CMI - TERMO DE REFERÊNCIA - TR - AQUISIÇÕES

Brasília, 09 de junho de 2023.

1. DEFINIÇÃO DO OBJETO

1.1. Aquisição de solução tecnológica de segurança, proteção antivírus e EndPoint Detection Response (EDR), incluindo licenças de uso, instalação, configuração, atualização da base de vacinas e software, treinamento e suporte técnico especializado pelo período contratado, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

ITEM	ESPECIFICAÇÃO	MÉTRICA OU UNIDADE DE MEDIDA	QUANTITATIVO MÍNIMO DE LICENÇAS A SEREM ADQUIRIDAS ANUALMENTE .	QUANTITATIVO MÁXIMO DE LICENÇAS A SEREM ADQUIRIDAS ANUALMENTE, SOB DEMANDA, APENAS EM CASO DE NECESSIDADE.	QUANTITATIVO TOTAL	VALOR UNITÁRIO	SUBTOTAL	VALOR TOTAL
1	Aquisição de solução tecnológica de segurança, proteção antivírus e EndPoint Detection Response (EDR), incluindo licenças de uso, instalação, configuração, suporte técnico especializado e atualização da base de vacinas e software, pelo período contratado para endpoints do tipo **estações de trabalho,** desktops, notebooks e máquinas virtuais.	licenças	1575	400	1975	R$ 264,53	R$ 522.446,75	**R$ 657.846,75**
2	Aquisição de solução tecnológica de segurança, proteção antivírus e EndPoint Detection Response (EDR), incluindo licenças de uso, instalação, configuração, suporte técnico especializado e atualização da base de vacinas e software, pelo período contratado para endpoints do tipo **plataformas móveis** tais como smartphones e tablets, compatíveis com sistema operacional Android e IOS - Apple.	licenças	31	119	150	R$ 416,00	R$ 62.400,00	
3	Operação assistida por 30 (trinta) dias corridos.	unidade	1	não aplicável	não aplicável	R$ 35.000,00	R$ 35.000,00	

4	Treinamento básico, capacitação e transferência de conhecimento para operação e gestão da solução de segurança contratada, com turma de 4 (quatro) alunos.	unidade	2	não aplicável	não aplicável	R$ 19.000,00	R$ 38.000,00	

1.2. Os bens objetos desta contratação são caracterizados como comuns, uma vez que trata-se de aquisição de software antívirus com EDR para proteção e segurança de dados no âmbito da segurança da informação da CLDF.

1.3. O prazo de vigência da contratação é de 12 meses contados da emissão do início da execução contratual a partir da emissão do Termo de Recebimento Definitivo, prorrogável para até 5 anos, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021.

1.3.1. O fornecimento de bens é enquadrado como continuado tendo em vista que trata-se de uma aquisição de segurança cibernética com necessidade perene de proteção de dados no âmbito da CLDF, sendo a vigência plurianual mais vantajosa considerando conforme demonstrado no curso do Estudo Técnico Preliminar.

2. DESCRIÇÃO DA SOLUÇÃO DE TI

2.1. A solução de TI ora tratada consiste na aquisição de:

1. Licenças de proteção antivírus e EndPoint Detection Response (EDR), incluindo licenças de uso, instalação, configuração, suporte técnico especializado e atualização da base de vacinas e software, pelo período contratado para endpoints do tipo **estações de trabalho,** desktops, notebooks e máquinas virtuais. Composta por 1975 (um mil quinhentos e setenta e cinco) licenças para endpoints do tipo **servidores virtuais** (Linux e Windows), **desktop e notebook**.
2. Licenças de antivírus e EndPoint Detection Response (EDR) para proteção de **smartphones e tablets** (androind ou IOS), incluindo licenças de uso, instalação, configuração, atualização da base de vacinas e software, treinamento, atualização e suporte por meio de chamados técnicos durante o período contratado pelo período contratado. Composta por 150 (cento e cinquenta) licenças para endpoits do tipo **plataformas móveis, como tablets e smartphones.**
3. **Operação assistida** por 30 (trinta) dias corridos. 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.
4. **Treinamento**, capacitação e transferência de conhecimento para 8 (oito) alunos divididos em 2 (duas) turma contendo 4 (quatro) alunos cada, para instruir e apoiar o inicio da operação, solucionando 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.

3. FUNDAMENTAÇÃO DA CONTRATAÇÃO

3.1. Este Termo de Referência foi elaborado em consonância com o Estudo Técnico Preliminar elaborado pela Equipe de Planejamento da Contratação, conforme 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 federal nº 14.133, de 1º de abril de 2021.

3.2. A segurança dos ativos de tecnologia da informação - TI da Câmara Legislativa do Distrito Federal -CLDF visa garantir a proteção dos dados, o funcionamento e continuidade das atividades administrativas e legislativas da Casa.

3.3. A CLDF possui diversos ativos em seu parque tecnológico, como computadores pessoais e máquinas servidores. Para prover segurança nesses ativos, faz-se necessário a aquisição de uma solução de *EndPoint Detection Response* - EDR, a SEINF pretende acrescentar uma abordagem avançada para a segurança cibernética que oferece uma visibilidade aprofundada em atividades no endpoint (por exemplo, um computador) e permite que as equipes de segurança respondam rapidamente a ameaças.

3.4. Já o Antivírus, solução atualmente adotada pela Casa, é um software de segurança que protege o sistema apenas contra ameaças de malware, tais como vírus, worm, trojan, spyware, etc. Eles são projetados para detectar e remover essas ameaças de forma automática ou manual. O EDR combina recursos de prevenção de ameaças, detecção de ameaças e resposta a incidentes em um único produto, oferecendo uma defesa mais abrangente e eficaz contra ameaças cibernéticas.

3.5. Enquanto o antivírus é uma ferramenta importante na proteção contra ameaças de malware, o EDR fornece uma visibilidade mais profunda e capacidade de resposta a ameaças mais avançadas e evoluídas.

4. JUSTIFICATIVA PARA CONTRATAÇÃO

4.1. JUSTIFICATIVA

O investimento em segurança da informação visa garantir a proteção dos dados, o funcionamento e continuidade das atividades administrativas e legislativas da Casa.

A CLDF possui diversos ativos em seu parque tecnológico, como computadores pessoais e máquinas servidores. Para prover segurança a esses ativos, faz-se necessário, como medidas primordiais, a proteção contra diversas ameaças digitais, como vírus, trojans etc. Em atendimento à proteção supracitada, a Seção de Infraestrutura de Tecnologia da Informação - SEINF, possui o Contrato-PG Nº 09/2022-NPLC (SEI 0711412), de proteção antivírus bem como a solução nativa integrado ao Windows (Windows Defender) presente em todas as estações de trabalho.

Entende-se que o nível de segurança atual oferecido por esse tipo de solução (antivírus), seja a do Contrato-PG Nº 09/2022-NPLC ou a nativa do Windows (Windows Defender) é insuficiente pra garantir um nível de segurança adequado ao parque tecnológico da CLDF. Portanto, como parte do projeto de modernização e adequação da infraestrutura de TI da CLDF, é necessário investir em outras soluções de segurança que ofereçam mecanismos de proteção mais modernos, avançados e profundos.

A solução de Endpoint Detection and Response (EDR) é a abordagem de segurança cibernética que oferece uma visibilidade aprofundada em atividades no endpoint (por exemplo, um computador) e permite que as equipes de segurança respondam rapidamente a ameaças. Esse tipo de produto combina recursos de prevenção de ameaças, detecção de ameaças e resposta a incidentes em um único produto, oferecendo uma defesa mais abrangente e eficaz contra ameaças cibernéticas.

Com aquisição, a CLDF aumentará sua segurança em camadas, com base nas melhores práticas, em promover um ambiente computacional mais seguro contra ataques cibernéticos, de captura e extorsão de dados, mitigando os riscos para os usuários no uso dos recursos de TI da CLDF.

4.2. **ALINHAMENTO DA SOLUÇÃO AO PDTI DA CLDF**

O objeto desta contratação está em consonância com o Plano Diretor de Tecnologia da Informação – PDTI 2023/2024, conforme abaixo:

OBJ - 5.1 - Garantir sustentação e funcionamento do complexo computacional, página 94 do documento SEI 0967709.			
Ação 3 - Adquirir solução de EDR, PE 29 - Alcançar as Metas e Ações estabelecidas nos Planos Setoriais atribuídos à CMI 2022/2023.			
NEC	**Declarante**	**Necessidade**	**Função institucional**
5.1.12	Coordenadoria de Modernização e Informática - CMI	Realizar manutenção do serviço de proteção de dados.	Representação Legiferação Fiscalização Administração (operação chave) (+) cb,tp

4.3. **Necessidades de negócio**

4.4. SEGURANÇA/ACESSO AOS SISTEMAS/SERVIÇOS DE TI DA CLDF PELOS USUÁRIOS DA CASA

- 4.5. Proteção antivírus e EDR
- 4.6. Controle de dispositivos, de prevenção de intrusão, proteção Endpoint Detection Response (EDR) para máquinas físicas e servidores no domínio da CLDF.
- 4.7. Proteção contra vírus, *zero day*, ransomware, exploits, e outras ameaças avançadas persistentes - ATP, com adoção de técnicas automatizadas de detecção e resposta.

4.8. GERENCIAMENTO E ADMINISTRAÇÃO

- 4.9. Gerência centralizada com relatórios dos dispositivos, informações, alertas e incidentes de segurança em tempo real.
- 4.10. Distribuição de pacotes para qualquer dispositivo n a partir de uma única console de gerenciamento.
- 4.11. Automatização dos procedimentos, reduzindo-se ao indispensável à interferência humana, com capacidade de enviar alertas para áreas correlatas.

4.12. **Necessidades tecnológicas**

4.13. Necessidade de adquirir uma solução de segurança do tipo EDR para proteção da organização contra às crescentes ameaças cibernéticas e à necessidade de uma abordagem proativa para detectar, responder e mitigar ataques em endpoints, como computadores, laptops, servidores e dispositivos móveis.

4.14. **Demais Requisitos**

- 4.15. Compatibilidade, atualização e integração. Compatibilidade com a solução existente **1575 (um mil quinhentos e setenta e cinco) licenças para endpoints do tipo desktop**, marquina virtual e notebook, e mais **31 (trinta e uma) licenças para plataformas móveis** compatíveis com os sistemas operacionais Windows 10, Windows Server 2012 e Windows Server 2016 e suportar integração com Microsoft Active Directory.
- 4.16. Inventário e controle com capacidade de identificar os ativos em toda extensão.
  Automatização dos procedimentos, reduzindo-se ao indispensável à interferência humana, com capacidade de enviar alertas para áreas correlatas.

4.17. **Demais requisitos necessários e suficientes à escolha da Solução de TI**

- 4.18. Manutenção e atualização tecnológica, prestação de garantia, suporte e assistência técnica, com serviços de atualização, manutenção (corretiva e preventiva) e atendimento técnico on-site, sem qualquer ônus adicional para a CLDF.
- 4.19. Central de atendimento e suporte via telefone. A empresa deverá manter central telefônica para abertura de chamados e atendimento técnico.

4.20. **FORMA DE CÁLCULO UTILIZADA PARA A DEFINIÇÃO DO QUANTITATIVO DE BENS E SERVIÇOS QUE COMPÕEM A SOLUÇÃO**

Foram realizadas diligências internas para identificar o quantitativo de licenças necessárias para proteger a infraestrutura da tecnologia da informação da CLDF. Além disso verificamos também expectativas futuras de médio a curto prazo.
Logo, foram realizadas consultas ao Setor de Apoio ao Plenário (SAPLE) que respondeu por meio do (Despacho 1126467). também foram realizadas consultas à Seção de Atendimento e Cultura Digital (SEATI) que indicou por meio Despacho (1124684) o quantivativo necessário presente e expectativas futura de curto e médio prazo. Além disso, o núclo de Servidores e Aplicação por meio do e-mail (SEI 1051613) sinalizo o quantivativo de máquinas virtuais aptas a receberem licenças de proteção.

Quantitativo necessário corrente				
Tipos de endpoints	**SAPLE**	**SEATI**	**SEINF**	**TOTAIS**
endpoint convencional, estações de trabalho, desktop e notebook	-	1410	165	1575
plataformas móveis como Android ou IOS - tablets	31	-	-	31

Quantitativo necessário futuro de curto e médio prazo				
Tipos de endpoints	**SAPLE**	**SEATI**	**SEINF**	**TOTAIS**
endpoint convencional, estações de trabalho, desktop e notebook	-	245	-	245
plataformas móveis como Android ou IOS - tablets	-	70	-	70

Sendo assim, para atender a essa possibilidade de demandas futuras, sugere-se especificar na contratação um quantitativo de **400 licenças para endpoints do tipo desktop**, notebook e máquinas virtuais, e **119 licenças para endpoints do tipo plataformas móveis que só serão adquiridas quando estiverem demonstradas a necessidade de licenças adicionais**.

Portanto a relação de demanda e necessidade fica assim demonstrada:

RELAÇÃO DEMANDA X NECESSIDADE				
Id	**DEMANDA PREVISTA**	**QUANTITATIVO MÍNIMO DE LICENÇAS A SEREM ADQUIRIDAS ANUALMENTE**	**QUANTITATIVO MÁXIMO DE LICENÇAS A SEREM ADQUIRIDAS ANUALMENTE, SOB DEMANDA, APENAS EM CASO DE NECESSIDADE.**	**QUANTITATIVO TOTAL**
1	Aquisição de solução tecnológica de segurança, proteção antivírus e EndPoint Detection Response (EDR), incluindo licenças de uso, instalação, configuração, suporte técnico especializado e atualização da base de vacinas e software, pelo período contratado para endpoints do tipo **estações de trabalho,** desktops, notebooks e máquinas virtuais.	1575	400	1975
2	Aquisição de solução tecnológica de segurança, proteção antivírus e EndPoint Detection Response (EDR), incluindo licenças de uso, instalação, configuração, suporte técnico especializado e atualização da base de vacinas e software, pelo período contratado para endpoints do tipo **plataformas móveis** tais como smartphones e tablets, compatíveis com sistema operacional Android e IOS - Apple.	31	119	150
3	Operação assistida por 30 (trinta) dias corridos	1, apenas no primeiro ano.	0	1
4	Treinamento básico, capacitação e transferência de conhecimento para operação e gestão da solução de segurança contratada, com turma de 4 (quatro) alunos.	0	2	2

4.21. **DETALHAMENTO DA AQUISIÇÃO DE LICENÇAS**

4.21.1. A CLDF emitirá inicialmente, após a reunião inicial, a Ordem de Serviço de aquisição, de no mínimo, 1575 licenças anuais para endpoints do tipo estações de trabalho, e 31 licenças anuais para plataformas móveis.

4.21.2. Quantitativo do provisionamento das licenças flutuantes, que poderão ser solicitadas sob demanda (400 licenças do tipo estações de trabalho, desktops, notebooks e máquinas virtuais, e 119 licenças do tipo plataformas móveis para smartphones e tablets), se faz necessário para reserva no atendimento de futuras necessidades de licenças não previstas - são demandas provenientes de novas contratações

de pessoal, aquisição ou atualização de sistemas, e(ou) novas demandas para uso de decorrente de atividades legislativas parlamentares no âmbito da CLDF.

4.21.3. Durante a execução contratual, as licenças flutuantes adquiridas sob demanda serão solicitadas por meio de Ordem de Serviço própria, após prévia análise e verificação da necessidade da CLDF por licenças adicionais no curso da contratação, respeitando os quantitativos mínimos e máximos para os Id 1 e Id 2 - tabela RELAÇÃO DEMANDA X NECESSIDADE, que poderão serem solicitadas nesta contratação. A CLDF não é obrigada a adquirir nenhuma dessas licenças.

4.21.4. Com relação ao pagamento das licenças adicionais solicitadas durante a vigência do contrato, além das licenças iniciais (1575 por endpoint do tipo desktop e 31 por endpoint do tipo móvel), o faturamento será calculado proporcionalmente, em dias, ao tempo de utilização da licença, desde o momento da instalação efetiva até o término do contrato atual.

4.21.5. A CLDF não é obrigada a consumir o quantitativo de licenças flutuantes sob demanda contratadas, no entanto, reserva-se o direito de solicitar a aquisição dessas licenças "flutuantes", após prévia verificação da necessidade por licenças adicionais, respeitando-se o limite máximo de 400 licenças do tipo estações de trabalho, desktops, notebooks e máquinas virtuais, e de 119 licenças do tipo plataformas móveis para smartphones e tablets, durante a vigência da contratação.

4.21.6. Quanto ao pagamento das licenças, ele só será realizado após atesto do recebimento e a respectiva emissão do Termo de Recebimento Definitivo, pela Equipe de Fiscalização do Contrato. Apenas após a emissão do TRD, a CONTRATADA estará autorizada a emitir fatura indicando o quantitavo de licenças utilizadas pela CLDF, na ocasião, respeitando os limites de licenças que poderão serem consumidas sob demanda nesta contratação.

4.22. **RESULTADOS E BENEFÍCIOS ESPERADOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO**

4.22.1. CONSOLIDAÇÃO - GERENCIAMENTO E MONITORAMENTO POR MEIO DE UMA INTERFACE ÚNICA

A consolidação do gerenciamento e monitoramento de segurança por meio de uma interface única é um benefício esperado para a CLDF, pois simplifica e melhora a eficiência do gerenciamento de segurança, reduz a complexidade, minimiza a possibilidade de erros humanos e melhora a tomada de decisão. Além disso, uma interface única também pode melhorar a visibilidade e a compreensão da postura de segurança da CLDF, permitindo que os administradores monitorem mais efetivamente as ameaças, identifiquem vulnerabilidades e reduzam o risco de violações de dados e outras ameaças de segurança.

4.22.2. MELHORIA NA SEGURANÇA CONTRA ATAQUES CIBERNÉTICOS

A melhoria na segurança contra ataques cibernéticos é um benefício esperado de recursos de segurança como EDR, que podem detectar e responder a ameaças avançadas e desconhecidas que outras soluções de segurança podem não detectar. Esses recursos são capazes de analisar o comportamento do sistema em tempo real e identificar atividades maliciosas, isolando e remediando a ameaça antes que ela possa causar danos significativos. Ao melhorar a detecção e resposta a ameaças, os recursos de segurança podem ajudar a reduzir o tempo de exposição e minimizar os danos causados por um ataque cibernético, aumentando a segurança geral da CLDF.

4.22.3. GERENCIAMENTO PROATIVO E RACIONALIZADO DE RECURSOS

O benefício esperado do recurso de gerenciamento proativo e racionalizado de recursos é a melhoria da eficiência e redução de custos na gestão de ativos de TI da organização. Com esse recurso, é possível monitorar proativamente o uso dos recursos de TI, identificar gargalos e alocar recursos adequadamente. Isso pode ajudar a maximizar a eficiência da infraestrutura de TI e minimizar os custos associados, evitando a sobrecarga ou subutilização de recursos. Além disso, o gerenciamento proativo e racionalizado de recursos também pode ajudar a identificar e corrigir possíveis problemas antes que eles se tornem críticos, reduzindo o tempo de inatividade e melhorando a disponibilidade de serviços.

4.22.4. POSSIBILIDADE PARA IDENTIFICAÇÃO FORENSE

O benefício esperado do recurso de possibilidade para identificação forense é a capacidade de coletar e analisar dados para identificar a causa raiz de um incidente de segurança. Esse recurso permite a coleta e armazenamento de informações de eventos de segurança para uso em investigações forenses, auxiliando a equipe de segurança na identificação da origem e do escopo do incidente. Com a capacidade de identificar a causa raiz, a equipe de segurança pode tomar medidas preventivas para evitar futuros incidentes similares, aumentando a segurança geral da organização. Além disso, esse recurso pode ser usado para cumprir requisitos regulatórios e legais, como a manutenção de registros de auditoria e a notificação de violações de dados.

4.22.5. FACILIDADE DE MANUTENÇÃO E EVOLUÇÃO TECNOLÓGICA

O benefício esperado do recurso de facilidade de manutenção e evolução tecnológica é a melhoria da eficiência e redução de custos na manutenção e atualização das soluções de segurança da CLDF. Com esse recurso, é possível implementar atualizações e correções de maneira mais rápida e fácil, minimizando o impacto na operação da CLDF. Além disso, a facilidade de manutenção também pode ajudar a minimizar a necessidade de recursos especializados em segurança, permitindo que a equipe de TI da CLDF gerencie as soluções de segurança de maneira mais eficiente. Esse recurso também pode facilitar a evolução tecnológica, permitindo a implementação de novas tecnologias e recursos de segurança à medida que eles se tornam disponíveis, mantendo a CLDF atualizada e segura contra as ameaças cibernéticas em constante evolução.

4.22.6. ATUALIZAÇÃO TECNOLÓGICA DA FERRAMENTA DE PROTEÇÃO E SEGURANÇA DOS ATIVOS DIGITAIS DA CLDF

O benefício esperado do recurso de atualização tecnológica da ferramenta de proteção e segurança dos ativos digitais da CLDF é a melhoria da eficácia da proteção contra ameaças cibernéticas e a garantia da conformidade com as regulamentações de segurança. Com esse recurso, é possível manter as soluções de segurança atualizadas com as últimas tecnologias de detecção e prevenção de ameaças, garantindo que a organização esteja protegida contra as ameaças cibernéticas em constante evolução. Além disso, a atualização tecnológica também pode ajudar a garantir a conformidade com as regulamentações de segurança, que exigem que as organizações implementem medidas adequadas de segurança para proteger seus ativos digitais. Isso pode ajudar a minimizar os riscos legais e financeiros associados a violações de segurança e proteger a reputação da organização.

5. REQUISITOS DA CONTRATAÇÃO

ANEXO I – REQUISITOS DA CONTRATAÇÃO

6. RESPONSABILIDADES

6.1. São obrigações da **CONTRATANTE**:

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

6.1.2. 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.

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

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

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

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

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

6.1.8. 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.

6.2. São obrigações da **CONTRATADA**:

6.2.1. Indicar formalmente Preposto apto a representá-la junto à CONTRATANTE, que deverá responder pela fiel execução do contrato.

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

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

6.2.4. 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.

6.2.5. 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.

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

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

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

6.2.9. 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.

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

6.2.11. 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.

6.2.12. 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.

6.2.13. 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.

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

6.2.15. Entregar um checklist de verificação de todos os requisitos de arquitetura tecnológica, do item 1 ao item 8 listados no Anexo I deste TR, com a respectiva indicação da documentação e da página da documentação que contém a comprovação daquele requisito.

7. PROTEÇÃO DE DADOS (LGPD)

7.1. 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.

7.2. 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.

7.3. 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.

7.4. 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.

7.5. 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:

I - cumprimento de obrigação legal ou regulatória pelo controlador;

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

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

7.6. 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.

7.7. 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. MODELO DE EXECUÇÃO DO CONTRATO

8.1. ROTINAS DE EXECUÇÃO

8.1.1. As parcelas serão entregues nos seguintes prazos e condições:

Parcela	**Prazo de entrega**
FASE I Assinatura do Contrato.	D*
FASE II Entrega do Plano de Instalação e Configuração - até 10 (dez) dias corridos;	FI+ 10
FASE III Instalação, configuração e teste dos serviços - até 10 (dez) dias corridos;	FII+ 10
FASE IV Análise de conformidade e homologação dos serviços. a) Emissão de Relatório Técnico e comunicação à CONTRATADA – estimado 15 (quinze) dias corridos; b) Prazo para regularizar as desconformidades - 5 (cinco) dias corridos	FIII + 20
FASE V a) Emissão de Termo de Recebimento Definitivo e comunicação à CONTRATADA – estimado 5(cinco) dias corridos - instalação e configuração da solução tecnológica de segurança, proteção antivírus e EndPoint Detection Response (EDR), incluindo atualização da base de vacinas e software, treinamento e suporte técnico especializado pelo período contratado.	FIV + 5
FASE VI a) Emissão de Termo de Recebimento Definitivo e comunicação à CONTRATADA – estimado 5(cinco) dias corridos - Operação assistida	FV + 30
FASE VII a)Emissão de Termo de Recebimento Definitivo e comunicação à CONTRATADA – 5(cinco) dias corridos - Capacitação, treinamento e transferência de conhecimento.	FV + 365
FASE VIII a) monitoramento da solução, prestação de suporte e atualização das licenças durante todo o período do contrato pela CONTRATADA; b)Encerramento da Contratação: Remoção e desinstalação dos softwares instalados - prazo 30 (trinta) dias corridos a partir do recebimento da Ordem de Serviço própria.	a) FV + 365 b) Ordem de Serviço de Encerramento+30

Observações:

- D* = Data da assinatura do contrato;
- A FASE II poderá ser abreviada caso a entrega ocorra antes do prazo estipulado;
- A FASE III poderá ser abreviada caso a instalação, configuração e os testes de stress ocorram antes do prazo estipulado;
- A FASE IV poderá ser abreviada caso não ocorram desconformidades.
- A FASE VII poderá ocorrer em qualquer momento durante a vigência do contrato à critério da contratante.

- F = fase

8.1.1.1. Caso não seja possível a entrega na data assinalada, a empresa deverá comunicar as razões respectivas com pelo menos 5 dias de antecedência para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior;

8.1.1.2. Os bens deverão ser entregues na sede da Câmara Legislativa do Distrito Federal, no endereço Praça Municipal, Quadra 2, Lote 5, Zona Cívico-Administrativa, Brasília – DF, CEP: 70.094-902;

8.1.1.3. O horário de recebimento do objeto contratual será de 08h as 18h, em dias de expediente normal da Casa apenas;

8.1.1.4. 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.

8.1.1.5. Para o agendamento da instalação, a licitante vencedora deverá informar a CLDF a data de instalação, com no mínimo de 2 (dois) dias úteis de antecedência.

8.1.1.6. Ficará a critério da CONTRATANTE prorrogar ou não o prazo estipulado, devendo a CONTRATADA protocolar carta de solicitação de prorrogação de prazo, em papel timbrado da empresa, com assinatura e data, explicando as causas do atraso.

8.1.1.7. Ficará a critério da CONTRATANTE prorrogar ou não o prazo estipulado, porém para que isso ocorra, a CONTRATADA deverá protocolar na CONTRATANTE carta de solicitação de prorrogação de prazo, em papel timbrado da empresa, com assinatura e data, explicando as causas do atraso. A CONTRATANTE terá até 3 (três) dias úteis para responder.

8.1.1.8. Na existência de desconformidade e em caso de recusa, deverá a CONTRATADA retirar todas licenças, softwares e serviços, no prazo de 10 (dez) dias corridos, a contar da comunicação da CONTRATANTE, sem prejuízo da rescisão contratual e demais penalidades cabíveis.

8.1.2. **DOCUMENTAÇÃO MÍNIMA EXIGIDA**

FASE V - Licenças, Gerência, Suporte e Atualização O pagamento será realizado depois do aceite da Equipe de Fiscalização do Contrato, mediante envio, pela CONTRATADA, da nota fiscal após a emissão do Termo de Recebimento Definitivo, desde que não haja pendências de responsabilidade da CONTRATADA e 100% das licenças, softwares e serviços tenham sido instalados, configurados e testados.

FASE VI - Operação Assistida O pagamento será realizado depois do aceite da Equipe de Fiscalização do Contrato, mediante envio, pela CONTRATADA, da nota fiscal após a emissão do Termo de Recebimento Definitivo, indicando a conclusão da Operação Assistida.

FASE VII - Capacitação, treinamento e transferência de conhecimento. O pagamento será realizado depois do aceite da Equipe de Fiscalização do Contrato, mediante envio, pela CONTRATADA, da nota fiscal após a emissão do Termo de Recebimento Definitivo, indicando a conclusão do treinamento e transferência de conhecimento.

8.2. **QUANTIFICAÇÃO OU ESTIMATIVA PRÉVIA DA QUANTIDADE DE BENS A SEREM FORNECIDOS, PARA COMPARAÇÃO E CONTROLE**

8.2.1. Cada Ordem de Fornecimento de Bens conterá a quantidade a ser fornecida, incluindo a sua localização e o prazo, conforme definições deste TR.

8.3. **MECANISMOS FORMAIS DE COMUNICAÇÃO**

8.3.1. São definidos como mecanismos formais de Comunicação, entre a CONTRATANTE e a CONTRATADA, os seguintes:

Ordem de Fornecimento de Bens;

8.3.1.1. Ordem de Serviço;

8.3.1.2. Ata de Reunião;

8.3.1.3. Ofício;

8.3.1.4. Sistema de abertura de chamados;

8.3.1.5. E-mails e Cartas;

8.3.1.6. Whatsapp e/ou Telegram;

8.4. **PAGAMENTO**

8.4.1. Os critérios de medição e pagamento, que será efetuado em função dos resultados obtidos, serão tratados no Modelo de Gestão do Contrato, constante deste Termo de Referência.

8.5. **MANUTENÇÃO DE SIGILO E NORMAS DE SEGURANÇA**

8.5.1. A CONTRATADA deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pela CONTRATANTE a tais documentos.

8.5.2. O Termo de Compromisso e Manutenção de Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na CLDF, a ser assinado pelo representante legal da CONTRATADA, e Termo de Ciência, a ser assinado por todos os empregados da CONTRATADA diretamente envolvidos na contratação, encontram-se nos ANEXOS II e III deste TR.

9. MODELO DE GESTÃO DO CONTRATO

9.1. A gestão do contrato e os papeis de cada integrante serão realizados conforme 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 federal nº 14.133, de 1º de abril de 2021.

9.2. 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.

9.3. 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.

9.4. 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.

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

9.6. 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.

9.7. A reunião inicial do início da execução ocorrerá em até 7 dias úteis da assinatura do Contrato, podendo ser prorrogada a critério da CONTRATANTE.

9.8. A pauta desta reunião observará, pelo menos:

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

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

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

9.8.4. 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;

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

9.9. 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:

9.9.1. 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.

9.9.2. 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.

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

9.9.4. 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.

9.9.5. 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.

9.9.6. 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.

9.9.7. 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.

9.9.8. 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.

9.9.9. 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.

9.9.10. 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.

9.9.11. 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.

9.9.12. 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.

9.9.13. 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.

9.9.14. 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.

9.10. **INSTALAÇÃO - GERAL**

9.10.1. A instalação será realizada por técnicos designados pela licitante vencedora e poderá ser acompanhada pela equipe técnica designada pela CLDF.

9.10.2. A CONTRATADA deverá finalizar a instalação no prazo máximo estabelecido no cronograma de execução.

9.10.3. A CONTRATADA deverá remover, após a instalação, qualquer resíduo oriundo dessa atividade.

9.10.4. É de responsabilidade da CONTRATADA, a correção das falhas decorrentes de erros durante as atividades de instalação, sejam operacionais ou por problemas de mau funcionamento dos softwares, dispositivos e/ou equipamentos fornecidos, responsabilizando-se por todos os custos envolvidos na correção de falhas que impeçam a instalação dos softwares, dispositivos e/ou equipamentos fornecidos.

9.10.5. Eventuais despesas de custeio com deslocamento de técnicos da CONTRATADA ao local de instalação, bem como todas as despesas de transporte, diárias, seguro ou quaisquer outros custos envolvidos ficam a cargo exclusivo da licitante vencedora.

9.10.6. Deverá ser fornecida documentação completa da instalação realizada.

9.10.7. A CONTRATANTE poderá fazer anotações na documentação entregue e repassar à CONTRATADA para que sejam providenciadas as eventuais correções necessárias, sem prejudicar o cronograma de instalação e sem gerar ônus à CONTRATANTE.

9.10.8. A documentação de instalação não isenta a CONTRATADA das responsabilidades sobre o pleno funcionamento dos equipamentos, softwares e serviços, ao longo de todo o período de garantia e contratação contratado.

9.10.9. A falta de instalação de quaisquer equipamentos, softwares e serviços constitui-se em motivo de suspensão dos compromissos financeiros. Permanecendo a situação por mais de 30 (trinta) dias corridos, o contrato poderá ser rescindido.

9.10.10. Ficará a critério da CONTRATANTE prorrogar ou não o prazo estipulado, devendo a CONTRATADA protocolar carta de solicitação de prorrogação de prazo, em papel timbrado da empresa, com assinatura e data, explicando as causas do atraso.

9.10.11. O pagamento das licenças só ocorrerá após a efetiva instalação e configuração pela CONTRATADA.

9.11. **INSTALAÇÃO – ESPECÍFICOS DA SOLUÇÃO DE TI**

9.11.1. Executar o previsto e acertado no Plano de Instalação e Configuração, fornecido na Fase de Entrega (Fase II), do Cronograma de Execução.

9.11.2. A execução não precisa ser necessariamente contígua, mas deverá ocorrer dentro do prazo estipulado na Fase II, do Cronograma de Execução.

9.11.3. Durante a Fase de Instalação (Fase III), a CONTRATADA deverá atualizar, caso haja patch de atualização mais atual, os agentes instalados nos endpoints bem como a console de administração. Garantindo a solução de antivírus e EDR mais atualizada possível.

9.11.4. Ao término, a CONTRATADA deverá fornecer documentação (arquivo do tipo PDF) dos procedimentos de instalação/atualização executados.

9.11.5. ANÁLISE DE CONFORMIDADE

9.11.6. Descrição do Requisito

9.11.7. A CONTRATANTE realizará a análise de conformidade dos serviços fornecidos, observando as especificações técnicas e demais aspectos do Edital, e emitirá o relatório com o resultado da análise.

9.11.8. Na existência de desconformidade, a CONTRATANTE emitirá relatório técnico relacionando os itens que não atenderem as exigências da especificação técnica e demais aspectos do Edital.

9.11.9. Na existência de desconformidade, a CONTRATANTE comunicará, dentro do prazo estabelecido no Cronograma de Execução, o resultado da análise de conformidade à CONTRATADA por meio de carta de advertência;

9.11.10. Na existência de desconformidade, a CONTRATADA, após comunicação da CONTRATANTE, deverá regularizar as desconformidades relatadas no prazo estabelecido no Cronograma de Execução.

9.11.11. Ficará a critério da CONTRATANTE prorrogar ou não o prazo estipulado, porém para que isso ocorra, a CONTRATADA deverá protocolar na CLDF carta de solicitação de prorrogação de prazo, em papel timbrado da empresa, com assinatura e data, explicando as causas do atraso. A CONTRATANTE terá até 3 (três) dias úteis para responder

9.11.12. Na existência de desconformidade e em caso de recusa, deverá a CONTRATADA retirar todos os softwares e serviços, no prazo de 10 (dez) dias corridos, a contar da comunicação da CONTRATANTE, sem prejuízo da rescisão contratual e demais penalidades cabíveis.

9.11.13. Caso os softwares e serviços entregues, instalados e configurados atendam às exigências da CONTRATANTE, conforme especificação técnica e demais aspectos do Edital, a CONTRATANTE emitirá o relatório com o resultado da análise de conformidade e comunicará, dentro do prazo previsto no Cronograma de Execução, o resultado à CONTRATADA.

9.11.14. O resultado sem ressalvas dos testes constitui condição para a emissão do Termo de Recebimento Definitivo.

9.12. **CRITÉRIOS DE ACEITAÇÃO**

9.12.1. A avaliação da qualidade dos produtos entregues, para fins de aceitação, consiste na verificação dos critérios relacionados a seguir:

9.12.2. Todos os equipamentos fornecidos deverão ser novos (incluindo todas as peças e componentes presentes nos produtos), de primeiro uso (sem sinais de utilização anterior), não recondicionados e em fase de comercialização normal através dos canais de venda do fabricante no Brasil (não serão aceitos produtos end-of-life);

9.12.3. Todos os componentes do(s) equipamento(s) e respectivas funcionalidades deverão ser compatíveis entre si, sem a utilização de adaptadores, frisagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos não previstos nas especificações técnicas ou, ainda, com emprego de materiais inadequados ou que visem adaptar forçadamente o produto ou suas partes que sejam fisicamente ou logicamente incompatíveis;

9.12.4. Todos os componentes internos do(s) equipamento(s) deverá(ão) estar instalado(s) de forma organizada e livres de pressões ocasionados por outros componentes ou cabos, que possam causar desconexões, instabilidade, ou funcionamento inadequado;

9.12.5. O número de série de cada equipamento deve ser obrigatório e único, afixado em local visível, na parte externa do gabinete e na embalagem que o contém. Esse número deverá ser identificado pelo fabricante, como válido para o produto entregue e para as condições do mercado brasileiro no que se refere à garantia e assistência técnica no Brasil;

9.12.6. Serão recusados os produtos que possuam componentes ou acessórios com sinais claros de oxidação, danos físicos, sujeira, riscos ou outro sinal de desgaste, mesmo sendo o componente ou acessório considerado como novos pelo fornecedor dos produtos;

9.12.7. Os produtos, considerando a marca e modelo apresentados na licitação, não poderão estar fora de linha comercial, considerando a data de LICITAÇÃO (abertura das propostas). Os produtos devem ser fornecidos completos e prontos para a utilização, com todos os acessórios, componentes, cabos, etc;

9.12.8. Todas as licenças, referentes aos softwares e drivers solicitados, devem estar registrados para utilização da CONTRATANTE, em modo definitivo (licenças perpétuas), legalizado, não sendo admitidas versões "shareware" ou "trial". O modelo do produto ofertado pelo licitante deverá estar em fase de produção pelo fabricante (no Brasil ou no exterior), sem previsão de encerramento de produção, até a data de entrega da proposta;

9.12.9. A CONTRATANTE poderá optar por avaliar a qualidade de todos os equipamentos fornecidos ou uma amostra dos equipamentos, atentando para a inclusão nos autos do processo administrativo de todos os documentos que evidenciem a realização dos testes de aceitação em cada equipamento selecionado, para posterior rastreabilidade;

9.12.10. Só haverá o recebimento definitivo, após a análise da qualidade dos bens e/ou serviços, em face da aplicação dos critérios de aceitação, resguardando-se à CONTRATANTE o direito de não receber o objeto cuja qualidade seja comprovadamente baixa ou em desacordo com as especificações definidas neste Termo de Referência – situação em que poderão ser aplicadas à CONTRATADA as penalidades previstas em lei, neste Termo de Referência e no contrato. Quando for o caso, a empresa será convocada a refazer todos os serviços rejeitados, sem custo adicional.

9.13. **PROCEDIMENTOS DE TESTE E INSPEÇÃO PARA AVALIAÇÃO DO CUMPRIMENTO DAS EXIGÊNCIAS DE CARÁTER TÉCNICO E DA CONFORMIDADE DO MATERIAL**

9.13.1. Serão adotados como procedimentos de teste e inspeção, para fins de elaboração dos Termos de Recebimento Provisório e Definitivo:

9.13.2. Constação de que 100% das licenças demandadas, foram instaladas, configuradas e testadas, com toda a documentação entregue.

9.13.3. Inexistência de desconformidades.

9.13.4. Verificar a capacidade do antivírus de identificar e detectar diferentes tipos de ameaças, como vírus, malware, spyware, ransomware, entre outros.

9.13.5. Avaliar o impacto do antivírus no desempenho do sistema durante a execução de tarefas comuns, como abrir aplicativos, navegar na internet, copiar/arquivar arquivos, etc.

9.13.6. Verificar a eficácia do antivírus em remover ou quarentenar com sucesso as ameaças detectadas.

9.13.7. Avaliar a capacidade do antivírus de obter atualizações de definições de vírus regularmente e aplicá-las com sucesso para manter a proteção atualizada.

9.13.8. Verificar se as licenças são compatíveis com as especificações de sistemas operacionais listados no item 5.1.

9.13.9. Verificar a capacidade do antivírus de monitorar e proteger o sistema em tempo real, detectando e bloqueando ameaças à medida que ocorrem.

9.13.10. Avaliar a capacidade do antivírus de detectar comportamentos suspeitos e atividades maliciosas, mesmo sem ter definições específicas de vírus.

9.13.11. Verificar se o antivírus é capaz de remover completamente as ameaças detectadas, incluindo arquivos infectados, registros do sistema e outras alterações feitas pelas ameaças.

9.14. **NÍVEIS MÍNIMOS DE SERVIÇO EXIGIDOS**

9.14.1. 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:

IAE – INDICADOR DE ATRASO NO FORNECIMENTO DO EQUIPAMENTO	
Tópico	**Descrição**
Finalidade	Medir o tempo de atraso na entrega dos produtos e serviços constantes na Ordem de Fornecimento de Bens - OFB.
Meta a cumprir	**IAE < = 0** A meta definida visa garantir a entrega dos produtos e serviços constantes nas OFB dentro do prazo previsto.
Instrumento de medição	OFB, Termo de Recebimento Provisório (TRP)
Forma de acompanhamento	A avaliação será feita conforme linha de base do cronograma registrada na OFB. Será subtraída a data de entrega dos produtos da OFB (desde que o Fiscal Técnico reconheça aquela data, com registro em Termo de Recebimento Provisório) pela data de início da execução da OFB.
Periodicidade	Para cada OFB encerrada e com Termo de Recebimento Definitivo.
Mecanismo de Cálculo (métrica)	**IAE = TEX – TEST** Onde: **IAE** – Indicador de Atraso de Entrega da OFB; **TEX** – Tempo de Execução – corresponde ao período de execução da OFB, da sua data de início até a data de entrega dos produtos da OFB; **TEST** – Tempo Estimado para a execução da OFB – constante na OFB, conforme estipulado no Termo de Referência; A data de início será aquela constante na OFB. Caso não esteja explícita, será o primeiro dia útil após a emissão da OFB; A data de entrega da OFB deverá ser aquela reconhecida pelo Fiscal Técnico, conforme critérios constantes neste Termo de Referência. Para os casos em que o Fiscal Técnico rejeita a entrega, o prazo de execução da OFB continua a correr, findando-se apenas quanto a CONTRATADA entrega os produtos da OFB e haja aceitação por parte do Fiscal Técnico.
Observações	Obs1: Serão utilizados dias corridos na medição. Obs2: Os dias com expediente parcial na CLDF serão considerados como dias corridos no cômputo do indicador.
Início de vigência	Primeiro dia útil após a emissão da OFB.
Faixas de ajuste no pagamento (glosa) e sanções	Para valores do indicador **IAE**: Menor ou igual a 0: pagamento integral da OFB; De 1 a 60: aplicar-se-á glosa de 0,1% por dia de atraso sobre o valor da OFB ou fração em atraso; Acima de 60: aplicar-se-á glosa de 6% bem como multa de 1% sobre a fração em atraso.

9.15. **VALORES E PROCEDIMENTOS PARA RETENÇÃO OU GLOSA DO PAGAMENTO**

9.15.1. Nos casos de inadimplemento na execução do objeto, as ocorrências serão registradas pela CONTRATANTE, conforme a tabela abaixo:

Id	**Ocorrência**	**Glosa / Sanção**
1	Não atender ao indicador de nível de serviço IAE (Indicador de Atraso de Entrega)	Glosa de 0,1% sobre o valor da OFB ou fração em atraso para valores do indicador IAE de 1 a 60.
		Glosa de 7 % sobre o valor da OFB ou fração em atraso para valores do indicador IAE maiores de 60.

9.16. **SANÇÕES ADMINISTRATIVAS**

9.16.1. Comete infração administrativa nos termos da Lei nº 14.133, de 2021, a LICITANTE ou CONTRATADA que:

I - der causa à inexecução parcial do contrato;

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

III - der causa à inexecução total do contrato;

IV - deixar de entregar a documentação exigida para o certame;

V - não mantiver a proposta, salvo em decorrência de fato superveniente devidamente justificado;

VI - não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

VII - ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

VIII - apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;

IX - fraudar a licitação ou praticar ato fraudulento na execução do contrato;

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

XI - praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

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

9.16.2. Pela inexecução total ou parcial do objeto deste contrato, a Administração pode aplicar à CONTRATADA as seguintes sanções:

I - advertência;

II - multa;

III - impedimento de licitar e contratar;

IV - declaração de inidoneidade para licitar ou contratar.

9.16.3. Na aplicação das sanções serão considerados:

I - a natureza e a gravidade da infração cometida;

II - as peculiaridades do caso concreto;

III - as circunstâncias agravantes ou atenuantes;

IV - os danos que dela provierem para a Administração Pública;

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

9.16.4. A ADVERTÊNCIA será aplicada exclusivamente quando a CONTRATADA der causa à inexecução parcial do contrato e quando não se justificar a imposição de penalidade mais grave.

9.16.5. A MULTA será calculada na forma do edital ou do contrato, não podendo ser inferior a 0,5% (cinco décimos por cento), nem superior a 30% (trinta por cento) do valor do contrato licitado ou celebrado com contratação direta e será aplicada ao responsável por qualquer das infrações administrativas previstas no subitem 8.14.1 acima (infrações previstas no art. 155 da Lei nº 14.133, de 2021).

9.16.6. O IMPEDIMENTO DE LICITAR E CONTRATAR será aplicado ao responsável pelas infrações administrativas previstas nos incisos II, III, IV, V, VI e VII do subitem 8.14.1 acima, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos (infrações previstas no art. 155 da Lei 14.133, de 2021).

9.16.7. A DECLARAÇÃO DE INIDONEIDADE PARA LICITAR OU CONTRATAR será aplicada ao responsável pelas infrações administrativas previstas incisos VIII, IX, X, XI e XII do subitem 8.14.1 acima, bem como pelas infrações administrativas previstas nos incisos II, III, IV, V, VI e VII do referido subitem que justifiquem a imposição de penalidade mais grave que a sanção referida no art. 156 da Lei nº 14.133/21, e impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos (infrações previstas no art. 155 da Lei 14.133, de 2021).

9.16.8. A DECLARAÇÃO DE INIDONEIDADE PARA LICITAR OU CONTRATAR será precedida de análise jurídica e observará as seguintes regras:

I - quando aplicada por órgão do Poder Executivo, será de competência exclusiva de ministro de Estado, de secretário estadual ou de secretário municipal e, quando aplicada por autarquia ou fundação, será de competência exclusiva da autoridade máxima da entidade;

II - quando aplicada por órgãos dos Poderes Legislativo e Judiciário, pelo Ministério Público e pela Defensoria Pública no desempenho da função administrativa, será de competência exclusiva de autoridade de nível hierárquico equivalente às autoridades referidas no inciso I acima, na forma de regulamento.

9.16.9. As sanções previstas nos incisos III e IV do subitem 8.14.2 poderão ser aplicadas cumulativamente com a prevista no inciso II do mesmo subitem.

9.16.10. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor de pagamento eventualmente devido pela Administração à CONTRATADA, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.

9.16.11. A aplicação das sanções previstas no caput deste artigo não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Administração Pública.

9.16.12. As infrações previstas nos incisos I, II, III, IV, VII, IX e X do primeiro subitem desta cláusula têm as seguintes definições, nos termos do Ato da Mesa Diretora nº 70, de 2023 da CLDF (infrações administrativas aplicadas a licitantes ou contratadas):

I - A inexecução parcial do contrato prevista no inciso I do primeiro subitem desta cláusula compreende o atraso no início da execução contratual ou na entrega do bem e pelas seguintes ocorrências, além de outras estabelecidas no edital:

a) serviço iniciado em desacordo com o contrato;

b) descumprimento de prazo de entrega do serviço contratado sem justificativa ou consentimento da administração;

c) utilização de materiais em desacordo com o contrato sem justificativa ou consentimento da administração;

d) transferência a terceiros de parte da execução dos serviços contratados sem previsão contratual ou consentimento da administração;

e) entrega de item em desacordo com as especificações;

f) entrega de item em quantidade inferior àquela adjudicada.

- A entrega do objeto fora do prazo previsto, até o limite de 30 dias corridos de atraso, sujeitará a CONTRATADA à sanção calculada na faixa entre 0,5% e 2,5% sobre o valor total da contratação ou da parcela não entregue, conforme o caso, considerando-se a gravidade do caso e o tempo de atraso.
- A entrega do objeto em data posterior a 30 dias corridos de atraso, sujeitará a CONTRATADA à sanção calculada na faixa entre 2,5% a 5% sobre o valor total da contratação ou da parcela não entregue, considerando-se a gravidade do caso e o tempo de atraso.
- A CLDF poderá admitir tolerância de até 5 dias de atraso na entrega do bem, sem a aplicação da penalidade de multa.

II - Considera-se a conduta do inciso II do primeiro subitem desta cláusula como sendo o inadimplemento grave ou inescusável de obrigação assumida pela CONTRATADA.

III - Considera-se inexecução total do contrato prevista no inciso III do primeiro subitem desta cláusula a recusa da prestação do serviço contratado ou a recusa em entregar o bem adjudicado e ainda:

a) entrega parcial do serviço que, por suas características, não possa ser concluído por meio de nova contratação;

b) a entrega parcial de item que, por sua característica, somente tenha aplicação se entregue por completo.

IV - Constituem comportamentos que serão enquadrados no inciso IV do primeiro subitem desta cláusula, sem prejuízo de outros que venham a ser verificados no decorrer da licitação ou da execução contratual, ressalvadas exigências meramente formais ou falhas sanáveis:

a) entregar documentação em manifesta desconformidade com as exigências do instrumento convocatório;

b) fazer entrega parcial de documentação exigida no instrumento convocatório;

c) deixar de entregar documentação complementar exigida pelo Agente de contratação, necessária para a comprovação de veracidade e/ou autenticidade de documentação exigida no edital de licitação.

V - Considera-se a conduta do inciso VII primeiro subitem desta cláusula como sendo o atraso que inviabilize o cumprimento das obrigações e importe em consequências graves para a Administração, observando-se o seguinte:

a) a conduta de inexecução parcial: entrega do objeto fora do prazo previsto, até o limite de 30 dias corridos, sujeitará a CONTRATADA à sanção calculada na faixa entre 0,5% e 5% sobre o valor total da contratação ou da parcela não entregue, conforme o caso, considerando-se a gravidade do caso e o tempo de atraso;

b) a conduta de inexecução total: será caracterizada pela entrega além do prazo limite de 30 dias corridas, bem como de outras assim expressamente previstas no termo de referência ou projeto básico, sujeitando-se a CONTRATADA à sanção calculada na faixa entre 5% a 10% sobre o valor total da contratação, considerando-se a gravidade do caso e o tempo de atraso, facultando-se à Administração aceitar ou não o objeto em atraso;

c) além dos percentuais previstos neste inciso, serão observadas outras hipóteses de penalidade e respectivos percentuais definidos no termo de referência ou projeto básico, de acordo com o objeto CONTRATADO.

VI - Considera-se a conduta do inciso IX do primeiro subitem desta cláusula como sendo a prática de qualquer ato destinado à obtenção de vantagem ilícita ou que induza ou mantenha em erro agentes públicos da Câmara Legislativa do Distrito Federal, com exceção da conduta disposta no inciso VIII do mesmo subitem.

VII - Considera-se a conduta do inciso X do primeiro subitem desta cláusula como sendo a prática de atos direcionados a prejudicar o bom andamento do certame ou do contrato, sem prejuízo de outras que venham a ser verificadas no decorrer da licitação ou da execução contratual.

9.16.13. Não será admitido pedido de prorrogação do prazo de entrega de bem ou serviço:

I - Eventuais justificativas para o atraso incorrido pela CONTRATADA apenas serão analisadas após a efetiva entrega do bem ou serviço e durante a fase destinada à defesa prévia.

II - Os emitentes das garantias contratuais serão notificados pela CLDF quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais que ensejem a rescisão contratual ou a aplicação de penalidade de multa em valor superior a 50% (cinquenta por cento) do valor de alçada para ajuizamento de ações de cobrança de créditos tributários e não tributários.

9.16.14. As sanções previstas no caput do primeiro subitem desta cláusula deste instrumento serão aplicadas de acordo com as disposições seguintes:

I - A sanção de advertência, prevista no inciso I do primeiro subitem desta cláusula será aplicada exclusivamente pela infração administrativa de inexecução parcial correspondente a, dentre outras:

a) ausência de habilitação fiscal, trabalhista;

b) não providenciar reposição de pessoal;

c) outras definidas no ETP ou TR como hipóteses da aplicação da sanção de advertência.

II - As penalidades de multa a serem aplicadas por descumprimento de obrigações assumidas por ata de registro de preços deverá ter como base a parte inadimplida.

III - A sanção de impedimento de contratar, prevista no inciso III do caput do primeiro subitem desta cláusula será aplicada ao responsável pelas infrações administrativas previstas nos incisos II, III, IV, V, VI e VII do caput do primeiro subitem desta cláusula, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar ou contratar no âmbito da Administração Pública do Distrito Federal, pelo prazo máximo de 3 (três) anos.

IV - A sanção de declaração de inidoneidade prevista no inciso IV do caput do primeiro subitem desta cláusula será aplicada ao responsável pelas infrações administrativas previstas nos incisos VIII, IX, X, XI e XII do caput do primeiro subitem desta cláusula, bem como pelas infrações administrativas previstas nos incisos II, III, IV, V, VI e VII do caput do referido subitem que justifiquem a imposição de penalidade mais grave que a sanção referida no inciso III deste subitem, e impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos.

9.16.15. As infrações definidas no do primeiro subitem desta cláusula serão sancionadas de acordo com as disposições seguintes em conjunto com os critérios estabelecidos no segundo subitem desta cláusula, sem prejuízo da aplicação de outras disposições cominadas no edital ou contrato, quando a licitante ou a CONTRATADA:

I - Der causa à inexecução parcial do contrato: Penalidade de advertência;

II - Der causa à inexecução parcial do contrato que cause grave dano à Câmara Legislativa do Distrito Federal: Penalidade de impedimento de licitar e contratar com o Distrito Federal pelo período de 3 (três) anos e multa de 10 (dez) a 20 (vinte) por cento do valor do contrato/nota de empenho;

III - Der causa à inexecução total do contrato: Penalidade de impedimento de licitar e contratar com Distrito Federal pelo período de 2 (dois) anos e multa de 5 (cinco) a 10 (dez) por cento do valor do contrato/nota de empenho;

IV - Deixar de entregar a documentação exigida para o certame, ressalvadas meras falhas formais e passíveis de saneamento: Penalidade de impedimento de licitar e contratar com o Distrito Federal pelo período de 6 (seis) meses;

V - Não mantiver a proposta, salvo em decorrência de fato superveniente devidamente justificado: Penalidade de impedimento de licitar e contratar com o Distrito Federal período de 6 (seis) meses;

VI - Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta: Penalidade de impedimento de licitar e contratar com o Distrito Federal pelo período de 4 (quatro) meses e multa de 5 (cinco) a 10 (dez) por cento do valor do contrato/nota de empenho;

VII - Ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado: Penalidade de impedimento de licitar e contratar com o Distrito Federal pelo período de 4 (quatro) meses e multa de 1 (um) a 5 (cinco) por cento do valor do contrato/nota de empenho;

VIII - Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato: Penalidade de declaração de inidoneidade pelo período de 5 (cinco) anos e multa de 20 (vinte) a 30 (trinta) por cento do valor estimado da contratação ou contrato;

IX - Fraudar a licitação ou praticar ato fraudulento na execução do contrato: Penalidade de declaração de inidoneidade pelo período de 5 (cinco) anos e multa de 20 (vinte) a 30 (trinta) por cento do valor estimado da contratação ou contrato;

X - Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza: Penalidade de declaração de inidoneidade pelo período de 3 (três) anos e multa de 10 (dez) a 20 (vinte) por cento do valor estimado da contratação ou contrato;

XI - Praticar atos ilícitos com vistas a frustrar os objetivos da licitação: Penalidade de declaração de inidoneidade pelo período de 5 (cinco) anos e multa de 20 (vinte) a 30 (trinta) por cento do valor estimado da contratação.

9.17. **CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO**

9.17.1. **RECEBIMENTO DO OBJETO**

9.17.1.1. Os bens serão recebidos provisoriamente no ato da entrega, juntamente com a nota fiscal ou instrumento de cobrança equivalente e com o restante da documentação exigida no Edital e no Contrato, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta;

9.17.1.2. Os bens poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 7 dias úteis, a contar da notificação da CONTRATADA, às suas custas, sem prejuízo da aplicação das penalidades;

9.17.1.3. O recebimento definitivo ocorrerá no prazo de 7 dias úteis, a contar do recebimento da nota fiscal ou instrumento de cobrança equivalente pela Administração, após a verificação da qualidade e quantidade do material e consequente aceitação;

9.17.1.4. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais;

9.17.1.5. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal no que concerne à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento;

9.17.1.6. O prazo para a solução, pela CONTRATADA, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo;

9.17.1.7. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

9.18. **FORMA DE PAGAMENTO**

9.18.1. Os pagamentos serão efetuados pela CLDF, em moeda corrente nacional, mediante Ordem Bancária, de acordo com o Cronograma Físico-Financeiro, se existir, e no valor correspondente ao somatório dos serviços efetivamente executados, segundo as medições efetuadas pela fiscalização. No caso de medição relativa à última fase, o pagamento somente será efetuado após o Recebimento Provisório.

9.18.2. 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:

9.18.2.1. o prazo de validade;

9.18.2.2. a data da emissão;

9.18.2.3. os dados do contrato e do órgão CLDF;

9.18.2.4. o período de prestação dos serviços;

9.18.2.5. o valor a pagar; e

9.18.2.6. eventual destaque do valor de retenções tributárias cabíveis.

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

9.18.3.1. 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;

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

9.18.3.3. 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.

9.18.4. 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.

9.18.5. 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.

9.18.6. 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.

9.18.7. 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.

9.19. **INDICAÇÃO ESTRUTURA DA COMISSÃO DE FISCALIZAÇÃO DO CONTRATO**

9.19.1. A fiscalização do contrato, objeto deste Termo de Referência, será realizada pelo(a):

9.19.1.1. Comissão de Fiscalização, constituída pelo Gestor do contrato e os fiscais Técnico, Administrativo e Requisitante, incluindo seus substitutos.

10. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

ITEM	ESPECIFICAÇÃO	MÉTRICA OU UNIDADE DE MEDIDA	QUANT.	VALOR UNITÁRIO	VALOR TOTAL
1	Aquisição de solução tecnológica de segurança, proteção antivírus e EndPoint Detection Response (EDR), incluindo licenças de uso, instalação, configuração, suporte técnico especializado e atualização da base de vacinas e software, pelo período contratado para endpoints do tipo **estações de trabalho,** desktops, notebooks e máquinas virtuais.	licenças	1975	R$ 264,53	R$ 522.446,75
2	Aquisição de solução tecnológica de segurança, proteção antivírus e EndPoint Detection Response (EDR), incluindo licenças de uso, instalação, configuração, suporte técnico especializado e atualização da base de vacinas e software, pelo período contratado para endpoints do tipo **plataformas móveis** tais como smartphones e tablets, compatíveis com sistema operacional Android e IOS - Apple.	licenças	150	R$ 416,0	R$ 62.400,00
3	Operação assistida por 30 (trinta) dias corridos.	unidade	1	R$ 35.000,0	R$ 35.000,0
4	Treinamento básico, capacitação e transferência de conhecimento para operação e gestão da solução de segurança contratada, com turma de 4 (quatro) alunos.	unidade	2	R$ 19.000,00	R$ 38.000,00
				TOTAL	**R$ 657.846,75**

11. ADEQUAÇÃO ORÇAMENTÁRIA

11.1. DOTAÇÃO ORÇAMENTÁRIA

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

11.1.2. Programa de Trabalho: 01.126.8204.1471 - Modernização de Sistemas de Informação.

11.1.3. Elemento de Despesa: 44.90.52 - Equipamentos e Material Permanente.

11.2. CRONOGRAMA FÍSICO FINANCEIRO

Eventos	Prazo Estimado	Valor
Recebimento provisório após instalação e configuração da solução tecnológica de segurança, proteção antivírus e EndPoint Detection Response (EDR), incluindo atualização da base de vacinas e software, suporte técnico especializado pelo período contratado.	20 dias após a emissão da Ordem de Fornecimento de Bens -OFB	R$ 0,00
Recebimento definitivo após instalação e configuração da solução tecnológica de segurança, proteção antivírus e EndPoint Detection Response (EDR), incluindo atualização da base de vacinas e software, suporte técnico especializado pelo período contratado.	20 dias após a emissão da Ordem de Fornecimento de Bens -OFB	R$ 584.846,75
Recebimento definitivo da operação assistida	60 dias após dias após a emissão da Ordem de Serviço	R$ 35.000,00
Recebimento Definitivo do treinamento, capacitação e transferência de conhecimento.	60 dias após emissão da Ordem de Serviço	R$ 38.000,00

12. REGIME DE EXECUÇÃO DO CONTRATO

12.1. O regime de execução do contrato será de empreitada por preço unitário.

13. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

13.1. FORMA DE SELEÇÃO E CRITÉRIO DE JULGAMENTO DA PROPOSTA

13.1.1. 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.

13.1.2. O fornecedor deverá comprovar que a solução contém os requisitos da contratação e arquitetura tecnológica - Anexo I.

13.2. **QUALIFICAÇÃO TÉCNICA**

13.2.1. 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 em conformidade com as especificações descritas neste documento e anexos.

13.2.2. Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante.

13.2.3. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

13.2.4. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da CONTRATANTE e local em que foi executado o objeto CONTRATADO, dentre outros documentos.

14. DO REAJUSTE

14.1. Será adotado como índice de reajuste do Contrato o Índice de Custos de Tecnologia da Informação – ICTI.

15. DA AMOSTRA DO OBJETO

15.1. Não será exigida amostra para o objeto deste Termo de Referência.

16. DA VISTORIA

16.1. 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) 3348-8558 ou 3348-8655 ou 3348-9258 ou 3348-9257.

16.2. 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.

17. GARANTIA CONTRATUAL

17.1. Será exigida a garantia da contratação no percentual de 5% do valor contratual, conforme regras previstas no contrato.

18. SUBCONTRATAÇÃO

18.1. Não é admitida a subcontratação do objeto contratual, conforme justificativa constante do Estudo Técnico Preliminar.

19. REPONSÁVEIS

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO				
Integrante	**Nome**	**Matrícula**	**Lotação**	**Ramal**
Requisitante	**LUÍS FELIPE RABELLO TAVEIRA**	22970	SEINF	8344
Técnico	**HUGO LEITE FLORENCO MAIA**	23526	SEINF	8321
Administrativo	**GUSTAVO TRINDADE OLIVEIRA**	16700	DIAP	8570

ÁREA TÉCNICA DE TI			
NOME DA ÁREA TÉCNICA DE TI	**NOME DO CHEFE OU SUBSTITUTO**	**Matrícula**	**Ramal**
CMI	JEFFERSON MOURA PARAVIDINE	22751	8344

20.	**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.

JEFFERSON MOURA PARAVIDINE
Coordenador da CMI

ANEXO I – REQUISITOS DA CONTRATAÇÃO

1. REQUISITOS DA CONTRATAÇÃO E ARQUITETURA TECNOLÓGICA

1	**Requisitos do Agente**	
id	**Descrição do requisito**	Evidência de atendimento ao requisito (a ser preenchido pelo licitante).
1	Monitoramento em tempo real: recursos de monitoramento em tempo real, permitindo que os administradores de segurança identifiquem rapidamente ameaças e atividades maliciosas em seus ambientes.	
2	A solução proposta deve ser capaz de impedir violações de segurança e tentativas de ransomware em tempo real.	
3	A solução proposta deve ser capaz de registrar em tempo real informações do processo e informações adicionais, como o conhecimento do usuário associado aos eventos.	
4	A solução proposta deve ter a opção de definir a senha para desinstalar o agente no terminal.	
5	A solução deve ser compatível com storages Dell da linha Unity XT. Assumindo a contratada a responsabilidade pela referida integração, incluindo-se análise, descoberta, quarentena e remoção de ameaças detectadas em sistemas de arquivos hospedados sobre os NAS virtualizados nos referidos equipamentos, tanto no formato Linux via ICAP, fazendo-se uso do recurso de integração nativa do storage, juntamente com documento do fabricante da solução Endpoint que afirme contar com a referida funcionalidade e atestar a compatibilidade com o referido equipamento.	
6	A solução proposta deve ser capaz de gerar um instalador Windows pré-configurado. Esta configuração deve permitir a instalação sem a necessidade de interação ou configuração do usuário.	
7	A solução deve deve ser compatível com endpoints e servidores virtuais com os sistemas operacionais: Microsoft Windows 8.1, 10, 11 e pro, Windows Server 2016 e 2019, Red Hat Enterprise Linux versão 7 ou superior, CentOS 7 (64 bits) ou superior, Ubuntu versão 20 ou superior.	
8	A solução proposta deve ser compatível com plataformas móveis tais como smartphones e tablets, com sistema operacional Android (versões 11.0 ou superior)e Apple IOS (versões 14.0 ou superior).	
9	A solução proposta deve ser compatível com os seguintes sistemas operacionais: Ambientes de Virtual Desktop Infrastructure (VDI) em VMware ESXi 7.0.3.	
10	A solução proposta deve oferecer suporte à implantação em massa por meio de ferramentas como MS System Center.	
11	A solução proposta deve ter a capacidade de atualizar o terminal sem interação do usuário e sem exigir uma reinicialização.	
12	A solução proposta deve ter proteção "Anti-adulteração" no Agente.	
2	**Requisito - Prevenção de Malware**	
id	**Descrição do requisito**	
1	A solução proposta deve ser capaz de impedir violações de segurança e tentativas de ransomware em tempo real.	
2	A solução proposta deve ter a capacidade de prevenir a execução de arquivos maliciosos.	
3	A solução proposta deve ter a capacidade de controlar dispositivos USB.	
4	A solução proposta deve ter a capacidade de criar exceções para dispositivos USB com base em uma combinação de: nome do dispositivo, fornecedor, número de série.	
5	A solução proposta deve ser capaz de bloquear o tráfego malicioso de exfiltração de dados.	
6	A solução proposta deve ser capaz de tratar ameaças por ransomware, evitando a modificação de arquivos ou registros dos dispositivos.	
7	A solução proposta deve ser capaz de permitir verificações periódicas dos arquivos contidos nos dispositivos com o Agente instalado.	
3	**Requisito - Detecção de Malware**	
id	**Descrição do requisito**	Evidência de atendimento ao requisito (a ser preenchido pelo licitante).
1	Detecção de ameaças avançadas: A solução deve ser capaz de detectar ameaças avançadas, incluindo ataques de dia zero e ameaças persistentes avançadas (APTs), usando técnicas de análise de comportamento e aprendizado de máquina (machine learning).	
2	A solução proposta deve ser capaz de funcionar no modo "offline" sem que o Agente esteja conectado à rede corporativa.	
3	A solução proposta deve ser capaz de detectar processos em execução, inícios de processos, paradas de processos e interações entre processos.	
4	A solução proposta deve ser capaz de detectar, eliminar e retornar ao seu valor inicial as alterações feitas por processos maliciosos no registro do PC.	
5	A solução proposta deve ser capaz de detectar as solicitações de DNS enviadas do dispositivo.	
6	A solução proposta deve ser capaz de detectar conexões de rede a partir do dispositivo.	
7	A solução proposta deve ser capaz de detectar atividades suspeitas associadas a arquivos DLL.	

8	A solução proposta deve ser capaz de incorporar inteligência de ameaças ao esquema de detecção.	
9	A solução proposta deve ser capaz de incorporar as técnicas MITER ATT & CK no esquema de detecção e mostrar quais dessas técnicas foram utilizadas.	
10	A solução proposta deve ter a capacidade de realizar consultas de texto livre (customizável) para filtrar as informações disponíveis para a caça de ameaças.	
11	A solução proposta deve ter a capacidade de armazenar pesquisas realizadas para serem reutilizadas no futuro.	
12	A solução proposta deve identificar atividades maliciosas conhecidas.	
13	A solução proposta deve ter a capacidade de receber atualizações diárias de inteligência.	
14	A solução proposta deve ter a capacidade de categorizar os eventos detectados em diferentes categorias.	
4	**Requisito - Resposta ao Incidente**	
id	**Descrição do requisito**	Evidência de atendimento ao requisito (a ser preenchido pelo licitante).
1	A solução proposta deve permitir um histórico dos eventos por no mínimo 30 (trinta) dias.	
2	Análise forense: A solução deve possuir recursos de análise forense para ajudar a investigar incidentes de segurança, identificar a origem e o escopo das ameaças e coletar evidências para fins de investigação.	
3	A solução proposta deve permitir a integração com syslog.	
4	A solução deve ser compatível com software de monitoramento de redes e sistemas de computadores de código aberto Zabbix.	
5	A solução proposta deve ter capacidade de proteção de memória (Memory Protection), para a monitoração, proteção de aplicativos e componentes críticos do sistema operacional de serem adulterados em tempo de execução, isto é, durante operação e execução em memória.	
6	A solução proposta deve ter a capacidade de encerrar um processo com base em sua classificação, e deve também ter a capacidade de excluir um arquivo com base em sua classificação.	
7	A solução proposta deve ser a capacidade de restaurar as configurações de registro básicas com base na classificação de atividade predefinida.	
8	A solução proposta deve ter a capacidade de isolar os dispositivos infectados da rede.	
9	A solução proposta deve obter visibilidade total da cadeia de ataques e alterações maliciosas.	
10	A solução proposta deve permitir a limpeza automática do dispositivo e reverter alterações maliciosas, mantendo o tempo de atividade do dispositivo.	
11	A solução proposta deve permitir o envio de executáveis para análise em um sandbox, a fim de determinar se são maliciosos ou inofensivos.	
12	A solução proposta deve fornecer vários mecanismos de proteção, incluindo o encerramento de um processo, a exclusão de um arquivo malicioso, o bloqueio de uma conexão de rede.	
5	**Requisito - Difusão (Pós-infecção)**	
id	**Descrição do requisito**	Evidência de atendimento ao requisito (a ser preenchido pelo licitante).
1	A solução proposta deve permitir o isolamento manual do tráfego de rede de um dispositivo onde foi encontrada uma atividade causada por malware.	
2	A solução proposta deve permitir o bloqueio de atividades realizadas por arquivos maliciosos.	
3	A solução proposta deve ter a capacidade de criar exceções com base na localização do arquivo, tráfego realizado e processo executado.	
4	A solução proposta deve ter a capacidade de criar exceções manualmente para falsos positivos para marcar a atividade como um falso positivo e evitar a ocorrência de falhas futuras.	
5	A solução proposta deve permitir a criação de exceções de eventos.	
6	**Requisito - Controle de Vulnerabilidade e Comunicação**	
id	**Descrição do requisito**	Evidência de atendimento ao requisito (a ser preenchido pelo licitante).
1	A solução proposta deve ter a capacidade de descobrir aplicativos que estão se comunicando através da rede e que representam risco para o terminal.	
2	A solução proposta deve reduzir a superfície de ataque utilizando bloqueio da aplicação que apresentar comportamento anômalo, com base no CVE/MITRE ATT&CK.	
3	A solução proposta deve ter a capacidade de impedir que aplicativos não autorizados se comuniquem pela rede.	
4	A solução proposta deve ter a capacidade de criar políticas que tenham a capacidade de impedir a comunicação de aplicativos de acordo com a versão do aplicativo instalado.	
5	A solução proposta deve ser capaz executar o bloqueio de aplicações.	
6	A solução proposta deve ser capaz de visualizar e entregar informações sobre o uso dos aplicativos de rede mostrando informações como os destinos IP do tráfego gerado pelo aplicativo.	
7	**Requisito - Cenários de Ataque**	
id	**Descrição do requisito**	Evidência de atendimento ao requisito (a ser preenchido pelo licitante).
1	A solução proposta deve identificar e prevenir tentativas de perseguição de privilégios.	
2	A solução proposta deve bloquear ataques de ransomware conhecidos.	
3	A solução proposta deve detectar malware desconhecido como RAT (Trojan de acesso remoto) por meio das atividades do malware e não de uma assinatura.	
4	A solução proposta deve proteger contra scripts Powershell maliciosos.	
5	A solução proposta deve proteger contra scripts CScript maliciosos.	

6	A solução proposta deve proteger contra macros maliciosas do Microsoft Office.	
8	**Requisitos - Console de Gerenciamento Centralizado de políticas de Segurança, Logs e relatórios**	
id	**Descrição do requisito**	Evidência de atendimento ao requisito (a ser preenchido pelo licitante).
1	Gerenciamento centralizado: a solução deve permitir o gerenciamento centralizado de endpoints, simplificando a implantação, configuração e gerenciamento das soluções em toda a organização.	
2	Console de administração deve ser compatível com modelo de instalação em nuvem.	
3	A console de administração em núvem deve possuir suporte a autenticação multifatorial (MFA) para garantir maior segurança no acesso e gestão da solução de segurança.	
4	A solução deve deve possuir interface gráfica para configuração, administração e monitoração das licenças instaladas nos endpoints.	
5	Deve possuir capacidade de coletar e analisar dados de eventos de segurança em endpoints e em toda a rede, incluindo registros de sistema, atividades de processos, conexões de rede e arquivos executados.	
6	Relatórios e análises: a solução deve ser capaz de fornecer relatórios e análises detalhados sobre atividades de endpoints, ajudando as equipes de segurança a entender melhor os padrões de ameaças e o comportamento do usuário, fornecendo visibilidade e relatórios detalhados sobre ameaças, incluindo a identificação do tipo de ataque, o vetor de ataque e o impacto nas vítimas.	
7	A solução deve possuir console de gerenciamento com capacidade de integração, gestão e atualização de no mínimo 1575 (um mil quinhentos e setenta e cinco reais) licenças instaladas nos endpoint - máquina de usuário final ou servidores virtuais windows e linux no ambiente virtualizado. A console deve possuir capacidade de gerenciar e controlar endpoints de forma centralizada, incluindo implantação de políticas de segurança, atualizações de software, configurações e relatórios.	
8	O console de gerenciamento da solução proposta deve permitir a integração com o "Active Directory" para garantir o cumprimento dos requisitos da política de senhas da empresa.	
9	O console de administração da solução proposta deve permitir o uso de funções granulares para administradores. Permitindo a gestão da gerência por meio de delegação de funções e atribuições baseado em papeis dentro da solução.	
10	A console de administração deve ser capaz de realizar a instalação e distribuição do agente nos endpoints.	
11	O console de administração da solução proposta deve permitir a visualização dos eventos registrados nos dispositivos que requerem atenção.	
12	O console de administração da solução proposta deve permitir a visualização da saúde dos Agentes instalados.	
13	O console de administração da solução proposta deve permitir a desinstalação remota do Agente instalado nos dispositivos.	
14	O console de administração da solução proposta deve permitir a desativação / ativação remota do Agente instalado nos dispositivos.	
15	O console de administração da solução proposta deve permitir a atualização remota do Agente instalado nos dispositivos.	
16	O console de administração da solução proposta deve permitir a criação de relatórios executivos contendo um resumo que descreva os eventos de segurança e o status do sistema.	
17	O console de administração da solução proposta deve permitir a criação de grupos organizacionais de dispositivos nos quais cada grupo possa ter regras de proteção independentes dos demais.	
18	O console de administração da solução proposta deve permitir a exportação dos logs locais gerados pelos Agentes a partir do mesmo console.	
19	O console de administração da solução proposta deve permitir a criação de relatórios de inventário dos Agentes implantados contendo informações como: Endereço IP, Nome do Host, Sistema Operacional, Endereço MAC, Versão do Agente instalado, Status do Agente, último dia visto pelo console.	
20	O console de gerenciamento da solução proposta deve ter a visibilidade dos eventos gerados pelos dispositivos ou eventos de acordo com o processo executado.	
21	O console de administração da solução proposta deve permitir a integração de um SMTP externo para envio de alertas por e-mail.	
22	O console de administração da solução proposta deve permitir auditorias de alterações feitas por administradores / operadores. Exportação dos relatórios, no mínimo, para o formato CSV e PDF.	
23	A solução proposta deve permitir a configuração de perfis nas informações coletadas para a função de caça a ameaças.	
24	A solução proposta deve permitir exclusões de informações que não serão coletadas na função de caça a ameaças.	
25	A solução proposta deve permitir que os administradores desabilitem as notificações para um evento de descoberta.	
26	A solução proposta deve permitir que as funções de filtragem da web sejam realizadas bloqueando o acesso a páginas da web categorizadas como maliciosas.	
27	A solução proposta deve permitir compatibilidade na integração com o firewall FortiGate da Fortinet por meio do Security Fabric do ForiGate Fortinet ou via API (Application Programming Interface).	

9.	**REQUISITOS INTERNOS NÃO-FUNCIONAIS**
INSTALAÇÃO, CONFIGURAÇÃO E SUPORTE TÉCNICO ESPECIALIZADO	
id	**Descrição do Requisito**
1	Todas as despesas e ônus dos serviços de instalação e configuração correrão por conta da CONTRATADA.
2	A solução é composta por licenças de software.
3	A solução de segurança pode consistir em um único produto ou em um conjunto de módulos e aplicativos que juntos fornecem recursos de antivírus e detecção e resposta de endpoint (EDR). Quando a solução é composta por vários módulos, não cabe qualquer ônus ou despesas adicionais por parte do CONTRATANTE para adquirir softwares, módulos ou serviços extras que atendam aos requisitos funcionais do objeto desta contratação. Em outras palavras, a solução contratada deve oferecer todos os recursos necessários para a proteção de endpoint em um único pacote, sem a necessidade de custos extras para complementar a funcionalidade da solução de segurança, antivírus e EDR.
4	No início da execução contratual, a CONTRATANTE deverá definir, por meio de uma Ordem de Serviço própria, a instalação dos agentes nos endpoints, bem como a instalação e configuração da console de gerenciamento dos endpoints da solução em nuvem, respeitado os quantitativos de aquisição de licenças descritos no item 5.1.1 e item 5.1.2.
5	As licenças adquiridas serão avaliadas, durante a contratação, quanto a sua necessidade, podendo ser solicitadas ou retiradas, por meio de Ofício do Gestor do Contrato e do Fiscal do Contrato, conforme estudo interno e necessidade da CONTRATANTE.

6	A CONTRATADA será responsável por instalar os agentes nos endpoints na infraestrutura da CONTRATANTE e prestar suporte e atualização durante todo o período de vigência das licenças. A console de gerenciamento poderá ser ofertada tanto no modelo on-premises ou em nuvem, e a decisão caberá à Equipe de Fiscalização do contrato na emissão da Ordem de Serviço, ouvida a CONTRATADA.
7	No ato de entrega deverão ser fornecidas, pela CONTRATADA, as últimas versões dos softwares disponíveis no mercado pelo fabricante.
8	Os serviços de instalação, configuração, testes, suporte técnico e garantia deverão atender às especificações técnicas contidas neste Termo de Referência.
9	Deve possuir garantia de funcionamento para todos os softwares fornecidos, durante o período contratado, a partir da emissão do Termo de Recebimento Definitivo pela CLDF.
10	A CONTRATADA deverá dispor de central de atendimento para abertura de chamados na modalidade mínima de 24 (vinte e quatro) horas x 7 (sete) dias. Os chamados poderão ser efetuados através de ligação local, ou através de telefone 0800 (ligação gratuita), acesso web ou e-mail. Os chamados serão registrados e ficarão disponíveis para consulta pela CLDF.
11	A CONTRATADA deverá possuir assistência técnica autorizada, certificada pelo fabricante da solução - mediante comprovação; e prestar serviço de suporte em Brasília-DF.
12	Na ocasião de término da contratação, seja por exaurimento contratual ou interrupção da contratação. Para garantir a proteção dos dados e a gestão da continuidade, a CONTRATADA será notificada por meio de uma Ordem de Serviço própria e deverá tomar todas as providências necessárias, sem qualquer ônus para a CONTRATANTE, para remover a aplicação instalada nos endpoints, máquinas virtuais e quaisquer outros locais onde houver resquícios da instalação da aplicação que se encerra. O exaurimento contratual implica o fim das obrigações e dos direitos decorrentes do contrato entre as partes. No entanto, o exaurimento contratual não exclui a responsabilidade civil ou administrativa por eventuais danos causados durante a execução do contrato.
13	A contratada compromete-se a cumprir na integralidade a Lei Geral de Proteção de Dados.
10	**OPERAÇÃO ASSISTIDA**
id	**Descrição do Requisito**
1	A operação assistida terá início após a instalação e configuração da solução e a emissão de ordem de serviço específica, ou em conjunto com o fornecimento das licenças.
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.
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, pelo período de 30 (trinta) dias corridos.
4	O técnico deverá ter experiência com todos recursos da solução de segurança, tanto das licenças nos endpoints como a solução de gerência, para que oriente e opere todo sistema e transfira para a equipe da CONTRATANTE o conhecimento necessário para que possa operá-la.
5	O técnico alocado deve ser devidamente certificado pelo fabricante para suporte e na solução de segurança e sua gerência.
6	O técnico deverá estar identificado com crachá da CONTRATADA durante sua permanência nas dependências da CLDF.
7	O técnico compromete-se a cumprir na integralidade a Lei Geral de Proteção de Dados.
11	**CAPACITAÇÃO - GERAL**
id	**Descrição do Requisito**
1	A capacitação terá cronograma específico, a ser acertado entre a CONTRATANTE e a CONTRATADA, durante a FASE II, do Cronograma de Execução, por meio do Plano de Capacitação Técnica. A aquisição do treinamento é opcional pela CONTRATANTE.
2	O material didático deverá ser oficial e homologado pelo fornecedor/fabricante. Não obstante, a pós a emissão da Ordem de Serviço para o treinamento a CONTRATADA acordará com a CONTRATANTE, previamente ao inicio do treinamento, a ementa temática do treinamento.
3	O treinamento inicial poderá ser realizado em qualquer momento durante a vigência contratual.
4	O treinamento terá início após a emissão de Ordem de Serviço específica.
5	O treinamento poderá ser dividido em duas turmas de 4 (quatro) alunos cada, totalizando 8 alunos capacitados ao final da fase de treinamento e capacitação. Sendo que cada turma deve ser ministrada em 4 (quatro) horas aulas por dia, preferencialmente por cinco dias úteis consecutivos, totalizando uma carga horária de 20 (vinte) horas/aulas.
6	O treinamento deverá abranger habilidades e competências essenciais sobre segurança da informação, tanto conceituais quanto práticas, que sejam adequadas para compreensão e operação da solução de segurança contratada. Será necessário fornecer aos participantes as informações necessárias para entender os principais conceitos relacionados à segurança da informação, bem como as melhores práticas para implementá-los. Além disso, o treinamento deve garantir que os participantes tenham conhecimento suficiente para operar a solução de segurança de maneira eficaz e segura.
7	A CONTRATADA deverá arcar com todos os custos relacionados à realização do treinamento, incluindo o custeio com instrutoria, de recursos tecnológicos, plataforma de ensino, link de internet e conectividade necessários para a sua execução. Isso significa que quaisquer despesas associadas ao treinamento não serão transferidas para a CONTRATANTE. É importante ressaltar que a contratada deve fornecer recursos adequados para garantir a qualidade do treinamento e a participação efetiva dos envolvidos.
8	Para avaliar o treinamento, a CONTRATANTE considerará uma série de itens, incluindo o programa, o domínio do conteúdo, os recursos de aprendizagem, o material, o ambiente e os resultados obtidos. Esses critérios serão utilizados para determinar se será necessária a repetição da capacitação ou se os objetivos do treinamento foram alcançados de forma satisfatória. É importante ressaltar que a avaliação do treinamento será realizada de forma objetiva e baseada em critérios pré-definidos, garantindo a transparência e a equidade no processo de avaliação.
9	No caso de resultado insatisfatório na avaliação da capacitação, o treinamento deverá ser novamente realizado, sem ônus adicionais para a CONTRATANTE.
10	Será tolerada apenas uma nova realização de cada curso da capacitação por servidor.
11	O material didático deverá ser oficial e homologado pelo fornecedor/fabricante. Não obstante, após a emissão da Ordem de Serviço para o treinamento a CONTRATADA acordará com a CONTRATANTE, previamente ao inicio do treinamento, a ementa temática do treinamento.
12	Os serviços de treinamento serão pagos de acordo com a sua execução, mediante envio, pela CONTRATADA, dos certificados e da nota fiscal, e emissão de recebimento, desde que não haja pendências de responsabilidade da CONTRATADA.

1.2 REQUISITOS DE PROJETO E DE IMPLEMENTAÇÃO

1.2.1 Todas as despesas e ônus dos serviços de instalação das licenças nos endpoints e da console de gerenciamento ocorrerão por conta da CONTRATADA;

1.2.2 Todos os serviços (instalação, suporte técnico, assistência técnica, monitoração e garantia) deverão atender as especificações técnicas contidas neste Termo de Referência;

1.2.3 Possuir garantia de funcionamento, assistência técnica e suporte técnico para todos os equipamentos (incluídos softwares) fornecidos, durante o período de 36 (trinta e seis) meses, a partir da emissão do Termo de Recebimento Definitivo pela CLDF;

1.2.4 A CONTRATADA deverá dispor de central de atendimento para abertura de chamados na modalidade mínima de 24 (vinte e quatro) horas x 7 (sete) dias. Os chamados poderão ser efetuados através de ligação local, ou através de telefone 0800 (ligação gratuita), acesso Web ou e-mail. Os chamados serão ser registrados e ficarão disponíveis para consulta pela CLDF.

1.3 REQUISITOS DE IMPLANTAÇÃO

1.3.1 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.

1.4 REQUISITOS DE GARANTIA E MANUTENÇÃO

1.4.3 O prazo de garantia contratual dos bens, complementar à garantia legal, é de, no mínimo, 12 meses, ou pelo prazo fornecido pelo fabricante, se superior, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.
1.4.4 Caso o prazo da garantia oferecida pelo fabricante seja inferior ao estabelecido nesta cláusula, o fornecedor deverá complementar a garantia do bem ofertado pelo período restante.
1.4.5 A garantia será prestada com vistas a manter os equipamentos fornecidos em perfeitas condições de uso, sem qualquer ônus ou custo adicional para a CONTRATANTE.
1.4.6 A garantia abrange a realização da manutenção corretiva dos bens pela própria CONTRATADA, ou, se for o caso, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.
1.4.7 Entende-se por manutenção corretiva aquela destinada a corrigir os defeitos apresentados pelos bens, compreendendo a substituição de peças, a realização de ajustes, reparos e correções necessárias.
1.4.8 As peças que apresentarem vício ou defeito no período de vigência da garantia deverão ser substituídas por outras novas, de primeiro uso, e originais, que apresentem padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento.
1.4.9 Uma vez notificado, a CONTRATADA realizará a reparação ou substituição dos bens que apresentarem vício ou defeito no prazo de até 7 dias úteis, contados a partir da data de retirada do equipamento das dependências da CLDF pela CONTRATADA ou pela assistência técnica autorizada.
1.4.10 O prazo indicado no subitem anterior, durante seu transcurso, poderá ser prorrogado mediante solicitação escrita e justificada da CONTRATADA, aceita pela CONTRATANTE.
1.4.11 Na hipótese do subitem acima, a CONTRATADA deverá disponibilizar solução equivalente, de especificação igual ou superior ao anteriormente fornecido, para utilização em caráter provisório pela CONTRATANTE, de modo a garantir a continuidade dos trabalhos administrativos durante a execução dos reparos.

1.5 REQUISITOS DE CAPACITAÇÃO

1.5.1 A capacitação terá cronograma específico, a ser acertado entre a CONTRATANTE e a CONTRATADA, durante a FASE II, do Cronograma de Execução, por meio do Plano de Capacitação Técnica. A aquisição do treinamento é opcional pela CONTRATANTE.
1.5.2 O material didático deverá ser oficial e homologado pelo fornecedor/fabricante. Não obstante, a pós a emissão da Ordem de Serviço para o treinamento a CONTRATADA acordará com a CONTRATANTE, previamente ao inicio do treinamento, a ementa temática do treinamento.
1.5.3 O treinamento inicial poderá ser realizado em qualquer momento durante a vigência contratual.
1.5.4 O treinamento terá início após a emissão de Ordem de Serviço específica.
1.5.5 O treinamento poderá ser dividido em duas turmas de 4 (quatro) alunos cada, totalizando 8 alunos capacitados ao final da fase de treinamento e capacitação. Sendo que cada turma deve ser ministrada em 4 (quatro) horas aulas por dia, preferencialmente por cinco dias úteis consecutivos, totalizando uma carga horária de 20 (vinte) horas/aulas.
1.5.6 O treinamento deverá abranger habilidades e competências essenciais sobre segurança da informação, tanto conceituais quanto práticas, que sejam adequadas para compreensão e operação da solução de segurança contratada. 1.5.7 1.5.7 Será necessário fornecer aos participantes as informações necessárias para entender os principais conceitos relacionados à segurança da informação, bem como as melhores práticas para implementá-los. Além disso, o treinamento deve garantir que os participantes tenham conhecimento suficiente para operar a solução de segurança de maneira eficaz e segura.
1.5.8 A CONTRATADA deverá arcar com todos os custos relacionados à realização do treinamento, incluindo o custeio com instrutoria, de recursos tecnológicos, plataforma de ensino, link de internet e conectividade necessários para a sua execução. Isso significa que quaisquer despesas associadas ao treinamento não serão transferidas para a CONTRATANTE. É importante ressaltar que a contratada deve fornecer recursos adequados para garantir a qualidade do treinamento e a participação efetiva dos envolvidos.
1.5.9 Para avaliar o treinamento, a CONTRATANTE considerará uma série de itens, incluindo o programa, o domínio do conteúdo, os recursos de aprendizagem, o material, o ambiente e os resultados obtidos. Esses critérios serão utilizados para determinar se será necessária a repetição da capacitação ou se os objetivos do treinamento foram alcançados de forma satisfatória. É importante ressaltar que a avaliação do treinamento será realizada de forma objetiva e baseada em critérios pré-definidos, garantindo a transparência e a equidade no processo de avaliação.
1.5.10 No caso de resultado insatisfatório na avaliação da capacitação, o treinamento deverá ser novamente realizado, sem ônus adicionais para a CONTRATANTE.
1.5.11 Será tolerada apenas uma nova realização de cada curso da capacitação por servidor.
1.5.12 O material didático deverá ser oficial e homologado pelo fornecedor/fabricante. Não obstante, após a emissão da Ordem de Serviço para o treinamento a CONTRATADA acordará com a CONTRATANTE, previamente ao inicio do treinamento, a ementa temática do treinamento.
1.5.13 Os serviços de treinamento serão pagos de acordo com a sua execução, mediante envio, pela CONTRATADA, dos certificados e da nota fiscal, e emissão de recebimento, desde que não haja pendências de responsabilidade da CONTRATADA.

1.6 REQUISITOS DE METODOLOGIA DE TRABALHO

1.6.1 O fornecimento dos equipamentos está condicionado ao recebimento pela CONTRATADA de Ordem de Fornecimento de Bens (OFB) ou equivalente emitida pela CONTRATANTE.
1.6.2 A OFB indicará o tipo de equipamento, a quantidade e a localidade na qual os equipamentos deverão ser entregues.
1.6.3 A CONTRATADA deve fornecer meios para contato e registro de ocorrências da seguinte forma: com funcionamento de 24 horas por dia e 7 dias por semana de maneira eletrônica e de 24 horas por dia e 7 dias por semana por semana por via telefônica.
1.6.4 O andamento do fornecimento dos equipamentos dever ser acompanhado pela CONTRATADA, que dará ciência de eventuais acontecimentos à CONTRATANTE.

1.9 REQUISITOS DE SEGURANÇA, SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

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

1.10 REQUISITOS LEGAIS

1.10.1 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.

1.11 REQUISITOS TEMPORAIS

1.11.1 A entrega das licenças deverá ser efetivada no prazo máximo de 30 dias corridos, a contar do recebimento da Ordem de Fornecimento de Bens (OFB) ou equivalente, emitida pela CONTRATANTE, podendo ser prorrogada, excepcionalmente, desde que justificado previamente pela CONTRATADA e autorizado pela CONTRATANTE.

ANEXO II – TERMO DE COMPROMISSO

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 V - 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.

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 **HUGO LEITE FLORENCO MAIA - Matr. 23526**, **Integrante Técnico**, em 14/06/2023, às 16:42, conforme Art. 22, do Ato do Vice-Presidente n° 08, de 2019, publicado no Diário da Câmara Legislativa do Distrito Federal nº 214, de 14 de outubro de 2019.

Documento assinado eletronicamente por **GUSTAVO TRINDADE OLIVEIRA - Matr. 16700**, **Integrante Administrativo**, em 14/06/2023, às 18:09, conforme Art. 22, do Ato do Vice-Presidente n° 08, de 2019, publicado no Diário da Câmara Legislativa do Distrito Federal nº 214, de 14 de outubro de 2019.

Documento assinado eletronicamente por **RONALDO MARCIANO DA SILVA - Matr. 11214**, **Analista Legislativo**, em 14/06/2023, às 18:20, conforme Art. 22, do Ato do Vice-Presidente n° 08, de 2019, publicado no Diário da Câmara Legislativa do Distrito Federal nº 214, de 14 de outubro de 2019.

Documento assinado eletronicamente por **LUIS FELIPE RABELLO TAVEIRA - Matr. 22970**, **Chefe da Seção de Infraestrutura de Tecnologia da Informação**, em 14/06/2023, às 18:47, conforme Art. 22, do Ato do Vice-Presidente n° 08, de 2019, publicado no Diário da Câmara Legislativa do Distrito Federal nº 214, de 14 de outubro de 2019.

Documento assinado eletronicamente por **JEFFERSON MOURA PARAVIDINE - Matr. 22751**, **Coordenador(a) de Modernização e Informática**, em 15/06/2023, às 11:25, conforme Art. 22, do Ato do Vice-Presidente n° 08, de 2019, publicado no Diário da Câmara Legislativa do Distrito Federal nº 214, de 14 de outubro de 2019.

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: **1210816** Código CRC: **06B471FE**.