinatários designados;

1.3.14. Permitir forçar o encerramento da sessão remota pelo supervisor, com notificação ao cliente;

1.3.15. Prover monitoramento ao vivo e gravação da sessão, com registro completo das atividades executadas durante a sessão executada pelos usuários;

1.3.16. Limitar o acesso a aplicativos especificados no sistema remoto, incluindo a acesso a área de trabalho remota;

1.3.17. Suportar filtro de comandos durante as sessões SSH, visando evitar que o usuário inadvertidamente use um comando que pode causar danos ao servidor acessado;

1.3.18. Suportar a injeção automática de credenciais em sistemas Windows, permitindo que os usuários autentiquem ou elevem privilégios sem revelar credenciais, bem como a ação de "executar como";

1.3.19. Suportar a injeção automática de credenciais em sistemas Unix/Linux, permitindo que os usuários autentiquem ou elevem privilégios sem revelar credenciais, bem como a utilização em conjunto com o sudo;

1.3.20. Suportar o acesso com os seguintes modos:

1.3.20.1. Através de clientes instalados;

1.3.20.2. Através de agente de proxy local, que permite o acesso a sistemas autônomos em uma rede, sem cliente pré-instalado;

1.3.20.3. Acesso via agente de proxy local, que permite o acesso a sistemas em uma rede remota que não tenha uma conexão de internet nativa;

1.3.21. Suportar Remote Desktop Protocol (RDP), permitindo que os usuários colaborem em sessões auditadas e gravadas;

1.3.22. Prover acesso a dispositivos de rede habilitados para SSH através de um cliente de proxy efetuando a conexão localmente;

1.3.23. Prover acesso a páginas Web a partir de agente de proxy local, onde os usuários receberão apenas uma conexão a uma página Web local em uma sessão auditada e gravada;

1.3.24. Permitir o monitoramento em tempo real das sessões de acesso feitas a ativos publicados na ferramenta;

1.3.25. Permitir a configuração de tempos limites para sessões ociosas, em que seja possível definir o tempo máximo para que um usuário inativo seja desconectado automaticamente;

1.3.26. É desejável que a solução permita que os usuários transfiram arquivos da máquina em que está conectado para o sistema remoto, através da console da solução e sem necessidade de uso de ferramentas de terceiros;

1.3.27. É desejável que a solução permita que os usuários compartilhem sessões de acesso com outros usuários do sistema, permitindo que os administradores colaborem em uma mesma sessão. Esta colaboração deve ser possível com usuários internos e externos através de convite;

1.3.28. É desejável que a solução permita oferecer aos usuários conectados a capacidade de ver informações do sistema sem que seja necessário ter acesso a console do ativo;

1.3.29. É desejável que a solução permita oferecer aos usuários a capacidade de executar tarefas do sistema fora do compartilhamento de tela, como por exemplo reiniciar um serviço em servidores com sistema operacional Windows;

1.3.30. É desejável que a solução permita oferecer a opção de prover acesso à linha de comandos dos servidores sem a necessidade de compartilhamento de tela, permitindo aos administradores a execução de comandos remotos via conexões lentas de internet.

1.4. Serviço de operação assistida

1.4.1. A operação assistida terá início após a instalação e configuração da solução e a emissão de ordem de serviço específica.

1.4.2. A operação assistida consiste na permanência de técnico da CONTRATADA para operar e solucionar todas as dúvidas e problemas que possam ocorrer com a solução; na transferência de conhecimento e esclarecimento de dúvidas para a equipe técnica da CLDF; no acompanhamento presencial do funcionamento dos equipamentos instalados e a pronta intervenção em caso de qualquer problema detectado no ambiente.

1.4.3. A CONTRATADA deverá fornecer o serviço de operação assistida com presença física, ou remota (desde que acordado com a CONTRATANTE), de técnico da CONTRATADA, em horário comercial (8 x 5) e suporte em regime 24 x 7, em até 60 (sessenta) dias corridos.

1.4.4. O técnico deverá ter experiência com todos os componentes do sistema, para que oriente e opere todo sistema e transfira para a equipe da CONTRATANTE o conhecimento necessário para que possa operá-lo.

1.4.5. O técnico alocado deve ser devidamente certificado pelo fabricante para suporte na solução adquirida.

1.4.6. O técnico deverá estar identificado com crachá da CONTRATADA durante sua permanência nas dependências da CLDF.

1.5. **Serviço de capacitação:**

1.5.1. A CONTRATADA deverá prestar serviço de capacitação técnica referente à solução fornecida, observando os seguintes requisitos:

1.5.1.1. A capacitação deverá ter **carga horária mínima de 20 (vinte) horas**, distribuídas em dias consecutivos, com duração máxima de **4 (quatro) horas por dia**, totalizando ao menos 5 dias de treinamento.

1.5.1.2. A capacitação deverá contemplar a participação de até **10 (dez) integrantes** indicados pela CONTRATANTE, com foco nos aspectos operacionais, administrativos e técnicos da solução.

1.5.1.3. O treinamento deverá ocorrer **presencialmente no Distrito Federal** ou por **meio remoto**, desde que a carga horária total seja respeitada e haja interação síncrona com o instrutor. No caso de modalidade presencial, as **instalações físicas serão fornecidas pela CONTRATADA**.

1.5.1.4. A capacitação deverá incluir o **fornecimento de material didático digital oficial do fabricante**, em língua portuguesa, com acesso antecipado ao conteúdo pelo menos 48h antes do início do curso.

1.5.1.5. A capacitação deverá ser ministrada por **instrutor com qualificação técnica compatível com a solução**, cuja competência deverá ser comprovada por:

1.5.1.5.1. **Certificação oficial do fabricante da solução contratada**; e

1.5.1.5.2. **Experiência mínima de 2 (dois) anos na aplicação ou implantação da tecnologia contratada**, comprovada por meio de currículo, declarações ou atestados de capacidade técnica vinculados ao profissional.

1.5.2. A CONTRATADA deverá apresentar à CONTRATANTE, no prazo de até **10 (dez) dias após a assinatura do contrato**, um **cronograma detalhado de execução da capacitação**, contendo datas propostas, modalidade, nomes dos instrutores, estrutura de tópicos e recursos didáticos. O cronograma estará sujeito à **validação e aprovação pela CONTRATANTE**.

1.6. **Suporte, assistência técnica, manutenção e garantia da solução pelo prazo 36 (trinta e seis) meses.**

1.6.1. A CONTRATADA deverá prestar suporte técnico, assistência, manutenção e garantia da solução fornecida pelo período de 36 (trinta e seis) meses, a contar da data do recebimento

definitivo da solução, observando os seguintes requisitos:

1.6.1.1. O suporte deverá compreender manutenção corretiva e preventiva, abrangendo:

1.6.1.1.1. Correção de falhas ou inconsistências no funcionamento da solução;

1.6.1.1.2. Atualizações de software, versões e módulos;

1.6.1.1.3. Fornecimento de patches de segurança e correção, sem custos adicionais.

1.6.1.2. O suporte técnico será prestado de forma remota, em regime 24x7 (vinte e quatro horas por dia, sete dias por semana).

1.6.1.3. Havendo parada crítica ou falha grave que comprometa a continuidade operacional da solução, e mediante requisição formal da CONTRATANTE, o atendimento deverá ser prestado presencialmente (on-site) no local de prestação dos serviços, dentro dos prazos estipulados no contrato.

1.6.1.4. A assistência técnica deverá ser realizada por profissional devidamente qualificado e certificado pelo fabricante da solução contratada, com experiência comprovada de, no mínimo, 2 (dois) anos na tecnologia em questão, por meio de currículo e/ou declaração de capacidade técnica individual.

1.6.1.5. O suporte deverá incluir também:

1.6.1.5.1. Configuração de todos os componentes para garantir o funcionamento pleno e otimizado da solução;

1.6.1.5.2. Prestação de esclarecimentos e orientações técnicas à equipe da CONTRATANTE, de modo a garantir uso adequado e aproveitamento eficiente dos recursos disponíveis.

2. REQUISITOS DE PROJETO E DE IMPLEMENTAÇÃO

2.1. Todos os **serviços de instalação, suporte técnico, assistência técnica, monitoramento e garantia** deverão atender às **especificações técnicas descritas neste Termo de Referência**, abrangendo a **solução de software e seus componentes associados**, em conformidade com os requisitos funcionais e operacionais definidos.

2.2. **Não haverá fornecimento de equipamentos físicos (hardware)** ou instalação de pontos de rede estruturada por parte da CONTRATADA, sendo responsabilidade exclusiva da CONTRATANTE assegurar a infraestrutura necessária (rede, energia, conectividade, permissões administrativas etc.) para o correto funcionamento da solução contratada.

2.3. *Caso a solução envolva appliance virtual ou instalação local em servidor, caberá à CONTRATANTE prover o ambiente computacional adequado, conforme orientações técnicas da CONTRATADA.*

2.4. A CONTRATADA deverá prestar **garantia de funcionamento, suporte técnico e assistência técnica** para todos os **componentes da solução fornecida (inclusive os softwares)**, durante o prazo de **36 (trinta e seis) meses**, contados a partir da data de emissão do **Termo de Recebimento Definitivo**.

2.5. A CONTRATADA deverá disponibilizar uma **central de atendimento (Service Desk)** para abertura e acompanhamento de chamados técnicos, com atendimento em regime **24 (vinte e quatro) horas por dia, 7 (sete) dias por semana**.
O canal de atendimento deverá permitir abertura de chamados por, no mínimo:

2.5.1. Telefone local ou número 0800 (ligação gratuita);

2.5.2. Interface Web (portal);

2.5.3. Correio eletrônico (e-mail institucional).

2.6. Todos os chamados deverão ser **registrados em sistema eletrônico**, com número de protocolo, e permanecer **disponíveis para consulta pela CLDF**, contendo o histórico completo de interações e prazos de resolução.

3. REQUISITOS DE IMPLANTAÇÃO

3.1. Os serviços de instalação, configuração, manutenção, avaliação, bem como intervenções feitas pela CONTRATADA, no ambiente de TI da CLDF, deverão seguir as melhores práticas (forma de execução e apresentação dos resultados) preconizadas pelo ITIL (*Information Technology Infrastructure Library*), como, por exemplo, os aspectos de documentação, manutenção dos níveis de serviço, abertura de ordens de serviço e emissão de relatórios técnicos;

3.2. A instalação lógica e configuração deverá ser realizada por profissional detentor de certificação dos produtos.

4. REQUISITOS DE GARANTIA E MANUTENÇÃO

4.1. **Abrangência da Garantia**

4.1.1. A CONTRATADA deverá garantir o pleno funcionamento da **solução de software fornecida** por um período mínimo de **36 (trinta e seis) meses**, contados a partir do **primeiro dia útil subsequente ao recebimento definitivo do objeto**. A garantia deve abranger:

4.1.1.1. Manutenção corretiva (correção de falhas e inconsistências);

4.1.1.2. Aplicação de atualizações, patches de segurança e versões corretivas;

4.1.1.3. Suporte técnico contínuo, sem limitação de número de chamados.

4.1.2. **Plano de Suporte do Fabricante**

4.1.2.1. A CONTRATADA deverá adquirir e manter **plano de suporte oficial do fabricante da solução**, com as seguintes características:

4.1.2.2. Atendimento 24 horas por dia, 7 dias por semana (24x7);

4.1.2.3. SLA de **resposta inicial em até 2 horas**, para todos os chamados (críticos e não críticos);

4.1.2.4. Conclusão de atendimento conforme nível de criticidade (descritos abaixo).

4.1.3. **Prazo de Atendimento Técnico por Nível de Criticidade**

4.1.3.1. **Alta criticidade**:

4.1.3.1.1. Chamados que envolvam **interrupção de serviços de produção** deverão ser concluídos pela CONTRATADA no prazo máximo de **24 (vinte e quatro) horas**.

4.1.3.2. **Média criticidade**:

4.1.3.2.1. Chamados relacionados a **interrupções em serviços não críticos, redução de níveis de redundância**, ou necessidade de **aplicação de patches de segurança críticos** deverão ser concluídos no prazo máximo de **60 (sessenta) horas**.

4.1.3.3. **Baixa criticidade**:

4.1.3.3.1. Chamados que tratem de **requisições comuns, dúvidas operacionais, lentidão ou demais ocorrências sem impacto direto na continuidade dos serviços** deverão ser concluídos no prazo máximo de **96 (noventa e seis) horas**.

4.1.3.4. A **CONTRATADA será corresponsável**, em conjunto com o fabricante, pela **observância rigorosa dos prazos** estabelecidos para cada nível de criticidade.

5. REQUISITOS DE METODOLOGIA DE TRABALHO

5.1. O fornecimento e ativação da solução contratada está condicionado ao recebimento, pela CONTRATADA, de **Ordem de Serviço (OS)** ou instrumento equivalente, emitido pela CONTRATANTE.

5.2. A OS deverá indicar as **especificações da solução**, contendo a descrição dos componentes contratados, a quantidade de licenças, bem como os dados técnicos e operacionais necessários para instalação e ativação.

5.3. A CONTRATADA deverá disponibilizar **meios para contato e registro de ocorrências** com funcionamento em regime ininterrupto (**24 horas por dia, 7 dias por semana**), sendo:

5.3.1. Atendimento **eletrônico** (portal web, e-mail ou sistema próprio);

5.3.2. Atendimento **telefônico**, com número local ou 0800 (ligação gratuita).

5.4. O **acompanhamento da entrega e ativação da solução** deverá ser realizado continuamente pela CONTRATADA, que deverá **comunicar à CONTRATANTE** qualquer intercorrência relevante que possa afetar os prazos, a qualidade ou a continuidade da prestação dos serviços.

6. REQUISITOS DE SEGURANÇA, SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

6.1. A solução deverá atender aos princípios e procedimentos elencados na Política de Segurança da Informação da CLDF (POSID).

6.2. A solução deverá atender aos princípios da **Segurança da Informação**: confidencialidade, integridade, disponibilidade e autenticidade.

6.3. Deve possuir **criptografia de dados sensíveis**, autenticação multifator (MFA) e controle de sessões em tempo real.

6.4. Os registros de auditoria devem ser **imutáveis e exportáveis**, com controle de acesso restrito a usuários com perfil autorizado.

7. REQUISITOS LEGAIS

7.1. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, ao AMD nº 71/2023 da CLDF, à Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e a outras legislações aplicáveis.

7.2. A CONTRATADA deverá observar as disposições da Lei 13.709/2018, Lei Geral de Proteção de Dados - LGPD, quanto ao tratamento dos dados pessoais que lhe forem confiados, em especial quanto à finalidade e boa-fé na utilização de informações pessoais para consecução dos fins a que se propõe o presente contrato;

7.3. A CONTRATADA deverá observar as disposições do Ato da Mesa Diretora nº 85/2022 e suas alterações posteriores, que regulamenta a aplicação Lei nº 13.709/2018 no âmbito da CLDF.

7.4. A CLDF figura na qualidade de Controlador dos dados quando fornecidos à CONTRATADA para tratamento, sendo esta enquadrada como Operador dos dados. A CONTRATADA será Controladora dos dados com relação a seus próprios dados e suas atividades de tratamento.

7.5. A CONTRATADA está obrigada a guardar o mais completo sigilo por si, por seus empregados ou prepostos, nos termos da Lei Complementar nº 105/2001 e da LGPD, cujos teores declaram ser de seu inteiro conhecimento, em relação aos dados, informações ou documentos de qualquer natureza, exibidos, manuseados ou que por qualquer forma ou modo venham tomar conhecimento ou ter acesso, em razão deste contrato, ficando, na forma da lei, responsáveis pelas

consequências da sua divulgação indevida e/ou descuidada ou de sua incorreta utilização, sem prejuízo das penalidades aplicáveis nos termos da lei.

7.6. Os dados pessoais tratados e operados serão eliminados após o término contrato, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

7.6.1. cumprimento de obrigação legal ou regulatória pelo controlador;

7.6.2. estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

7.6.3. Uso exclusivo do Controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

7.7. Os casos omissos em relação ao tratamento dos dados pessoais que forem confiados à CONTRATADA, e não puderem ser resolvidos com amparo na LGPD, deverão ser submetidos à Administração do contrato para que decida previamente sobre a questão.

7.8. A Câmara Legislativa e aqueles que, sob sua determinação, atuarem na condição de Operadores de tratamento de dados pessoais, devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

8. REQUISITOS TEMPORAIS

8.1. A entrega, instalação e ativação da solução contratada deverá ser realizada no prazo máximo de **60 (sessenta) dias corridos**, contados a partir do recebimento da **Ordem de Serviço (OS)** ou instrumento equivalente, emitido pela CONTRATANTE.

8.2. Esse prazo poderá ser **prorrogado de forma excepcional**, mediante solicitação **formal e justificada** da CONTRATADA, desde que **expressamente autorizada** pela CONTRATANTE, nos termos da legislação vigente.

ANEXO II – TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO

CONTRATO Nº			
GESTOR DO CONTRATO		**MATRÍCULA**	
CONTRATADA		**CNPJ**	

DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de quaisquer informações de propriedade da CONTRATANTE e disponibilizadas por força dos procedimentos necessários para a execução do objeto do contrato celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18/11/2011, os Decretos 7.724, de 16/05/2012 e 7.845, de 14/11/2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em

qualquer grau de sigilo, e normas internas pertinentes ao assunto.

A CONTRATADA se compromete, por intermédio do presente instrumento, a não divulgar sem autorização quaisquer informações de propriedade da CONTRATADA, em conformidade com as seguintes cláusulas e condições:

DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do contrato principal.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I - A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II - A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao contrato.

III - A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV - Todas as condições, TERMOS e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V - O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI - Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII - O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo ao contrato principal;

VIII - Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar informações para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

CLÁUSULA PRIMEIRA

A CONTRATADA reconhece que, em razão da sua prestação de serviços à CLDF, consoante o Contrato ao qual esse termo de vincula, mantém ou poderá manter contato com informações sigilosas nos termos lei, normas e regulamentos. Estas informações devem ser tratadas

confidencialmente sob qualquer condição e não podem ser divulgadas a terceiros não autorizados, aí se incluindo servidores da CLDF e empregados da CONTRATADA, sem a expressa e escrita autorização do representante legal signatário do contrato ora referido.

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do contrato, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas informações, que se restringem estritamente ao cumprimento do contrato.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal dos servidores da CLDF que atuarão diretamente na execução do contrato sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as informações deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do contrato.

Parágrafo Sexto – A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das informações, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das informações por seus agentes, representantes ou por terceiros;

III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das informações, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações.

CLÁUSULA SEGUNDA

As informações a serem tratadas confidencialmente são aquelas assim consideradas no

âmbito da CLDF que, por sua natureza, não são ou não deveriam ser de conhecimento de terceiros, tais como:

I. Peças que compõem os autos de processos legislativos e administrativos;

II. Outras informações de natureza financeira, administrativa, contábil e jurídica;

III. Senhas, topologias, endereços de rede, formas de acesso aos serviços internos, etc;

III. O TERMO DE COMPROMISSO também abrange toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CLDF e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao contrato, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do contrato celebrado entre as partes.

CLÁUSULA TERCEIRA

A CONTRATADA reconhece que as referências dos incisos da Cláusula Segunda deste Termo são meramente exemplificativas, e que outras hipóteses de confidencialidade que já existam ou venham ser como tal definidas no futuro devem ser mantidas sob sigilo.

Parágrafo Único - Em caso de dúvida acerca da natureza confidencial de determinada informação, a CONTRATADA deverá mantê-la sob sigilo até que venha a ser autorizado expressamente pelo representante legal da CLDF, a tratá-la diferentemente. Em hipótese alguma, a ausência de manifestação expressa da CLDF poderá ser interpretada como liberação de qualquer dos compromissos ora assumidos.

CLÁUSULA QUARTA

A CONTRATADA reconhece que está ciente de que deverá seguir a Política de Segurança da Informação da CLDF, assim como todos os seus documentos acessórios já criados ou que venham a ser criados.

Parágrafo Único – A CONTRATADA declara que seguirá todas as políticas, normas e procedimentos de segurança da informação definidos e/ou seguidos pela CLDF, vigentes ou que venham a ser criados.

CLÁUSULA QUINTA

A CONTRATADA recolherá, ao término do respectivo contrato principal, para imediata devolução à CLDF, todo e qualquer material de propriedade deste, inclusive notas pessoais envolvendo matéria sigilosa a este relacionada, registro de documentos de qualquer natureza que tenham sido criados, usados ou mantidos sob seu controle ou posse, seja de seus empregados, prestadores de serviço, fornecedores, com vínculo empregatício ou eventual com a CONTRATADA, assumindo o compromisso de não utilizar qualquer informação sigilosa ou confidencial a que teve acesso enquanto contratado pela CLDF. Todos os equipamentos utilizados para a realização dos serviços do contrato deverão ter dados temporários apagados, e poderão ser conferidos pela equipe técnica da CLDF após o termino dos serviços.

Parágrafo Único - A CONTRATADA determinará a todos os seus empregados, e prestadores de serviços que estejam, direta ou indiretamente, envolvidos com a prestação de serviços objeto do

contrato, a observância do presente instrumento e a assinatura de Termos de Ciência individuais, adotando todas as precauções e medidas para que as obrigações oriundas do presente instrumento sejam efetivamente observadas.

CLÁUSULA SEXTA

A CONTRATADA obriga-se a informar imediatamente à CLDF qualquer violação das regras de sigilo ora estabelecidas que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo, bem como de seus empregados e preposto.

CLÁUSULA SÉTIMA

A quebra do sigilo e/ou da confidencialidade das informações, bem como o descumprimento de quaisquer das cláusulas do presente instrumento, devidamente comprovado, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do contrato firmado entre as partes.

Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades administrativa, civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme legislação vigente.

CLÁUSULA OITAVA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do contrato. Ou seja, as obrigações a que alude este instrumento perdurarão inclusive após a cessação do vínculo contratual entre a CONTRATADA e a CONTRATANTE e abrangem as informações presentes e futuras.

CLÁUSULA NONA

A CONTRATADA se compromete no âmbito do contrato objeto do presente instrumento, a apresentar à CLDF termo de ciência individual de adesão e aceitação das presentes cláusulas, de cada integrante ou participante da equipe que prestar ou vier a prestar os serviços especificados neste contrato.

ASSINATURA

Declaro manter sigilo e respeito às normas de segurança vigentes na Câmara Legislativa do Distrito Federal.

Representante Legal da Contratada:
Nome:
Cargo/Função:
CPF:
Telefone:
E-mail:

ANEXO III - TERMO DE CIÊNCIA

CONTRATO Nº		DATA	
GESTOR DO CONTRATO		MATRÍCULA	
CONTRATADA		CNPJ	

Por este instrumento, os funcionários abaixo declaram ter ciência e conhecer o teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes na Contratante.

FUNCIONÁRIOS

_____
<nome>

_____
<nome>

_____
<nome>

_____
<nome>

ANEXO IV - MODELO SUGERIDO PARA APRESENTAÇÃO DOS ATESTADOS DE CAPACIDADE TÉCNICA

ATESTADO DE CAPACIDADE TÉCNICA (OU DECLARAÇÃO)

Atestamos (ou Declaramos) que a empresa _____, inscrita no CNPJ (MF) nº _____, inscrição estadual nº _____, estabelecida no (a)_____ prestou serviços de _____ para este órgão (ou para esta empresa).

Atestamos (ou Declaramos), ainda, que os compromissos assumidos pela empresa foram cumpridos satisfatoriamente, nada constando em nossos arquivos que o desabone comercial ou tecnicamente.

Local e data

_____

Assinatura e carimbo do emissor

Observações:
1) Este atestado (ou declaração) deverá ser emitido(a) em papel que identifique o órgão (ou empresa) emissor; e
2) O objeto da contratação deve estar explícito no atestado/declaração de capacidade técnica.

ANEXO V - MODELO DE PROPOSTA DE PREÇOS

ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	QUANTIDADE	VALOR ESTIMADO UNITÁRIO (R$)	VALOR TOTAL ESTIMADO (R$)
1	Solução de gerenciamento de contas e de acessos privilegiados (PAM)	Licença	1	R$	R$
2	Serviço de instalação e configuração	Atividade	1	R$	R$
3	Serviço de operação assistida	Atividade	1	R$	R$
4	Serviço de capacitação	Atividade	1	R$	R$
VALOR TOTAL					**R$**

- Os valores acima incluem todos os encargos, tributos, despesas operacionais, licenciamento, suporte técnico, garantia e demais custos necessários à entrega integral do objeto, conforme definido no Termo de Referência.
- A proposta é válida por, no mínimo, 60 (sessenta) dias corridos.
- Declaro, sob as penas da lei, que os preços ofertados são exatos, completos e refletem a integralidade dos custos envolvidos.

Conforme AMD nº 71, de 2023, art. 13, § 6º, o Termo de Referência será assinado pela Equipe de Planejamento da Contratação e pelo Chefe da respectiva Área Técnica de TI e aprovado pelo Chefe da Área de TI.

Documento assinado eletronicamente por **AIMBERE GIANNACCINI - Matr. 18327, Integrante Técnico**, em 02/12/2025, às 18:39, conforme Art. 30, do Ato da Mesa Diretora n° 51, de 2025, publicado no Diário da Câmara Legislativa do Distrito Federal nº 62, de 27 de março de 2025.

Documento assinado eletronicamente por **FABIO VIRGILIO DE SOUZA NEVES - Matr. 24554, Integrante Técnico**, em 02/12/2025, às 18:41, conforme Art. 30, do Ato da Mesa Diretora n° 51, de 2025, publicado no Diário da Câmara Legislativa do Distrito Federal nº 62, de 27 de março de 2025.

Documento assinado eletronicamente por **PEDRO CUNHA REGO CELESTIN - Matr. 22858, Chefe do Setor de Infraestrutura de Tecnologia da Informação**, em 03/12/2025, às 11:32, conforme Art. 30, do Ato da Mesa Diretora n° 51, de 2025, publicado no Diário da Câmara Legislativa do Distrito Federal nº 62, de 27 de março de 2025.

A autenticidade do documento pode ser conferida no site: http://sei.cl.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 Código Verificador: **2446889** Código CRC: **EC4B5BA9**.