



Governo do Distrito Federal
Polícia Civil do Distrito Federal
Divisão de Tecnologia
Serviço de Governança de Projetos

Termo de Referência n.º 4/2026 - PCDF/DGPC/DGI/DITEC/SGP

MICROSSEGMENTAÇÃO

1. OBJETO DA CONTRATAÇÃO

1.1. Contratação de empresa para fornecimento de Solução de Segurança para Microsegmentação de rede, incluindo instalação, implantação, treinamento, garantia e suporte técnica, por 12 (doze) meses.

ITEM	CATSER	DESCRIÇÃO	U.M	Qtd.
1	27502	Fornecimento de Solução de segurança para microsegmentação de ambiente corporativo com licenciamento para Servidores.	Licença	516
2	27502	Fornecimento de Solução de microsegmentação de ambiente corporativo com licenciamento para Endpoints.	Licença	5000
3	27502	Fornecimento de Solução de microsegmentação de ambiente corporativo com licenciamento para Kubernetes.	Licença	21
4	26972	Serviço de Instalação da solução.	Serviço	1
5	20052	Serviço de Treinamento para 5 pessoas.	Serviço	5

1.2. Em caso de discordância existente entre as especificações descritas no <https://catalogo.compras.gov.br/cnbs-web/busca> – CATMAT/CATSER e as especificações constantes deste Termo de Referência, prevalecerão as especificações contidas neste Termo de Referência.

1.3. O objeto da contratação NÃO incide nas hipóteses vedadas pelos artigos 3º e 4º da IN SGD nº 94/2022.

1.4. Ademais, o objeto desta contratação é caracterizado como **serviço comum**, uma vez que possuem padrões de desempenho e características gerais e específicas usualmente encontradas no mercado, sendo passíveis de serem definidos de forma objetiva, conforme art. 6º, inciso XIII da Lei 14.133/2021, podendo, portanto, ser licitado por meio da modalidade Pregão Eletrônico.

1.5. O objeto desta contratação não se enquadra como sendo de bem de luxo, conforme Decreto nº 10.818/2021 e artigos 75 a 78 do Decreto Distrital 44.330/2023.

1.6. O prazo de vigência da contratação é de 12 (doze) meses contados da assinatura do contrato, podendo ser prorrogado por até 10 anos, na forma do art. 106, §2º, e art. 107 da Lei nº 14.133 de 2021, desde que as condições e preços se mantenham vantajosos para a Administração. O serviço é enquadrado como continuado considerando a gestão de continuidade de serviços de tecnologia, sendo parte integrante da Política de Segurança da Informação (PSI) da PCDF, conforme item 1.10 e 3.1.5 do TR.

1.7. Em observância ao art. 36, §1º do Decreto Distrital nº 44.330/2023 C/C Parecer Referencial nº 66/2024 - PGDF/PGCONS procedeu-se à consulta ao catálogo eletrônico de padronização do Poder Executivo Federal disponível no Portal Nacional de Compras e Contratações – PNCP, disponível em <https://www.gov.br/pncp/pt-br/catalogo-eletronico-de-padronizacao/catalogo-eletronico-de-padronizacao>, contudo o objeto em tela não consta no referido catálogo, e portanto, foi catalogado em consonância com o Catálogo de Materiais e Serviços - CATMAT/ CATSER do Compras.gov.br.

1.8. O objeto da contratação não possui contratações correlatas ou interdependentes que sejam

necessárias para a viabilidade e execução desta demanda.

1.9. Este Termo de Referência foi elaborado pela Equipe de Planejamento da Contratação instituída para este fim, após realização do Estudo Técnico Preliminar, fundamentado na Instrução Normativa SGD/ME nº 94/2022, alinhado à Lei Federal nº 14.133/2021, regulamentada no DF pelo Decreto Distrital nº 44.330/2023.

1.10. Os serviços a serem contratados são de natureza continuada, não se confundem com as atividades finalísticas, têm característica de alta relevância para manutenção, segurança e integridade do ambiente de TIC da PCDF, com impacto direto nos sistemas informatizados e nos dados corporativos, em especial, no atendimento aos sistemas de apoio ao negócio.

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1. MOTIVAÇÃO

2.1.1. Este Termo de Referência foi elaborado pela Equipe de Planejamento da **Contratação** instituída para este fim, após realização do Estudo Técnico Preliminar, fundamentado na Instrução Normativa SGD/ME nº 94/2022, alinhado à Lei Federal nº 14.133/2021, regulamentada no DF pelo Decreto Distrital nº 44.330/2023.

2.1.2. A Polícia Civil do Distrito Federal (PCDF) é uma instituição que tem como atribuição a apuração das infrações penais e a investigação criminal, conforme a Constituição Federal e leis específicas. Para cumprir sua missão, a instituição precisa de tecnologia e equipamentos atualizados, capazes de garantir a eficiência e a eficácia de seus processos.

2.1.3. Os objetivos estratégicos da PCDF incluem a modernização tecnológica, a otimização de processos, a valorização do servidor e a excelência na prestação de serviços. É importante destacar que, em meio a este contexto, a segurança da informação é um aspecto fundamental.

2.1.4. Diante de um cenário de evolução desafiador, onde os riscos de cibersegurança estão em ascensão, torna-se fundamental que a Instituição busque abordagens proativas que visam mitigar essas ameaças, aumentando sua resiliência cibernética.

2.1.5. As ameaças atuais, como ransomware e violações de dados, podem não ser barradas em sua totalidade com ferramentas tradicionais de prevenção, como as que são utilizadas atualmente pela PCDF.

2.1.6. As estratégias de ransomware estão em constante evolução visando burlar a detecção e os controles de segurança.

2.1.7. O objetivo dos ataques de ransomware é criar um mapeamento de todo o ambiente de redes. O trabalho é feito de modo lateral, movendo os invasores de uma máquina ou servidor para outro, utilizando credenciais roubadas para abrir portas dos sistemas, efetuando o sequestro dos dados. Quando os dados são sequestrados, é feito então o pedido de resgate para a recuperação.

2.1.8. A solução de microssegmentação é uma técnica avançada de segurança de rede cujo papel é o de dividir a rede em segmentos menores e mais isolados, denominados de microssegmentos. Cada segmento tem suas próprias políticas de segurança, controles de acesso e monitoramento, limitando a comunicação entre eles a apenas o que é estritamente necessário, dificultando assim a propagação de ameaças de um segmento para o outro.

2.1.9. Em caso de incidente de segurança da informação, como um ataque de ransomware ou violação de dados, a microssegmentação permite isolar a área afetada imediatamente, impedindo a propagação do ataque e permitindo uma recuperação mais eficiente do ambiente, fazendo com que aumente a resiliência da rede da PCDF.

2.1.10. O uso combinado de ferramentas tradicionais adotadas pela PCDF, como antivírus e firewall, junto com a solução de microssegmentação, também conhecida como segmentação de confiança zero (Zero Trust Segmentation), aumentará significativamente as chances de proteção bem sucedidas.

2.1.11. Diante dos cenários de riscos de ataques, a solução de microssegmentação por ser um processo de implementação de isolamento e segmentação da rede, passa a ser uma camada de segurança a mais, somando na contenção dos possíveis danos, contribuindo com a melhoria da maturidade dos

controles de segurança, diminuindo a superfície de ataques maliciosos, criando redes lógicas virtuais, independentes da estrutura física, possibilitando o monitoramento do tráfego e a identificação de ataques maliciosos, aumentando a proteção essencial para a missão crítica da PCDF, além de melhorar a eficiência operacional e conformidade com regulamentos.

2.2. NECESSIDADE E IMPORTÂNCIA DA CONTRATAÇÃO

2.2.1. A infraestrutura de TI da PCDF tem sua rede corporativa composta atualmente por servidores de rede, Kubernetes, dispositivos de armazenamento, firewalls, switches e endpoints, sendo a segmentação da rede realizada por meio de VLANs e firewalls de perímetro.

2.2.2. Estudo e dados de organizações que foram vítimas de ataques cibernéticos mostram que as medidas adotadas pela Instituição, em alguns casos, foram insuficientes para impedir movimentos laterais de ameaças mais avançadas.

2.2.3. Com o crescimento do ambiente de TI e buscando aprimorar a segurança das informações que são de responsabilidade da PCDF, levando-se em conta o cenário de evolução desafiador, onde os riscos de cibersegurança estão em ascensão, tendo como alvos principalmente as organizações governamentais, torna-se fundamental que a Instituição busque abordagens proativas que visem mitigar ameaças, aumentando sua maturidade em resiliência cibernética.

2.2.4. De acordo com os dados publicados pelo Gabinete de Segurança Institucional da Presidência da República (GSI) somente no primeiro mês do ano de 2024 foram, em média, 32 ataques cibernéticos por dia contra órgãos do Governo.

2.2.5. Diariamente os noticiários reportam incidentes de segurança que acontecem por transposição de defesas de perímetro, conforme os exemplos listados abaixo, envolvendo Órgãos do Governo e seus prejuízos: <https://www.gov.br/mj/pt-br/assuntos/noticias/ataque-cibernetico-contra-sistemas-do-governo-federal-sera-apurado-pela-pf>; <https://agenciabrasil.ebc.com.br/radioagencia-nacional/geral/audio/2024-07/sistema-do-governo-federal-que-sofreu-ataque-virtual-volta-funcionar>; <https://agenciabrasil.ebc.com.br/radioagencia-nacional/geral/audio/2024-07/sistema-do-governo-federal-que-sofreu-ataque-virtual-volta-funcionar>; <https://oglobo.globo.com/brasil/noticia/2024/03/01/ataques-ciberneticos-contra-orgaos-do-governo-federal-crescem-em-janeiro-puxados-por-vazamentos-de-dados.ghtml>; https://securityleaders.com.br/hackers-promovem-ataque-ddos-contra-instituicoes-brasileiras-apos-bloqueio-do-x/?utm_campaign=sr_daily_-_030924&utm_medium=email&utm_source=RD+Station; [Ataques a sistemas do governo se aproximam de marc... | VEJA \(abril.com.br\)](#); [ATUALIZADO: Linha do tempo destaca ataques mais recentes - Security Leaders](#)

2.2.6. Os incidentes cibernéticos contra órgãos públicos podem causar graves danos, como atraso na prestação de serviços, indisponibilidade desses, além de vazamentos de dados e violações da privacidade e da Lei Geral de Proteção de Dados (LGPD). No caso da PCDF, a indisponibilidade dos serviços prestados ou o vazamento de dados podem causar danos irreparáveis para a Sociedade.

2.2.7. As ameaças atuais, como ransomware, violações de dados e ameaças persistentes avançadas, podem não ser barradas em sua totalidade por ferramentas tradicionais de prevenção (defesas de perímetro) como as que são utilizadas pela PCDF no momento.

2.2.8. As ameaças persistentes avançadas (APTs) são classes de ataque que, após conseguirem o acesso ao ambiente, se escondem, sem serem detectados, exfiltrando dados ou aguardando o momento oportuno para lançar um ataque ainda mais devastador. O objetivo desse tipo de ataque é tornar extremamente difícil a prevenção, a proteção, a detecção e a resposta a ataques subsequentes. Esse tipo de ataque tem como alvo entidades de alto valor, que possuem dados significativos ou confidenciais, sendo as organizações de segurança uma das mais frequentemente visadas.

2.2.9. As APTS se destacam das demais ameaças cibernéticas por sua sofisticação e complexidade, combinando técnicas avançadas com táticas sociais. São planejadas e executadas após extensa pesquisa e estudo sobre a superfície de ataque da vítima. Em sua fase de execução, seu principal objetivo é não ser detectado na rede pelo maior tempo possível, podendo durar semanas e até anos.

2.2.10. A detecção dessas ameaças atuais requer estratégia de segurança abrangente, englobando busca de ameaças em processos, cargas de trabalho, plataformas, segmentos, além de um monitoramento meticuloso de todo ambiente, com análise contínua do tráfego da rede de entrada e saída.

2.2.11. A falta de uma solução na Instituição que se proponha a fazer todos esses papéis pode dificultar as respostas oportunas e eficazes da equipe de resposta a incidentes.

2.2.12. Diante do exposto e visando mitigar essas ameaças, a PCDF necessita de soluções que monitorem o ambiente, além de implementar diferentes camadas de segurança, complementando as proteções que já são implementadas no ambiente atualmente.

2.3. **OBJETIVOS PRETENDIDOS**

2.3.1. A contratação da solução de microssegmentação pela PCDF tem como objetivo:

2.3.1.1. **Segurança aprimorada:**

a) Isolamento de aplicações, sistemas e serviços: reduzindo o risco de que um ataque a uma parte da rede se propague para outras partes.

b) Políticas Granulares: facilita a aplicação de políticas de segurança específicas para diferentes segmentos da rede (quem pode acessar quais dados e em que circunstâncias), aumentando a precisão e a eficácia das medidas de proteção.

c) Resposta a Incidentes: em caso de incidente de segurança, a microssegmentação pode limitar a extensão do dano, facilitando a contenção e a resposta rápida.

2.3.1.2. **Controle de Acesso:**

a) Menor superfície de ataque: segmenta a rede em partes menores, reduzindo a superfície de ataque, tornando a tarefa de movimentação lateral dentro da rede mais difícil para os invasores.

b) Controle de Tráfego: permite controle mais rigoroso do tráfego entre as diferentes partes da rede, ajudando a detectar e bloquear atividades maliciosas.

2.3.1.3. **Conformidade e auditoria:**

a) Facilidade de Conformidade: a solução pode ajudar no cumprimento de requisitos regulatórios e de conformidade, como PCI, LGPD, GDPR, ao proporcionar um controle mais detalhado sobre o acesso a dados sensíveis (restringindo o acesso apenas aos usuários autorizados – princípio da necessidade/minimização da LGPD) minimizando o risco de acesso não autorizado e vazamentos de dados.

b) Melhoria na auditoria: com segmentos menores de rede, fica mais fácil monitorar e registrar o tráfego, bem como as atividades, facilitando auditorias de segurança.

c) Logs e relatórios: geração de logs detalhados e relatórios sobre atividades dentro dos microssegmentos, ajudando no cumprimento dos requisitos de transparência e prestação de contas.

d) Armazenamento Segregado: Dados pessoais podem ser segregados por tipo e sensibilidade, garantindo que informações mais sensíveis recebam um nível mais alto de proteção.

2.3.1.4. **Desempenho e eficiência:**

a) Gerenciamento do tráfego: otimiza o desempenho da rede ao gerenciar o tráfego interno, reduzindo gargalos e melhorando a eficiência.

b) Escalabilidade: facilita a escalabilidade da rede ao permitir a adição ou remoção de segmentos sem afetar significativamente o restante da infraestrutura.

2.3.1.5. **Resiliência e Continuidade de Negócios:**

a) Resiliência a falhas: se um dos microssegmentos for comprometido ou falhar, o impacto é contido sem que isso afete o restante da rede, que continuará operando normalmente.

b) Rápida Recuperação: facilita a recuperação rápida em casos de incidentes de segurança, uma vez que os microssegmentos podem ser isolados e restaurados individualmente.

2.3.1.6. **Automação e Gestão Simplificada:**

a) Automação de Políticas: a solução inclui recursos de automação que permitem simplificar a implementação e gestão de políticas de segurança de forma global ou seletiva.

b) Visibilidade Centralizada: proporciona uma visão centralizada de toda a rede (usuários e

dispositivos conectados à rede), facilitando a detecção de anomalias e a gestão de políticas de segurança, além de uma rápida tomada de decisões.

c) Visibilidade em nível de processo de aplicação.

d) Identificação de lacunas de segurança através de mapeamento de dependências e fluxos dos aplicativos.

e) Visibilidade de ambiente Kubernetes.

2.4. RESULTADOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

2.4.1. Complementar significativamente as estratégias de segurança multicamada da Instituição, dificultando a concretização de acessos indevidos (redução da superfície de ataque);

2.4.2. Contribuir para a garantia da disponibilidade e continuidade dos serviços de Tecnologia da Informação;

2.4.3. Agilidade na reação às ameaças e ataques, a partir da detecção de vulnerabilidades de segurança em tempo real, reduzindo o tempo de resposta;

2.4.4. Possibilidade de tratar e auditar ações em caso de incidentes de segurança, proporcionando subsídios para tomada de decisões e melhorias dos processos falhos;

2.4.5. Correlacionamento de eventos de segurança, permitindo a criação de inteligência de ameaças, a partir da identificação de padrões de comportamento que possam indicar uma anomalia ou ataque;

2.4.6. Resiliência Cibernética, aumentando a proteção do ambiente contra ataques avançados, como ransomware, de movimentação lateral ou ataques direcionados (APT- Advanced Persistent Threat), restringindo a propagação de ameaças dentro da rede;

2.4.7. Microsegmentação da rede, com configurações de comunicação entre as partes estritamente necessárias, de acordo com as políticas previamente estabelecidas, mitigando os riscos de segurança;

2.4.8. Mapeamento da rede corporativa permitindo correção de vulnerabilidades entre as comunicações internas;

2.4.9. Garantia de meios seguros para acesso remoto ao ambiente;

2.4.10. Automação de políticas de segurança, garantindo que as políticas sejam aplicadas consistentemente, independentemente da localização física dos recursos;

2.4.11. Isolamento granular de sistemas sensíveis, a partir da ação que permite dividir a rede em segmentos menores, isolando sistemas críticos, como bancos de dados de inteligência e dados corporativos de outros sistemas menos críticos;

2.4.12. Limitação de acesso dos usuários internos a sistemas e dados estritamente relevantes para suas funções, prevenindo abusos de acesso ou espionagem interna;

2.4.13. Visibilidade sobre interações entre sistemas e usuários na rede, facilitando o monitoramento contínuo do tráfego pela equipe de segurança.

2.4.14. Flexibilidade e escalabilidade permitindo ajustes, na medida em que a PCDF adquira novos sistemas e dispositivos integrando-os à estrutura existente.

2.4.15. Facilitação da gestão de políticas de segurança em ambientes híbridos, garantindo que a segurança seja mantida de forma consistente, independentemente da localização dos sistemas ou dos dados.

2.4.16. Automatização de respostas a ameaças detectadas, como o isolamento de um segmento comprometido, acelerando a contenção dos incidentes.

2.4.17. Redução de custos com incidentes de segurança uma vez que a prevenção de ataques e a minimização de danos causados por invasores, ajuda a reduzir significativamente os custos associados à recuperação de incidentes de segurança;

2.4.18. Continuidade Operacional no momento em que isolando incidentes, ajuda a garantir a

continuidade dos serviços da PCDF, minimizando o impacto das interrupções, evitando que um ataque tome grandes proporções e paralise a entrega dos serviços essenciais à população.

2.5. JUSTIFICATIVA DO PARCELAMENTO EM LOTES

2.5.1. O estudo técnico preliminar da contratação avaliou, entre outros aspectos técnicos, a viabilidade de parcelamento da solução de TIC a ser contratada, em tantos itens quanto se comprovarem tecnicamente viável e economicamente vantajoso, justificando-se a decisão, conforme § 2º do art. 12 da IN SGD/ME nº 94/2022, e ainda em observância ao disposto nos artigos 40 e 47 da Lei nº 14.133/2021.

2.5.2. O TCU se manifestou sobre o tema através da Súmula 247 – TCU/2007:

“É obrigatória a admissão da adjudicação por item e não por preço global, nos editais das licitações para a contratação de obras, serviços, compras e alienações, cujo objeto seja divisível, desde que não haja prejuízo para o conjunto ou complexo ou perda de economia de escala, tendo em vista o objetivo de propiciar a ampla participação de licitantes que, embora não dispondo de capacidade para a execução, fornecimento ou aquisição da totalidade do objeto, possam fazê-lo com relação a itens ou unidades autônomas, devendo as exigências de habilitação adequar-se a essa divisibilidade”.

2.5.3. Para que todos os serviços sejam prestados pela mesma CONTRATADA – que irá fornecer a solução de Segurança as licenças de software e serviços correlatos (implementação e treinamento) – a CONTRATANTE entende que a licitação ocorra em grupo único. Tratam-se de itens distintos de uma única solução, separados em itens por questões de clareza na composição e formação dos custos. Dissociar serviços e produtos de um único fornecimento traz prejuízos ao conjunto por razões de aumento da complexidade do gerenciamento, conflito de interesse entre diferentes partes prestadoras, além da privação dos ganhos de escala trazidos pela contratação em lote único.

2.5.4. O agrupamento dos diferentes itens da solução em grupo único não implica em restrição de competitividade, uma vez que os fornecedores dos serviços do mercado estão aptos a atender todos os itens especificados no grupo, mesmo que, caso necessário, seja feita a composição de diferentes ferramentas. Logo, além de ser um imperativo técnico, não há qualquer impedimento ou restrição do ponto de vista do mercado de fornecedores para que os itens venham a ser prestados por uma única empresa.

2.5.5. Do ponto de vista da eficiência técnica, a contratação em um único grupo é mais vantajosa, pois permite a plena integração entre os componentes da solução de microssegmentação, garantindo visibilidade centralizada dos ativos de rede e controle granular de acessos, bem como a aplicação automatizada de políticas de segmentação de tráfego. A integração entre os módulos da solução viabiliza o mapeamento detalhado das dependências entre aplicações e fluxos de dados, além da resposta automatizada a incidentes de segurança, como tentativas de movimentação lateral e ataques de ransomware.

2.5.6. Por se tratar de uma solução composta por múltiplos serviços interdependentes — como licenciamento para servidores, endpoints e clusters Kubernetes, implantação técnica, suporte contínuo e treinamento da equipe — a contratação conjunta se mostra fundamental para assegurar a qualidade das entregas e o desempenho adequado da solução como um todo. Isso otimiza recursos, facilita a gestão contratual em um único ponto e reduz o tempo de resposta em caso de falhas, contribuindo diretamente para a continuidade operacional e o aumento da resiliência cibernética da instituição.

2.5.7. Não há prejuízo à ampla competitividade, uma vez que existem diversos fornecedores no mercado capazes de ofertar a solução de forma integrada, conforme as especificações técnicas e regulatórias exigidas.

2.5.8. Conforme deliberações do TCU sobre a matéria, como a decisão que afirma que “A aquisição de itens diversos em lotes deve estar respaldada em critérios justificantes”, adotando o entendimento do Acórdão nº 5260/2011, de 06/07/2011, que decidiu que “Inexiste ilegalidade na realização de pregão com previsão de adjudicação por lotes, e não por itens, desde que os lotes sejam integrados por itens de uma mesma natureza e que guardem correlação entre si”.

2.5.9. Fundamenta-se ainda na necessidade de integração entre os componentes geridos por uma única empresa contratada, reduzindo o tempo de resposta caso ocorram problemas e proporcionando maior efetividade e entrega de informações integradas que consolidem os resultados dos diversos

componentes implantados.

2.5.10. Resta claro que o agrupamento dos itens em lote único não é opcional, mas sim, rigorosamente necessário para uma manutenção efetiva das licenças de software e serviços exclusivos ao software adquirido, não cabendo, assim, dividir o fornecimento do objeto em lotes distintos.

2.6. **ALINHAMENTO AO PLANEJAMENTO ESTRATÉGICO INSTITUCIONAL:**

2.6.1. O objeto da contratação está em alinhamento aos seguintes Objetivos Estratégicos do Mapa Estratégico da PCDF, parte integrante do Programa Avançar – 3º Ciclo (2024-2027), que orienta os programas, projetos, ações, atividades, indicadores e metas de gestão, assim como a elaboração dos demais planos e a identificação de oportunidades de inovação da Polícia Civil do Distrito Federal.

OBJETIVOS ESTRATÉGICOS – PEI/PCDF 2024-2027		
Perspectiva	ID	Objetivos Estratégicos Institucionais
Gestão	OEI 01	Aprimorar a Governança com foco na gestão por resultados
Estrutura	OEI 03	Aprimorar o uso da Tecnologia da Informação e Comunicação
Servidor	OEI 06	Desenvolver equipe de alta performance

2.6.2. Está também em conformidade com a Lei nº 7.378, de 29 de dezembro de 2023, que dispõe sobre o Plano Plurianual do Distrito Federal para 2024-2027, com o Programa Temático nº 6217 - DF mais seguro, referente ao eixo temático Segurança, em alinhamento aos objetivos:

ID	Objetivo – Programa Temático 6217
332	Enfrentamento qualificado da criminalidade aumentar a sensação de segurança por meio do enfrentamento qualificado da criminalidade, priorizando a redução da violência contra a mulher, dos crimes violentos letais intencionais e dos crimes contra o patrimônio.
334	Prevenção da violência com enfoque em grupos vulneráveis - atuar na prevenção da violência e implementar ações voltadas a grupos vulneráveis.
335	Fortalecimento da governança e inteligência na segurança pública - Racionalizar os recursos disponíveis para o combate à criminalidade, como foco em inteligência e estratégia

2.6.3. O PPA 2024-2027 do DF foi elaborado em conformidade com o Plano Estratégico do Distrito Federal 2019-2060, com os Objetivos de Desenvolvimento Sustentáveis – ODS, definidos pela Organização das Nações Unidas, e com o Plano Diretor de Ordenamento Territorial – PDOT, conforme preconiza o § 2º do art. 149 da Lei Orgânica do Distrito Federal.

2.7. **ALINHAMENTO AO PDTIC DA PCDF 2024-2027:**

2.7.1. O objeto da contratação encontra-se alinhado também aos objetivos estratégicos de TIC a seguir especificados:

Objetivos Estratégicos Institucionais de Tecnologia da Informação e Comunicação - OETIC	
OETIC1	Ampliar a Abrangência Estratégica de TIC
OETIC2	Evoluir a Maturidade de Governança, Gestão de TIC e Segurança da Informação
OETIC3	Aprimorar e documentar Processos Internos de TIC

2.7.1. O projeto atende à necessidade e à ação abaixo descritas, previstas no PDTIC da PCDF:

Necessidade	Ação
N4 - Gestão da segurança da informação	A96 - Contração de solução de segurança para microssegmentação.

2.7.2. **Alinhamento ao Plano Anual de Compras e Contratações – PACC**

2.7.2.1. O objeto da contratação não está previsto no Plano Anual de Compras e Contratações da PCDF para o ano de 2026. Contudo, a sua inclusão já foi solicitada no Despacho 194375128.

2.7.2.2. Conforme descrito na Nota Informativa 6 (194510773), o pedido foi registrado em lista de demandas pendentes de análise, com vistas à sua posterior apreciação na reunião trimestral de revisão do PACC.

3. **DEFINIÇÃO E ESPECIFICAÇÃO DE REQUISITOS DA CONTRATAÇÃO**

3.1. **REQUISITOS DE NEGÓCIO**

3.1.1. A Polícia Civil do Distrito Federal conforme definido no Mapa Estratégico Corporativo – 2024 a 2027, necessitará de ferramentas, pessoas e tecnologias adequadas para suportar o conjunto de atividades que necessita desempenhar visando atender a sociedade do Distrito Federal.

3.1.2. Nesse sentido, com vistas a garantir um serviço de qualidade à população do Distrito Federal, a Polícia Civil vem ao longo dos anos desenvolvendo e disponibilizando sistemas e soluções de Tecnologia da Informação e Comunicação cada vez mais eficientes aos cidadãos, seus usuários internos, bem como aos Órgãos parceiros como TJDF, Ministério Público, Detran/DF, SSP/DF, DPF, entre outros.

3.1.3. Para alcançar os objetivos acima descritos, a Instituição utiliza como balizadores o Plano Diretor de Segurança da Informação-PDTIC e a Política de Segurança da Informação-PSI, documentos estratégicos que estão alinhados entre si, buscando garantir o uso seguro, eficiente e eficaz da tecnologia da informação.

3.1.4. O Plano Diretor de Tecnologia da Informação e Comunicação da Polícia Civil do Distrito Federal-PDTIC/PCDF é o documento estratégico utilizado para planejar, organizar e direcionar as ações de Tecnologia da Informação e Comunicação em consonância com os objetivos estratégicos institucionais na PCDF, a fim de atender às demandas de alta qualidade dos serviços prestados à sociedade.

3.1.5. A Política de Segurança da Informação da PCDF-PSI foi publicada por meio da Resolução n.º 01 de 10 de agosto de 2022 visando estabelecer na estrutura organizacional da Instituição, princípios e diretrizes que visam manter a conformidade com as disposições legais vigentes para assegurar a confidencialidade, a disponibilidade e a integridade de suas informações.

3.1.6. No contexto orgânico da PCDF, a Divisão de Tecnologia – DITEC é responsável pelo processamento das Ocorrências e Inquéritos Policiais, Mandados de Prisão, Alvarás de Soltura, Registros de Identificação Civil e Criminal, além da automação de mais de 100 (cem) Unidades Policiais e a salvaguarda de informações relevantes e sigilosas que devem ser protegidas com a utilização de técnicas e equipamentos confiáveis capazes de prover a disponibilidade e a integridade das informações.

3.1.7. No âmbito da DITEC, o Serviço de Segurança em Tecnologia da Informação - SSTI tem como atribuição principal atuar na elaboração de planos e metas relacionadas à Segurança em Tecnologia da Informação em conformidade com o previsto pela Política de Segurança da Informação, assim como prestar auxílio na implantação, no monitoramento e na aplicação de melhorias desses recursos.

3.2. REQUISITOS TÉCNICOS

3.2.1. As necessidades tecnológicas, também conhecidas como requisitos da solução de tecnologia, descrevem as características de uma solução que atenda aos requisitos do negócio. A solução pretendida deve atender aos seguintes requisitos técnicos:

3.2.1.1. Deverá assegurar a microssegmentação da rede corporativa como medida para aumentar a segurança do ambiente.

3.2.1.2. Deverá permitir a visualização do fluxo de aplicativos – descobrir automaticamente os fluxos de aplicativos em toda a rede e mapear as cargas de trabalho até o nível do processo.

3.2.1.3. Deverá proteger o tráfego leste/oeste (movimentação lateral), reduzindo a superfície de ataque e os riscos associados ao movimento lateral no ambiente.

3.2.1.4. Deverá analisar de forma automatizada uma ameaça de ataque – Inteligência de ataque de alta fidelidade, incluindo ferramentas, táticas e fontes dos invasores.

3.2.1.5. Deverá possuir funcionalidades de Resposta a incidentes – Recomendações de isolamento e correção de ataques que aceleram a resposta a incidentes.

3.2.1.6. Deverá implementar camada de defesa contra ransomware tanto para o ambiente atual, quanto para futuras expansões.

3.2.1.7. Deverá permitir a descoberta de máquinas e aplicativos.

3.2.1.8. Deverá permitir a criação de grupos de segurança para cada uma das diferentes camadas de aplicativos (ou seja, servidores web/aplicativos/bancos de dados etc.).

3.2.1.9. Deverá permitir a criação de uma política rígida entre os diferentes grupos de segurança, de forma que apenas as portas necessárias para o bom funcionamento do aplicativo sejam abertas.

- 3.2.1.10. Deverá enviar as violações de políticas e incidentes de segurança detectados, em tempo real, para a solução de SIEM.
- 3.2.1.11. Deverá ser compatível com sistemas legados, garantindo que não haja interrupções nas operações.
- 3.2.1.12. Deverá garantir interoperabilidade com outras ferramentas de segurança já em uso pela Instituição.
- 3.2.1.13. Deverá ser escalável para suportar o crescimento futuro da Instituição, tanto em quantitativo de usuários quanto de novos sistemas e aplicativos.
- 3.2.1.14. Deverá desenvolver alto nível de desempenho mesmo com o aumento do tráfego e da complexidade das políticas de segmentação.
- 3.2.1.15. Deverá garantir abordagem de segurança que forneça proteção para aplicativos, a nível de processos, web e nuvem para usuários remotos.
- 3.2.1.16. Deverá assegurar a realização de testes de segurança e constante evolução do nível de proteção das soluções de endpoint e rede.
- 3.2.1.17. Deverá permitir a verificação de comportamento do tráfego em tempo real.
- 3.2.1.18. Deverá permitir que qualquer ajuste ou configuração das funcionalidades dos módulos da solução que requeiram integração com ferramentas externas seja realizado de forma nativa ou através do uso de APIs.
- 3.2.1.19. Deverão ser observados e aplicados minimamente, nos casos em que qualquer módulo da solução obrigatoriamente necessite ser hospedado ou utilize recursos em nuvem, os requisitos legais que constam no item 7.1 – Requisitos Legais.
- 3.2.1.20. As exigências acima se justificam com a busca de mitigar o risco de exposição indevida de informações ou de ataques que reduzam a disponibilidade dos Sistemas da PCDF, serviços estes que são indispensáveis para segurança do Distrito Federal.

3.2.2. **Restrições Técnicas**

- 3.2.2.1. Não serão aceitas soluções que sejam “Forks” de projetos de software existentes, ou seja, versões derivadas que tenham sido modificadas a partir do código fonte original.
- 3.2.2.2. Essa restrição visa garantir a integridade, o suporte contínuo e a segurança da solução adotada.
- 3.2.2.3. O objetivo da restrição é assegurar que a solução implementada possa:
- 3.2.2.4. Receber atualizações regulares e suporte oficial, minimizando riscos associados a vulnerabilidades de segurança e garantindo a continuidade operacional;
- 3.2.2.5. Manter a compatibilidade com outros sistemas e padrões tecnológicos, evitando problemas de interoperabilidade que possam surgir a partir de versões modificadas de softwares originais;
- 3.2.2.6. Estar em conformidade com as políticas de licenciamento e propriedade intelectual, assegurando que não ocorram infrações legais ou contratuais decorrentes do uso de versões não autorizadas ou modificadas de softwares.
- 3.2.2.7. Serão consideradas apenas as soluções que utilizem versões oficiais e não modificadas dos softwares, garantindo conformidade com os padrões estabelecidos e assegurando a qualidade e a confiabilidade da implementação.

3.2.3. **Demais Requisitos Necessários e Suficientes à Escolha da Solução de TIC**

- 3.2.3.1. A contratada deverá se submeter à Política de Segurança da Informação (PSI) da PCDF, nos termos da Resolução Nº 01 de 10 de agosto de 2022.
- 3.2.3.2. Conformidade Regulatória: Caso o contrato envolva solução que utilize computação em nuvem, a CONTRATADA deverá rigorosamente cumprir e comprovar as cláusulas de segurança estabelecidas na Norma de Gestão de Computação em Nuvem da PCDF, Seção III – Da Utilização e Contratação de Serviços em Nuvem, Art. 12. que solicita:

3.2.3.2.1. Garantia por parte da CONTRATADA de que os serviços ofertados estejam alinhados à legislação brasileira, bem como aos direitos à privacidade, à proteção dos dados pessoais e ao sigilo tanto das comunicações privadas, quanto dos registros das operações.

3.2.3.2.2. Os dados, metadados, informações e conhecimentos produzidos ou custodiados pela PCDF deverão ser hospedados preferencialmente em território brasileiro, com as exceções a isso sendo tratadas em procedimentos específicos.

3.2.3.2.3. No caso das exceções, as informações sobre as localizações geográficas onde os dados são armazenados, processados e transmitidos devem ser registradas para que seja possível determinar as entidades regulatórias e as jurisdições aplicáveis.

3.2.3.3. A CONTRATADA deverá assegurar que todos os serviços e soluções de computação em nuvem fornecidos estejam em conformidade com as com as normas e regulamentos aplicáveis ao setor de segurança pública, incluindo, mas não se limitando a Lei Nº 13.709/2018 - LGPD, o Marco Civil da Internet, normas de segurança da informação ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018.

3.2.3.4. Propriedade Intelectual e Dados: o contrato deve garantir que a PCDF mantenha a propriedade dos dados e que os mesmos estejam protegidos contra acessos não autorizados, inclusive pelo fornecedor da solução.

3.3. REQUISITOS DE MANUTENÇÃO, GARANTIA E SUPORTE TÉCNICO

3.3.1. O suporte técnico deverá ser prestado pelo período de 12 (doze) meses contados a partir da data de recebimento definitivo e contemplar a prestação dos serviços a seguir:

3.3.1.1. Para o suporte técnico a Contratada deverá disponibilizar uma central de atendimento, incluindo sítio na internet, telefone (preferencialmente 0800) e e-mail, para abertura de chamados para suporte e manutenção, consultas, envio de arquivos para análise, durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano;

3.3.1.2. Os chamados de suporte técnico deverão ser apresentados em sítio na internet, permitindo à CONTRATANTE o acompanhamento/evolução das informações relacionadas ao histórico dos atendimentos;

3.3.1.3. Nas atividades relacionadas ao atendimento do suporte técnico deverá ser empregada a língua portuguesa falada e escrita do Brasil;

3.3.1.4. A solicitação de suporte técnico deverá contemplar o esclarecimento de dúvidas, orientações no uso do software, configurações, instalação/desinstalação de funcionalidades da ferramenta, além de solução de problemas detectados pela equipe técnica da CONTRATANTE,

3.3.1.5. As atividades relacionadas ao suporte técnico deverão ser realizadas por profissionais certificados pelo fabricante, em razão da complexidade dos serviços a serem prestados;

3.3.1.6. Não haverá limitação para o número de chamados técnicos;

3.3.1.7. As atualizações de versão que ocorrerem durante a vigência contratual, deverão ser fornecidas automaticamente, sem ônus adicional para a CONTRATANTE;

3.3.1.8. Os serviços de manutenção compreendem as manutenções preventivas e corretivas, de forma que a solução esteja sempre em condições de funcionamento;

3.3.1.9. A CONTRATADA deverá garantir a atualização dos microcódigos, firmwares, drivers e softwares instalados, provendo o fornecimento de novas versões por necessidade de correção de problemas ou por implementação de novos releases, a partir do recebimento definitivo pela contratante, durante o período de garantia;

3.3.1.10. Caso seja necessário substituir licenças equivalentes durante a vigência do Contrato, isso deverá ocorrer sem qualquer ônus para a CONTRATANTE;

3.3.1.11. Os serviços deverão contemplar a resolução de qualquer problema nas licenças e serviços descritos neste documento, sem nenhum ônus adicional para a CONTRATANTE.

3.4. REQUISITOS DE TREINAMENTO

3.4.1. Deverá ser fornecido treinamento oficial pelo fabricante em português, com duração

mínima de 20 horas para cada turma alocada.

3.4.2. O treinamento deverá ser ministrado por profissional com certificação oficial do fabricante.

3.4.3. O treinamento ofertado deverá abordar todos os componentes da solução fornecida, devendo ainda estar de acordo com a utilização da solução instalada no ambiente da CONTRATANTE.

3.4.4. A CONTRATADA deverá prover treinamento para 5 (cinco) participantes, com 20 (vinte) horas de carga horária mínima, respeitando o limite de 4 (quatro) horas por dia, contemplando a utilização de todos os módulos da solução contratada.

3.4.5. O treinamento será efetuado em até 30 dias a contar emissão do TRD – Termo de Recebimento Definitivo.

3.4.6. Deverá utilizar como base a solução implementada na CONTRATANTE, visando facilitar os casos práticos.

3.4.7. O treinamento deverá ser realizado no horário compreendido entre 14h00 e 18h00, em dias úteis, podendo haver alteração, a critério da CONTRATANTE, em comum acordo com a CONTRATADA.

3.4.8. O treinamento deverá ser realizado presencialmente, nas dependências da CONTRATANTE, em data a ser definida em comum acordo com a CONTRATANTE.

3.4.8.1. A CONTRATANTE poderá excepcionalmente, a seu critério, aceitar que o treinamento seja realizado de forma remota.

3.4.9. A CONTRATANTE disponibilizará laboratório com computadores e acesso à internet para a realização do treinamento.

3.4.10. À exceção da disponibilização do laboratório, todas as despesas decorrentes do treinamento, tais como pagamentos aos instrutores, diárias, confecção do material didático, ferramentas, etc., serão de exclusiva responsabilidade da CONTRATADA.

3.4.11. O treinamento provido pela CONTRATADA será submetida à aprovação por parte dos alunos, conforme ficha de avaliação item 3.4.17.

3.4.12. Caso o treinamento seja avaliado como INSATISFATÓRIO, será realizado novo treinamento para a turma, sem ônus à CONTRATANTE:

3.4.12.1. A critério da CONTRATANTE, o conteúdo poderá ser ajustado e/ou o instrutor substituído para sanar os problemas identificados.

3.4.12.2. O novo treinamento deverá acontecer segundo um novo calendário, a ser definido pela CONTRATANTE.

3.4.13. Todo o material utilizado para o treinamento deverá ser disponibilizado aos alunos em mídia eletrônica removível ou e-mail, em formatos padrão de mercado (PDF, DOC ou PPT). A CONTRATANTE se reserva o direito de reproduzir trechos do material didático utilizado no treinamento, desde que registradas as devidas fontes, para realizar capacitações internas a seus servidores e colaboradores.

3.4.14. A CONTRATADA deverá confeccionar certificado de participação do curso aos participantes que obtiverem no mínimo 75% de presença.

3.4.15. A CONTRATADA deverá enviar à CONTRATANTE a lista de presença, assinada pelo instrutor, em que seja comprovada a participação dos treinandos, por meio de suas assinaturas em cada dia da capacitação.

3.4.16. Para fins de comprovação dos serviços prestados, visando o faturamento, a CONTRATADA deverá encaminhar à CONTRATANTE, em até 5 (cinco) dias úteis após o encerramento da turma, os certificados e o documento de presença digitalizados.

3.4.17. **Avaliação do curso**

3.4.17.1. O treinamento de que trata este tópico será avaliado pelos técnicos da DITEC/DGI/PCDF, sendo que no caso de avaliação não satisfatória, deverá a CONTRATADA providenciar novo curso adequado às exigências e necessidades técnicas e didáticas para um aproveitamento satisfatório por parte

dos técnicos inscritos;

3.4.17.2. O cálculo final da média de avaliação será feito pela soma das notas de cada uma das fichas de avaliação dividido pelo número de participantes. No caso de avaliação rejeitada (média final da avaliação inferior a 5), deverá a CONTRATADA providenciar novo curso adequado às exigências e necessidades técnicas e didáticas para um aproveitamento satisfatório por parte dos técnicos inscritos.

3.4.17.3. **Modelo de Ficha de Avaliação**

Marque com um "X" o conceito que melhor representa sua opinião sobre este curso:
1 – Deficitário; 2 – Regular; 3 – Bom; 4 – Muito Bom; 5 – Excelente

Item de Avaliação	Itens de Verificação	Notas				
		1	2	3	4	5
1	Metodologia utilizada					
2	Distribuição da programação					
3	Desempenho dos instrutores					
4	Adequação da carga horária					
5	Contribuição para a melhoria da qualidade do seu trabalho					
6	Adequação do conteúdo das aulas ao objetivo do curso					
7	Aulas práticas					
8	Participação pessoal					
9	Material audiovisual					
10	Instalações das aulas práticas					
Nota Final da Ficha de Avaliação (Soma da nota de cada item / 5)						

Registre:
Aspectos positivos:

Aspectos negativos:

Sugestões:

3.5. **REQUISITOS TEMPORAIS**

3.5.1. A reunião inicial deverá ocorrer em, no máximo, 5 (cinco) dias úteis após a assinatura do Contrato.

3.5.2. As licenças da solução ofertada deverão ser disponibilizadas à CONTRATANTE em no máximo 15 (quinze) dias corridos, podendo ser prorrogado por igual período caso haja justificativa plausível, a partir do recebimento da Ordem de Fornecimento de Serviço.

3.5.3. Todos os eventos de trabalho que envolvam participação de integrantes da CONTRATADA em ambiente da CONTRATANTE, tais como manutenção corretiva de software, deverão ser realizadas em regime 24x7, salvo acordo entre as partes.

3.5.4. Os esclarecimentos solicitados pela fiscalização do contrato deverão ser prestados imediatamente pela CONTRATADA.

3.5.5. A CONTRATADA deverá atender aos chamados técnicos de acordo com o item 7.4 Níveis Mínimos de serviço exigidos no Termo de Referência.

3.5.6. O direito de atualização e suporte técnico das licenças, prestado diretamente pelo fabricante,

deverá ser de 12 (doze) meses, contados do recebimento definitivo da solução.

3.5.7. A CONTRATADA deverá prover garantia de 12 (doze) meses, contados do recebimento definitivo da solução.

3.5.8. O treinamento será efetuado em até 30 dias a contar emissão do TRD – Termo de Recebimento Definitivo.

3.6. **REQUISITOS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE**

3.6.1. A CONTRATADA compromete-se, tanto em nome próprio quanto de seus colaboradores, a observar e cumprir rigorosamente todas as políticas, normas e procedimentos de segurança da informação, mantendo total conformidade com os normativos vigentes na CONTRATANTE, bem como com aqueles que possam ser estabelecidos durante a vigência do contrato.

3.6.2. Deverá ser firmado TERMO DE CONFIDENCIALIDADE E MANUTENÇÃO DE SIGILO entre a CONTRATADA e a CONTRATANTE, conforme modelo em anexo neste documento.

3.6.3. O TERMO DE CONFIDENCIALIDADE E MANUTENÇÃO DE SIGILO deverá ser assinado pelo representante legal da CONTRATADA, após a assinatura do contrato, em que se responsabiliza pela manutenção de sigilo e confidencialidade das informações a que possa ter acesso em decorrência da contratação.

3.6.4. A CONTRATADA deverá apresentar, para cada representante, empregado ou colaborador que vier a executar atividades referentes ao objeto da contratação, TERMO DE CIÊNCIA, conforme modelo em anexo neste documento, em que seus profissionais declaram estar cientes das responsabilidades pela manutenção de sigilo e confidencialidade.

3.6.5. A CONTRATADA deverá assumir total responsabilidade por todas as informações, documentos e especificações técnicas acessadas por seus representantes, empregados e colaboradores, no decorrer de todas as fases da execução dos serviços, devendo ser consideradas, em todo o tempo, como estritamente confidenciais. Fica proibida sua reprodução, utilização ou divulgação a terceiros, cabendo à CONTRATADA garantir a preservação total do **sigilo** das informações obtidas em função dos serviços prestados, em conformidade com o Termo de Compromisso e Manutenção de Sigilo e com os Normativos de Segurança da Informação.

3.6.6. A CONTRATADA deverá ser responsável por qualquer transferência ou remanejamento de seus colaboradores diretamente envolvidos na execução dos serviços objeto da contratação. Caso isso ocorra, a CONTRATANTE deverá ser comunicada com antecedência mínima de 5 (cinco) dias úteis, sendo obrigação da CONTRATADA providenciar a revogação de todos os privilégios de acesso às informações e recursos da CONTRATANTE.

3.6.7. Os profissionais da CONTRATADA que necessitem ter acesso às instalações físicas ou ao ambiente de rede da CONTRATANTE deverão, além de assinar o TERMO DE CIÊNCIA, ter seus dados previamente apresentados à CONTRATANTE, para realização de cadastro e concessão das permissões necessárias.

3.6.8. Não será permitido, em hipótese alguma, a divulgação, cópia ou retirada de quaisquer dados que estejam nos sistemas e bases de dados da CONTRATADA para fins que não estejam estritamente relacionados à prestação dos serviços contratados.

3.7. **REQUISITOS SOCIAIS, AMBIENTAIS, CULTURAIS E DE SUSTENTABILIDADE**

3.7.1. A CONTRATADA deverá adotar práticas de sustentabilidade ambiental na execução do objeto, quando couber, conforme disposto na Instrução Normativa SLTI/MPOG, Instrução Normativa nº 01/2010, de 19 de janeiro de 2010.

3.7.2. A CONTRATADA deverá adotar práticas de sustentabilidade ambiental na execução dos serviços, em consonância à Lei Distrital nº 4.774/2012, que dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens e na contratação de obras e serviços pelo Distrito Federal.

3.7.3. Deverá também estar aderente ao Plano de Logística Sustentável da PCDF, 3ª edição, vigente até 2027, disponível em <https://www.pcdf.df.gov.br/institucional/gestao-estrategica/9128/pls>.

3.7.4. É dever do CONTRATADO adotar na execução do contrato, práticas de sustentabilidade

ambiental, a recepção de bens, embalagens, recipientes ou equipamentos inservíveis e não reaproveitáveis pelo Incra, práticas de desfazimento sustentável, reciclagem dos bens inservíveis e processos de reutilização que sejam aplicáveis ao objeto desta licitação.

3.7.5. A utilização de tecnologias de virtualização, as quais podem ser definidas como soluções computacionais que permitem a execução de vários sistemas operacionais e seus respectivos softwares a partir de uma única máquina física, gera benefícios como melhor aproveitamento da infraestrutura existente, a redução no consumo de energia elétrica e menor emissão de carbono.

3.7.6. Os serviços prestados pela CONTRATADA deverão pautar-se sempre no uso racional de recursos e equipamentos, de forma a evitar e prevenir o desperdício de insumos e material consumidos, bem como a geração excessiva de resíduos, a fim de atender às diretrizes de responsabilidade ambiental adotadas pelo Governo do Distrito Federal e pela PCDF.

3.7.7. A CONTRATADA deve respeitar as Normas Brasileiras – NBR, publicadas pela ABNT, sobre resíduos sólidos.

3.7.8. Sem prejuízo aos demais critérios de sustentabilidade aplicados, a CONTRATADA deverá ainda observar os critérios estabelecidos na legislação ambiental.

3.8. REQUISITOS LEGAIS

3.8.1. **Lei nº 14.133, de 01 de abril de 2021** – estabelece normas gerais de licitação e contratação para as Administrações Públicas diretas, autárquicas e fundacionais da União, dos Estados, do Distrito Federal e dos Municípios;

3.8.2. **Lei nº 13.709, de 14 de agosto de 2018** – Lei Geral de Proteção de Dados Pessoais (LGPD).

3.8.3. **Decreto nº 3.555, de 08 de agosto de 2000** – aprova o regulamento para a modalidade de licitação denominada pregão, para a aquisição de bens e serviços comuns;

3.8.4. **Decreto nº 3.555, de 08 de agosto de 2000** – aprova o regulamento para a modalidade de licitação denominada pregão, para a aquisição de bens e serviços comuns;

3.8.5. **Decreto nº 7.845, de 14 de novembro de 2012** – regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

3.8.6. **Lei Distrital nº 4.611, de 09 de agosto de 2011** - regulamenta no Distrito Federal o tratamento favorecido, diferenciado e simplificado para microempresas, empresas de pequeno porte e microempreendedores individuais de que trata a Lei Complementar Federal nº 123, de 14 de dezembro de 2006, as Leis Complementares nº 127, de 14 de agosto de 2007, e nº 128, de 19 de dezembro de 2008, e dá outras providências;

3.8.7. **Lei Distrital nº 4.770, de 22 de fevereiro de 2012** – dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens e na contratação de obras e serviços pelo Distrito Federal;

3.8.8. **Decreto Distrital nº 38.934, de 15 de março de 2018** – dispõe sobre a aplicação, no âmbito da Administração Pública Direta e Indireta do Distrito Federal, da Instrução Normativa nº 05, de 25 de maio de 2017, da Secretaria de Gestão do Ministério do Planejamento, Desenvolvimento e Gestão;

3.8.9. **Decreto Distrital nº 44.330, de 16 de março de 2023** – Regulamenta a Lei Federal nº 14.133, de 1º de abril de 2021, Lei de Licitações e Contratos Administrativos, no âmbito da Administração Pública direta, autárquica e fundacional do Distrito Federal;

3.8.10. **Instrução Normativa SGD/ME nº 94/2022, de 23 de dezembro de 2022** – Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISF do Poder Executivo Federal.

3.8.11. **Parecer Referencial SEI-GDF n.º 066/2024 - PGDF/PGCONS** – Opinativo que tece considerações acerca da instrução da fase interna da licitação que tenha por finalidade a contratação de solução de tecnologia da informação e comunicação.

4. DESCRIÇÃO DA SOLUÇÃO

4.1. IDENTIFICAÇÃO DA SOLUÇÃO

4.1.1. **Composição básica da solução:** Solução de Microsegmentação.

4.1.2. **Detalhamento da solução:** Contratação de empresa para fornecimento de Solução de Segurança para Microsegmentação de rede, incluindo instalação, implantação, treinamento, garantia e suporte técnico, por 12 (doze) meses, conforme especificações detalhadas.

4.2. BENS E SERVIÇOS QUE COMPÕEM A SOLUÇÃO

ITEM	DESCRIÇÃO	Qtd
1	Fornecimento de Solução de segurança para microsegmentação de ambiente corporativo com licenciamento para Servidores	516
2	Fornecimento de Solução de microsegmentação de ambiente corporativo com licenciamento para Endpoints	5000
3	Fornecimento de Solução de microsegmentação de ambiente corporativo com licenciamento para Kubernetes	21
4	Serviço de Instalação da solução	1
5	Serviço de Treinamento para 5 pessoas	5

4.3. ESPECIFICAÇÕES TÉCNICAS

4.3.1. **Solução de Segurança para Microsegmentação para ambiente de servidores, estações de trabalho e Kubernetes (Itens 1, 2 e 3)**

4.3.1.1. Características Gerais

4.3.1.1.1. Deverá suportar a microsegmentação tanto em dispositivos físicos quanto em dispositivos virtualizados (independente da tecnologia utilizada para virtualização).

4.3.1.1.2. Deverá ser licenciado para todos os servidores, estações de trabalho e kubernetes, objeto da contratação.

4.3.1.1.3. Deverá possibilitar a criação de ilhas no ambiente, onde os ativos tenham sua comunicação restrita (tráfego Leste-Oeste/Norte-Sul), apenas ao que for previamente identificado e liberado, principalmente no contexto de aplicações, que devem ter sua comunicação liberada apenas no contexto estritamente necessário.

4.3.1.1.4. Toda a solução deverá ser gerenciada por uma console única de gerência centralizada, para todos os tipos de ativos especificados anteriormente. Serão aceitas exceções em casos de integrações com soluções de terceiros, quando especificado.

4.3.1.1.5. Toda a solução deverá ser do mesmo fabricante, sem qualquer tipo de customização não autorizada pelo mesmo.

4.3.1.1.6. A solução não poderá ser baseada em ferramentas open source.

4.3.1.1.7. Deverá ser oferecido retenção mínima de 45 dias para todos os dados enviados para a console, incluindo os fluxos de rede coletados, permitindo através desses fluxos a construção de mapas com retenção de pelo menos 90 dias;

4.3.1.1.8. Deverá suportar, minimamente, a instalação de agentes nos seguintes sistemas operacionais:

4.3.1.1.8.1. Amazon Linux;

4.3.1.1.8.2. CentOS Linux: 5.2 (32 bits), 5.2 até 5.11 (64 bits), 6 até 9 (64 bits);

4.3.1.1.8.3. Oracle Linux: 5.2 até 5.11, 6 até 9 (todos 64 bits);

4.3.1.1.8.4. Red Hat Linux: 5, 5.1, 5.2 até 5.11, 6, 7 e 8 (todos 64 bits);

4.3.1.1.8.5. Debian Linux: 7.5 até 12 (todos 64 bits);

4.3.1.1.8.6. Ubuntu Linux: 12.04 até 22.04 LTS (todos 64 bits);

4.3.1.1.8.7. Windows Server 2003 SP2 (32 e 64 bits), 2008 (32 bits), 2008 R2, 2012, 2016, 2016 Core, 2019 e 2022;

- 4.3.1.1.8.8. Windows Desktop: 7 (32 e 64 bits), 8 (32 e 64 bits), 8.1 (32 e 64 bits), 10 (32 e 64 bits) e 11;
- 4.3.1.1.8.9. MacOS 11 ou superior.
- 4.3.1.1.9. No caso de dispositivos que não possam receber os agentes, a solução deverá disponibilizar um mecanismo que permita cadastrar os mesmos e criar regras para ditar como estes recursos podem interagir com a rede protegida.
- 4.3.1.1.10. Deverá suportar a segmentação de ambientes em contêineres, atendendo minimamente as seguintes plataformas e tecnologias relacionadas:
- 4.3.1.1.10.1. Orchestration Platforms;
- 4.3.1.1.10.2. AWS Elastic Kubernetes Service (EKS);
- 4.3.1.1.10.3. Azure Kubernetes Service (AKS);
- 4.3.1.1.10.4. Kubernetes;
- 4.3.1.1.10.5. OpenShift;
- 4.3.1.1.10.6. Rancher Kubernetes Engine (RKE);
- 4.3.1.1.10.7. Container Runtime;
- 4.3.1.1.10.8. Containerd;
- 4.3.1.1.10.9. Docker;
- 4.3.1.1.10.10. CRI-O;
- 4.3.1.1.10.11. Network Plugins;
- 4.3.1.1.10.12. Kubenet;
- 4.3.1.1.10.13. Azure CNI;
- 4.3.1.1.10.14. Calico;
- 4.3.1.1.10.15. OVN-Kubernetes (OVN);
- 4.3.1.1.10.16. Canal.
- 4.3.1.1.11. Ser capaz de visualizar todo o fluxo de dados dos PODs no mesmo mapa de fluxo de dados, ou seja, o mapa de fluxo de dados deverá ser único para Servidores, Desktops, Cloud Workload e PODs.
- 4.3.1.1.12. Ser possível configurar regras de controle para comunicações no ambiente. Estas regras deverão também ser baseadas em etiquetas.
- 4.3.1.1.13. Deverá também refletir de forma automática, qualquer alteração de metadados e labels do cluster, ajustando as regras de segmentação já criadas.
- 4.3.1.1.14. Deverá apresentar informações de comunicação entre os PODs, incluindo qual o processo (container) que originou ou recebeu a comunicação, a porta e o protocolo utilizado, além da imagem e linha de comando utilizada, suportando a identificação de uso indevido dentro da plataforma de kubernetes.
- 4.3.1.1.15. Deverá apresentar o fluxo de dados leste-oeste e norte-sul (comunicação de e para a internet).
- 4.3.1.1.16. A solução não deve gerar nenhum tipo de impacto ou atraso na subida de recursos do ambiente de kubernetes (PODs, Serviços e Etc).
- 4.3.1.1.17. Deverá ser independente de hardware, ou seja, funcionar em qualquer infraestrutura de rede composta pela compatibilidade requirida já especificada.
- 4.3.1.1.18. Não deverá ser necessário qualquer parada (downtime) dos servidores ou aplicações, incluindo, mas não se limitando:
- 4.3.1.1.18.1. Reinício (Reboot) dos ativos, sejam servidores, estações de trabalho ou Nodes;
- 4.3.1.1.18.2. Alteração de IPs, Nomes, configurações de rede em geral, dos ativos;

- 4.3.1.1.18.3. Alteração da infraestrutura de rede, seja ela física ou virtual.
- 4.3.1.1.18.4. A solução deverá suportar IPv4 e IPv6;
- 4.3.1.1.19. Deverá ser capaz de monitorar todos os fluxos de tráfego do Datacenter: Leste-Oeste (servidor-servidor) e Norte-Sul (rede cliente-servidor ou servidor-externa, ou seja, internet). Ou seja, a solução deve monitorar os fluxos de tráfego de todos os ativos que possuem agentes instalado, incluindo o fluxo entre máquinas virtuais em execução no mesmo hipervisor, ativos de tipos diferentes, comunicação entre nuvem pública com datacenter privado, entre outros.
- 4.3.1.1.20. A solução também deverá permitir a criação de regras de filtragem de comunicação entre distintos tipos de ativos, bem como entre distintos tipos de ambientes;
- 4.3.1.1.21. A solução deverá manter registro de todos os Fluxos de Ativos, incluindo os que não foram bloqueados bem como aqueles que falharam (ex.: Timeout).
- 4.3.1.1.22. Toda a comunicação interna entre os componentes da solução deve ser completamente criptografada e autenticada.
- 4.3.1.1.23. A solução deverá possuir no mínimo as seguintes certificações de segurança: ISO 27001, ISO 27018 e SSAE 16 Type 2 (SOC2).
- 4.3.1.2. **Arquitetura e implementação**
- 4.3.1.2.1. Não serão aceitas soluções que sejam “Forks” de projetos de software existentes, ou seja, versões derivadas que tenham sido modificadas a partir do código fonte original.
- 4.3.1.2.2. Caso a solução suporte o modelo de serviço de nuvem (SaaS), a mesma deverá estar hospedada em um dos principais fornecedores de nuvem pública como Amazon, Google ou Microsoft, geograficamente localizada em território brasileiro, não sendo permitido sobre qualquer circunstância a transferência dos dados coletados para fora do território brasileiro.
- 4.3.1.2.3. A plataforma SaaS do fornecedor deve possuir certificação SOC 2 Tipo 2 emitido por auditor independente.
- 4.3.1.2.4. Para garantir os dados da PCDF, o ambiente em nuvem deverá ser dedicado para este Órgão. Nenhuma informação deverá ser compartilhada, incluindo os IPs e FQDNs de acesso da console de gerenciamento, bem como todos os outros componentes na nuvem do fabricante da solução.
- 4.3.1.2.5. A Console de Gerenciamento deverá ser única e centralizada para toda a Solução.
- 4.3.1.2.6. Os agentes deverão se comunicar diretamente com a plataforma SaaS sem a necessidade de agregadores caracterizando-se assim uma aplicação de duas camadas.
- 4.3.1.2.7. O agente deverá suportar a utilização de servidores proxies caso o seguimento de rede não possua comunicação direta com a internet.
- 4.3.1.2.8. Os componentes administrativos da solução não deverão possuir dependência de nenhum outro componente de rede ou infraestrutura para o seu perfeito funcionamento.
- 4.3.1.2.9. A implementação do agente deverá ser compatível com ferramentas de deployment de software de uso geral como SCCM, Chef, Ansible, Puppet ou outra que seja passível de execução de um script shell ou PowerShell.
- 4.3.1.2.10. A solução deverá utilizar agentes instalados nos ativos protegidos, responsável por coletar fluxos de dados e garantir a aplicabilidade das regras configuradas;
- 4.3.1.2.11. Deverá proporcionar a instalação do agente de forma manual, através de msi e scripts já elaborados e disponibilizados pelo fabricante da solução.
- 4.3.1.2.12. O agente deverá suportar a opção de auto proteção contra remoção, cabendo ao administrador habilitar ou desabilitar esta opção via console de gerenciamento.
- 4.3.1.2.13. O processo de instalação, atualização ou remoção dos agentes da solução não deverá exigir a reinicialização de dispositivos.
- 4.3.1.2.14. Deverá possibilitar a implementação dos agentes em modo apenas de monitoramento, fornecendo visibilidade do tráfego para que o administrador da solução criar regras e planejar a mudança

para modo bloqueio com visibilidade e contexto de todo o tráfego de rede.

4.3.1.2.15. A solução deverá permitir a criação de políticas, fornecendo apenas a visibilidade e impacto das mesmas, para posterior provisionamento da mesma e enforcement das regras.

4.3.1.2.16. Deverá permitir integração via SAML 2.0 com IDPs externos, como no mínimo o Microsoft Azure AD\Entra, possibilitando autenticação na console administrativa a partir de um usuário gerenciado internamente pela CONTRATANTE.

4.3.1.2.17. Deverá possuir auditoria para rastreamento de todas as modificações realizadas na console administrativa.

4.3.1.2.18. Deverá possibilitar a capacidade de filtragem de tráfego com base em aplicações, rótulos, ambientes, período de tempo, status da política, etc. Permitindo ainda exportação dos logs para consumo externo a ferramenta.

4.3.1.2.19. Não deverá haver limitação de número de regras e quantidade de tráfego a ser analisado pela ferramenta.

4.3.1.2.20. A comunicação entre o agente e a console central deverá ser criptografada.

4.3.1.2.21. Deverá possuir capacidade de etiquetamento de todos os ativos, incluindo os que possuem agentes ou outros ativos sem agentes, mas que se comunicaram ou receberam comunicação de um ativo protegido pela solução;

4.3.1.3. **Características da Console de Gerenciamento**

4.3.1.3.1. A console deverá ser única para toda a solução de microssegmentação;

4.3.1.3.2. Ter a capacidade de gerenciar todos os tipos de ativos (servidores, cloud, estações de trabalho e Kubernetes) em uma única console;

4.3.1.3.3. Ter a capacidade de visualizar os fluxos de dados e configurar as políticas de segurança em uma única console;

4.3.1.3.4. Possuir um Dashboard com as principais informações referentes ao ambiente;

4.3.1.3.5. Ter a capacidade de visualizar em modo gráfico, através de mapas, os fluxos de dados do ambiente;

4.3.1.3.6. Visualizar todos os ativos protegidos, incluindo informações como Nome, Sistema Operacional e IP;

4.3.1.3.7. Ter a capacidade de visualizar todas as etiquetas associadas a um único dispositivo;

4.3.1.3.8. Ter a capacidade de visualizar todos os ativos para uma única etiqueta;

4.3.1.3.9. Deve ser possível filtrar os fluxos de comunicação de dados, no mínimo em:

4.3.1.3.9.1. Bloqueado ou Permitido;

4.3.1.3.9.2. Origem: por etiqueta e nome do ativo;

4.3.1.3.9.3. Destino: por etiqueta e nome do ativo;

4.3.1.3.9.4. Comunicações com Origem ou Destino para a Internet;

4.3.1.3.9.5. Pelo nome do conjunto de regras de proteção aplicado no ambiente;

4.3.1.3.9.6. Porta e Protocolo;

4.3.1.3.9.7. Período de tempo;

4.3.1.3.9.8. Por processo utilizado da comunicação;

4.3.1.3.9.9. Ser possível criar novas etiquetas e gerenciar etiquetas existentes;

4.3.1.3.9.10. Exportar as etiquetas, no mínimo em CSV ou XLS;

4.3.1.3.9.11. Ter a capacidade, através de interface gráfica na própria console, de monitorar a saúde de todos os componentes da solução, no mínimo para os agentes e Clusters Kubernetes.

4.3.1.3.9.12. Ter a capacidade, através de interface gráfica na própria console, de parar e reiniciar os

componentes da solução, no mínimo para os agentes, coletores e servidores de Relay, ou possuir proteção nativa contra parada dos agentes, reiniciando automaticamente em caso de erro.

4.3.1.3.9.13. Ter a capacidade de atualizar os agentes instalados nos ativos de forma centralizada pela própria console, sem necessitar de execução manual no ativo ou de uso de scripts.

4.3.1.3.10. Deve possuir Logs de Auditoria, para no mínimo:

4.3.1.3.10.1. Autenticação do usuário: Com sucesso e falha de autenticação;

4.3.1.3.10.2. Política de Segmentação: Criação e alteração de políticas, bem como a ação de desabilitar a política;

4.3.1.3.10.3. Etiquetas: Criação e alteração;

4.3.1.3.10.4. Logs: Quem consultou os logs;

4.3.1.3.11. Os Logs de Auditoria devem conter, no mínimo: O dia, hora, Ação Executada, Nome do usuário, IP de Origem e Descrição;

4.3.1.3.12. Deve ser possível gerenciar os usuários com acesso a solução, não havendo limites para o número de usuários existentes;

4.3.1.3.13. Deve possuir integração com sistemas de diretório para integração de autenticação. Deve ser compatível com mínimo com LDAP e SAML 2.0;

4.3.1.3.14. Deve suportar autenticação Kerberos;

4.3.1.3.15. Deve ser possível criar usuários locais, e gerenciar os usuários existentes.

4.3.1.3.16. Deve suportar segundo fator de autenticação;

4.3.1.3.17. Possuir níveis de permissões diferentes para os usuários, no mínimo com as seguintes características:

4.3.1.3.17.1. Administrador da solução;

4.3.1.3.17.2. Somente Leitura;

4.3.1.3.17.3. Somente visualização dos Incidentes;

4.3.1.3.17.4. Administração das Políticas;

4.3.1.3.18. Ser possível verificar todos os incidentes gerados pela solução diretamente na própria console de administração;

4.3.1.3.19. Deve ser possível customizar o nível de criticidade dos incidentes;

4.3.1.3.20. Deve ser possível trabalhar com múltiplos sites, em console única e que permitam aos usuários aplicar seletivamente políticas e regras a um conjunto de ativos nessa localização;

4.3.1.3.21. Deve ser possível ao administrador total autonomia para criar, modificar e excluir regras, além de visualizar todos os logs para Ativos atribuídos aos seus sites.

4.3.1.4. **Características do Agentes**

4.3.1.4.1. A solução deverá possuir agentes instalados nos ativos protegidos;

4.3.1.4.2. Os agentes deverão ser compatíveis com as seguintes plataformas, no mínimo:

4.3.1.4.2.1. Windows Server 2003 SP2 (32 e 64 bits), 2008 (32 bits), 2008 R2, 2012, 2016, 2016 Core, 2019 e 2022;

4.3.1.4.2.2. Windows Desktop: 7 (32 e 64 bits), 8 (32 e 64 bits), 8.1 (32 e 64 bits), 10 (32 e 64 bits) e 11;

4.3.1.4.2.3. MacOS 11 ou superior;

4.3.1.4.2.4. Red Hat Linux: 5, 5.1, 5.2 até 5.11, 6, 7 e 8 (todos 64 bits);

4.3.1.4.2.5. CentOS Linux: 5.2 (32 bits), 5.2 até 5.11 (64 bits), 6 até 9 (64 bits);

4.3.1.4.2.6. Oracle Linux: 5.2 até 5.11, 6 até 9 (todos 64 bits);

- 4.3.1.4.2.7. Alma 8 e 9 (64bits);
- 4.3.1.4.2.8. Amazon Linux;
- 4.3.1.4.2.9. Amazon Linux 2;
- 4.3.1.4.2.10. Ubuntu Linux: 12.04 até 22.04 LTS (todos 64 bits);
- 4.3.1.4.2.11. Debian Linux: 7.5 até 12 (todos 64 bits);
- 4.3.1.4.2.12. SUSE Linux: 11, 12 e 15 (todos 64 bits);
- 4.3.1.4.2.13. Solaris: 10.8 até 10.11 (x86_64 e SPARCv9), 11 até 11.4 (x86_64 e SPARCv9);
- 4.3.1.4.2.14. AIX: 6.1, 7.1, 7.2 e 7.3;
- 4.3.1.4.2.15. Rocky 8 e 9 (64bits);
- 4.3.1.4.3. Para Containers e Kubernetes, a solução deverá atuar como um DaemonSet em todos os Nós do Cluster;
- 4.3.1.4.4. Deverá coletar todos os fluxos de dados de comunicação entre PODs, bem como origem e/ou destino de infraestrutura não baseada em micro serviço;
- 4.3.1.4.5. Os agentes deverão consumir no máximo 5% de CPU;
- 4.3.1.4.6. Os agentes deverão ser capazes de coletar informações do ativo, como flows de rede, e executar as políticas de proteção;
- 4.3.1.4.7. As políticas de proteção deverão permanecer em execução mesmo que o ativo não tenha acesso a Console de Gerenciamento;
- 4.3.1.4.8. Os agentes deverão armazenar os Logs de Fluxo de Dados e Incidentes mesmo que o ativo não tenha acesso a Console de Gerenciamento;
- 4.3.1.4.9. Caso os agentes não sejam uma implementação nativa de Firewall e dependam do Firewall do Sistema Operacional, deverão atender os seguintes requerimentos mínimos:
 - 4.3.1.4.9.1. Deverá estender as capacidades técnicas do Firewall do Sistema Operacional, não se limitando somente a versão nativamente existente, devendo atender aos itens técnicos deste documento;
 - 4.3.1.4.9.2. Deverá possuir controles nativos da solução que evitem alteração nas políticas definidas pelo administrador da solução de microssegmentação;
 - 4.3.1.4.9.3. Deverá possuir controles nativos que impeçam a parada do Firewall do Sistema Operacional;
 - 4.3.1.4.9.4. Bloquear caso o administrador da rede, ou do sistema operacional, tente efetuar alterações manuais nas regras de firewall diretamente no próprio Sistema Operacional;
 - 4.3.1.4.9.5. Bloquear caso outra solução, como um Antivírus ou EDR, tente efetuar a parada ou desinstalação do Firewall nativo do sistema operacional;
 - 4.3.1.4.9.6. Bloquear a tentativa de parada, desinstalação ou comprometimento do Firewall nativo do Sistema Operacional em casos de ataques;
 - 4.3.1.4.9.7. O Fabricante da solução de Microssegmentação deverá garantir a atualização, ou mecanismos de contorno/proteção, em caso de conhecidas e/ou publicação de novas vulnerabilidades existente no Firewall nativo do Sistema Operacional;
 - 4.3.1.4.9.8. Deverá suportar o uso do agente da solução em conjunto com o Firewall Nativo do Sistema Operacional, ou de terceiros, exceto em casos de Limitação do Sistema Operacional;
- 4.3.1.4.10. Os agentes deverão capturar todos os Fluxos de Dados nos ativos instalados e enviar para a console de gerenciamento.
- 4.3.1.4.11. As informações capturadas pelo agente deverão conter no mínimo:
 - 4.3.1.4.11.1. IP de Origem e Destino;
 - 4.3.1.4.11.2. Hostname de Origem e Destino;

- 4.3.1.4.11.3. Porta e Protocolo;
- 4.3.1.4.11.4. Quantidade de conexões;
- 4.3.1.4.11.5. Hora e Data;
- 4.3.1.4.11.6. Informações do processo/binário responsável pela comunicação, na origem e destino;
- 4.3.1.4.11.7. Caminho do binário no ativo;
- 4.3.1.4.11.8. Nome do Serviço do Windows (Ex.: BITS) responsável pela comunicação, quando este for executado em um processo padrão (Ex.: SVCHost.exe);
- 4.3.1.4.11.9. Usuário que executou o processo;
- 4.3.1.4.11.10. FQDN ou IP, quando for um acesso com origem ou destino para Internet;
- 4.3.1.4.11.11. A instalação do agente não deverá requerer qualquer tipo de parada no Sistema Operacional, incluindo reiniciar (Reboot);
- 4.3.1.4.12. A instalação do agente não deverá requerer qualquer tipo alteração no ativo, como mudança de IP, Hostname, ou instalação de software que possam comprometer o funcionamento normal da aplicação;
- 4.3.1.4.13. Os agentes deverão ter a capacidade de coletar informações dos ativos que estão instalados, como exemplo, mas não se limitando: Processos em execução, uptime do sistema, entre outros;

4.3.1.5. **Características de Visibilidade**

- 4.3.1.5.1. A solução deverá, a partir da instalação dos agentes, fornecer um mapa de dependência de aplicativos em tempo real de como a comunicação de rede está acontecendo, de forma a proporcionar o completo entendimento dos administradores para uma melhor tomada de decisão.
- 4.3.1.5.2. Além do mapa visual de comunicações, a solução ainda deverá fornecer meios para filtragem específica de comunicações em modo de log na console, contendo no mínimo os detalhes de origem, destino, portas, protocolos e aplicações internas que realizaram a comunicação.
- 4.3.1.5.3. Deverá possuir, no mapa de rede, filtros de inclusão e exclusão, permitindo filtrar no mínimo:
 - 4.3.1.5.3.1. IP;
 - 4.3.1.5.3.2. Porta;
 - 4.3.1.5.3.3. Aplicação, Binário e Serviço;
 - 4.3.1.5.3.4. Nome do Ativo;
 - 4.3.1.5.3.5. Tipo de Conexão - Estabelecida, bloqueada e as que violaram uma política;
 - 4.3.1.5.3.6. Internet - Com Origem e Destino da Internet;
 - 4.3.1.5.3.7. Usuário que iniciou o processo;
- 4.3.1.5.4. A tela do Mapa de Dados deve possuir mecanismo de busca;
- 4.3.1.5.5. Deve reter os fluxos de dados por um mínimo de 45 dias, sendo possível criar ou visualizar os mapas utilizando períodos históricos;
- 4.3.1.5.6. O mapa de dados deverá apresentar informações de comunicação em Camada 4 e Camada 7;
- 4.3.1.5.7. Deverá ser possível verificar as Etiquetas aplicadas a um ativo diretamente da tela do Mapa de Dados;
- 4.3.1.5.8. Ser possível identificar a quantidade de vezes que uma determinada comunicação aconteceu em um período de tempo;
- 4.3.1.5.9. Ser possível, no mapa de dados, obter informações do processo que efetuou uma determinada comunicação, possuindo no mínimo informações do Caminho do Binário no Ativo, o usuário que executou o processo e a linha de comando executada;

- 4.3.1.5.10. Deve ser possível, no mapa de dados, visualizar as comunicações de todos os ativos do ambiente, máquina a máquina;
- 4.3.1.5.11. Deve ser possível, no mapa de dados, agrupar os ativos através das etiquetas existentes no ambiente, permitindo ainda hierarquizar em subgrupos;
- 4.3.1.5.12. Deve registrar e apresentar todos os fluxos de comunicação do datacenter, em formato de tabela, juntamente com informações contextuais e detalhadas sobre as cargas de trabalho e aplicativos (processos) de comunicação;
- 4.3.1.5.13. Deve fornecer recursos de filtragem (Ip/Porta/Processo/Origem/Destino/Usuário que iniciou a comunicação) se a comunicação foi estabelecida/bloqueada;
- 4.3.1.5.14. Deve descobrir automaticamente qualquer novo fluxo de comunicação em tempo real;
- 4.3.1.5.15. Deve ser possível filtrar os fluxos de dados por um conjunto de regras aplicados no ambiente;
- 4.3.1.5.16. Deve ser possível exportar os fluxos de dados no mínimo em CSV;
- 4.3.1.5.17. Deve ser possível visualizar todos os ativos, através da console, obtendo informações da primeira vez que foi visto e a última vez que o ativo se comunicou com a console;
- 4.3.1.5.18. Deverá ser possível etiquetar ou aplicar TAGs nos ativos do ambiente, ativos com agentes e sem agentes, para utilizar tanto na visualização, em políticas bem como em filtros;
- 4.3.1.5.19. A etiquetas deverão seguir um modelo de Categoria e Valores, por exemplo Ambiente / Produção, ou de forma similar onde é possível incluir valores diferentes para uma mesma categoria;
- 4.3.1.5.20. As etiquetas deverão ser criadas através da própria console de gerenciamento, no mínimo das seguintes formas:
- 4.3.1.5.20.1. Dinamicamente - Ex: Todo dispositivo que o nome contém PROD, ou que estão na subrede 10.0.0.0/8, aplicar Etiqueta Ambiente: Produção
- 4.3.1.5.20.2. Através de integração com CMDB - Coletar os dados diretamente da solução de CMDB utilizada;
- 4.3.1.5.20.3. Através de Integração com sistemas que já possuem TAGs - Como VMWare VCenter, Nuvens públicas (AWS, GCP, Azure, OCI), Kubernetes (Metadados dos clusters) e CSV;
- 4.3.1.5.20.4. Através de APIs públicas;
- 4.3.1.5.20.5. Deverá ser possível agrupar etiquetas em Grupos de Etiquetas, para uso nas políticas e outras partes da solução;
- 4.3.1.5.20.6. Deverá ser registrado em Log toda a criação, remoção ou modificação das etiquetas, informando no mínimo o usuário responsável, hora e data e a etiqueta alterada. Esses logs deverão ser acessíveis através da própria console de gerenciamento;
- 4.3.1.5.20.7. Deverá ser possível aplicar uma etiqueta a um único dispositivo, e também a um conjunto de dispositivos;
- 4.3.1.5.21. A console de gerenciamento deverá possuir uma área específica de informações dos ativos que devem apresentar todas as Etiquetas aplicadas ao ativo;
- 4.3.1.5.22. As etiquetas poderão ser utilizadas no Mapa de Visualizações de Fluxo de Dados e na criação de políticas;
- 4.3.1.5.23. Deverá apresentar no mapa de fluxo de dados os dispositivos gerenciados e não-gerenciados pela solução.
- 4.3.1.5.24. A visão detalhada dos logs deve permitir a criação de regras para fluxos detectados como bloqueados a partir de interação com os logs, apenas selecionando as comunicações desejadas.
- 4.3.1.5.25. A solução deve realizar sugestões inteligentes de como a regra deverá ser criada, de forma a facilitar a ação do administrador da ferramenta.
- 4.3.1.5.26. A visão detalhada do tráfego de rede deverá mostrar quais os processos do sistema

operacional foram responsáveis por aquela comunicação, permitindo ainda que as regras possam controlar essa comunicação apenas quando esse mesmo processo iniciar a comunicação, garantindo que aquela comunicação de fato corresponde a aplicação de origem para a plataforma do sistema operacional.

4.3.1.5.27. Os agentes da solução deverão alimentar continuamente a console central, de forma que o administrador de rede sempre tenha contexto atualizado sobre as comunicações que estão ocorrendo.

4.3.1.5.28. A visibilidade gerada pela solução deverá suportar conceitos de RBAC, ou seja, segmentar a possibilidade de controle e visibilidade na console baseado no nível de permissão atribuído ao administrador autenticado na plataforma.

4.3.1.5.29. Os dados de visibilidade deverão estar disponíveis para consulta na console por pelo menos 90 dias.

4.3.1.6. **Regras de segmentação e visibilidade**

4.3.1.6.1. A solução deverá fornecer a capacidade de criar, gerenciar e monitorar políticas de tráfego Leste-Oeste e Norte-Sul flexíveis até o nível de uma única carga de trabalho e aplicativo (processo ou serviço do MS Windows);

4.3.1.6.2. Deve permitir criar e monitorar políticas de comunicação de aplicativo a partir do mapa de visualização;

4.3.1.6.3. Deve suportar regras definidas sobre grupos de ativos de acordo com sua função ou etiquetamento;

4.3.1.6.4. Deve possuir no mínimo 2 (dois) tipos de regras:

4.3.1.6.4.1. Bloqueio e

4.3.1.6.4.2. Permissão

4.3.1.6.5. Deverá permitir a criação de regras de microsegmentação utilizando os seguintes parâmetros:

4.3.1.6.5.1. Etiquetas e Grupo de Etiquetas;

4.3.1.6.5.2. Ativo (nome do ativo);

4.3.1.6.5.3. IP/Subrede;

4.3.1.6.5.4. Aplicação / Processo do Windows (Ex.: BITS);

4.3.1.6.5.5. Grupo de usuários;

4.3.1.6.5.6. FQDN;

4.3.1.6.5.7. Internet (Comunicação vindo da Internet / Rede Interna);

4.3.1.6.5.8. Qualquer (Any).

4.3.1.6.6. Deverá possuir filtros de informações no gerenciamento das regras do ambiente;

4.3.1.6.7. Deve salvar as revisões de política e permitir a reversão para versões anteriores;

4.3.1.6.8. A solução deverá possuir nativamente modelos (templates) pré-definidos para aplicações conhecidas de mercado (Ex.: Active Directory), tendo o catálogo disponibilizado na própria console de gerenciamento;

4.3.1.6.9. Deverá possuir nativamente modelos (templates) pré-definidos para políticas de Prevenção de Ransomware;

4.3.1.6.10. Deverá sugerir a criação de regras de forma automática com base no fluxo histórico de comunicação das aplicações;

4.3.1.6.11. Deve poder sugerir políticas automaticamente de acordo com os dados coletados;

4.3.1.6.12. A solução deverá possuir mecanismos que através dos fluxos de dados históricos, possam sugerir a criação de regras de acesso;

4.3.1.6.13. Deve ser possível criar políticas com Lógicas de E e OU;

- 4.3.1.6.14. A solução deverá permitir a inclusão de listas de FQDNs, através de importação de arquivo, para serem utilizadas durante a consulta DNS em bloqueio ou liberação de acesso a sites específicos;
- 4.3.1.6.15. Deve permitir a criação de regras com usuários em ambientes VDI/Terminal/Citrix de forma a garantir que apenas determinados grupos do Active Directory possam chegar a determinados endereços e/ou aplicações na rede;
- 4.3.1.6.16. Deverá fornecer dados e contexto para detecção de tentativas de movimento lateral;
- 4.3.1.6.17. Deve registrar tentativas de violação da política e fornecer informações detalhadas sobre a violação da conexão, indicando inclusive qual processo iniciou a comunicação;
- 4.3.1.6.18. A solução deverá permitir a criação de etiquetas a serem aplicadas nas cargas de trabalho, de maneira que a identificação dos servidores e aplicações do ambiente sejam facilmente reconhecidos.
- 4.3.1.6.19. As etiquetas deverão suportar o conceito de escopo da rede, ou seja, produção, homologação e desenvolvimento, assim como a qual ambiente e localização o ativo está incluso.
- 4.3.1.6.20. As regras deverão ser criadas baseadas em dois critérios principais, sendo eles: Escopo interno, ou seja, apenas entre serviços pertencentes a mesma aplicação identificada ou também no contexto de escopo externo, no caso de aplicações diferentes que precisam de comunicação de rede entre si.
- 4.3.1.6.21. Todas as etiquetas e atributos definidos nos tópicos anteriores deverão estar disponíveis amplamente para criação de políticas, seja pelo papel que o ativo executa, ou aplicação representada, ambiente ou localização.
- 4.3.1.6.22. As regras deverão possibilitar a criação granular, baseado nas etiquetas e atributos solicitados, baseados em origem, destino, porta, protocolo, aplicação e processos do sistema operacional.
- 4.3.1.6.23. As regras deverão conseguir utilizar listas de IPs, sub redes, FQDNs, range de portas e portas customizadas para controles específicos.
- 4.3.1.6.24. Deverá suportar a utilização de portas dinâmicas, ou seja, baseado no processo do sistema operacional e não em um range específico.
- 4.3.1.6.25. A solução deverá permitir a duplicação de políticas por parte do administrador, de forma a facilitar o processo de criação de regras.
- 4.3.1.6.26. A solução deverá suportar a importação e exportação de políticas.
- 4.3.1.6.27. A solução deverá permitir a atribuição de políticas em grupos específicos de hosts ou em hosts específicos.
- 4.3.1.6.28. No caso de remoção do agente da solução, todas as regras criadas deverão ser imediatamente removidas.
- 4.3.1.6.29. A solução deverá possuir integração nativa com scanners de vulnerabilidade para controle contextual de ativos com base nas vulnerabilidades que ele possui.
- 4.3.1.6.30. Essa integração deverá permitir a ingestão de dados de, pelo menos, os seguintes fabricantes: Qualys e Tenable.
- 4.3.1.6.31. A solução deverá permitir integração com Active Directory para controle de regras de acesso baseado em grupos do Active Directory.
- 4.3.1.6.32. A solução deverá suportar meios para visualização de impacto das políticas antes de aplicação de modificações das mesmas.
- 4.3.1.6.33. A visibilidade da solução deverá permitir facilmente a identificação de quais tráfegos estão ocorrendo por qual política definida e até mesmo se não existe uma política para o tráfego identificado.
- 4.3.1.6.34. O enforcement de políticas e instalação do agente não deverá requerer nenhum tipo de modificação no kernel do sistema operacional.
- 4.3.1.6.35. A solução deverá suportar o controle de políticas para regras de inbound e outbound no firewall dos ativos protegidos.
- 4.3.1.6.36. Deverá ser possível a criação de regras para “isolamento” de ativos na rede, de forma que a comunicação dos mesmos seja restrita apenas ao que tenha sido previamente definido, impedindo, por

exemplo, que ativos contaminados por ameaças possam se comunicar na rede com os demais servidores do datacenter.

4.3.1.6.37. Deverá possibilitar a integração com recursos IPSEC nativos do sistema operacional para criptografar o tráfego entre componentes protegidos pela solução.

4.3.1.6.38. As políticas da solução deverão possibilitar a coexistência com políticas de firewall que já existam em determinados hosts protegidos

4.3.1.6.39. Deverá permitir a identificação e proteção do ambiente a partir de componentes que não tenham o agente instalado.

4.3.1.6.40. O agente da solução deverá se automonitorar quanto a falhas de processo ou eventos de adulteração e reiniciar, se necessário, para garantir a funcionalidade contínua.

4.3.1.6.41. O agente da solução deverá monitorar continuamente as regras aplicadas evitando assim que as mesmas sejam modificadas ou mesmo eliminadas (“anti tampering”).

4.3.1.6.42. O agente deverá ser protegido por uma senha adicional prevenindo a remoção acidental ou proposital do mesmo.

4.3.1.6.43. Deverá reter ao menos as 100 versões da política para rollback em caso de necessidade e remoção automática das versões mais antigas para melhorar o desempenho.

4.3.1.7. **Gestão de vulnerabilidades**

4.3.1.7.1. A solução deverá possuir integração nativa com scanners de vulnerabilidade para realizar o controle contextual de ativos com base nas vulnerabilidades identificadas nos mesmos.

4.3.1.7.2. Essa integração deverá permitir a ingestão de dados de, pelo menos, os seguintes fabricantes: Qualys e Tenable.

4.3.1.7.3. A solução deverá gerar visões específicas, a partir da ingestão de dados de vulnerabilidades, sobre como as portas e aplicações vulneráveis estão se comunicando na rede corporativa.

4.3.1.7.4. Deverá permitir, a partir da integração com scanners de vulnerabilidade, a coleta de metadados e a criação de etiquetas baseadas nas vulnerabilidades existentes

4.3.1.7.5. Quando não existir a possibilidade de correção da vulnerabilidade do ativo, a solução deverá fornecer sugestões de ajustes para regras de microssegmentação daquele ativo, de forma a mitigar o maior número possível de brechas do mesmo.

4.3.1.8. **API e integrações**

4.3.1.8.44. A solução deverá possuir uma API forte e bem documentada.

4.3.1.8.45. Via API deverá ser possível realizar operações em políticas e controlar os ativos da solução.

4.3.1.8.46. Deverá ser baseada em HTTP e ser compatível com métodos GET, PUT, POST e DELETE.

4.3.1.8.47. Deverá ser autenticada via chave a ser gerada no portal da solução.

4.3.1.8.48. Deverá possibilitar integração com ferramentas DevOps como Chef, Puppet, Ansible e SCCM.

4.3.1.8.49. Deverá possuir integração com ferramentas de SIEM, sendo no mínimo suportado as soluções QRadar, Splunk, Arcsight ou ElasticSearch.

4.3.1.8.50. Deverá possuir integração com ferramentas de análise de vulnerabilidades, para coleta de metadados e posterior criação de etiquetas baseadas nas vulnerabilidades existentes;

4.3.1.8.51. Deverá possuir integração com F5 BIG-IP;

4.3.1.8.52. Deverá possuir integração com Firewall Fortigate da Fortinet, ou permitir o uso de API, para envio de IPs maliciosos;

4.3.1.8.53. Deverá fornecer contexto de comunicação em tempo real contendo todas as informações de comunicação de rede;

4.3.1.8.54. Deverá permitir envio de relatórios por e-mail;

4.3.1.8.55. Deverá permitir a exportação de IOCs.

4.3.2. **Requisitos do Serviço de Instalação, implantação e suporte da solução de Microsegmentação de rede (para os itens 1, 2 e 3)**

4.3.2.1. Os serviços de instalação, configuração e documentação deverão ser executados pela equipe técnica da CONTRATADA;

4.3.2.2. O(s) profissional(is) técnico(s) da CONTRATADA responsável(is) pela execução dos serviços contratados deve(m) obrigatoriamente possuir os certificados do fabricante da solução.

4.3.2.3. **A implantação da solução deverá contemplar as seguintes fases:**

4.3.2.2.1. **Planejamento:** nesta etapa a CONTRATADA deverá realizar o planejamento do projeto, onde serão definidos os prazos por atividade, as pessoas envolvidas, a estratégia de implantação do serviço, o plano de testes, arquitetura da solução, bem como quaisquer outros itens que sejam necessários para a implantação do projeto.

4.3.2.2.2. **Documentação:** deverá ser entregue a documentação do projeto, conforme descrita a seguir, em formato, quantidade e datas a serem acordados entre as partes.

4.3.2.2.3. **Plano de Requisitos de Infraestrutura:** A CONTRATADA deverá, antes do início da execução das configurações, elaborar documentação técnica fundamentando todas as ações que serão realizadas.

4.3.2.2.4. Após a aprovação do planejamento pela CONTRATANTE, o processo de implantação será iniciado, levando-se em consideração o cumprimento dos prazos pactuados.

4.3.2.2.5. O suporte do desenvolvedor da solução deverá ser 24 horas, 7 dias por semana, 365 dias por ano durante toda a vigência do Contrato.

4.3.2.2.6. O fabricante deverá possuir, falando em língua portuguesa, um responsável dedicado por atuar em ações decorrentes durante o período do contrato, sendo um Facilitador de comunicação entre os times do fabricante, como o suporte por exemplo, e o time da CONTRATANTE. Também será responsável por realizar reuniões trimestrais de acompanhamento da evolução e uso da solução.

5. **PAPÉIS E RESPONSABILIDADES**

5.1. **Obrigações da CONTRATANTE:**

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

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

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

5.1.4. Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis;

5.1.5. Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em Contrato;

5.1.6. Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da Solução/Serviços que serão contratados;

5.1.7. Proporcionar todos os meios para que a CONTRATADA possa desempenhar os serviços objeto da contratação;

5.1.8. Efetuar os pagamentos devidos, de acordo com as normas orçamentárias, financeiras e contábeis do Distrito Federal;

5.1.9. Fornecer e colocar à disposição da CONTRATADA todos os elementos e informações que se fizerem necessários à execução dos serviços;

5.1.10. Notificar, formal e tempestivamente a CONTRATADA sobre as irregularidades observadas no cumprimento do contrato;

5.1.11. Notificar a CONTRATADA, por escrito e com antecedência, sobre multas e penalidades a serem aplicadas;

5.1.12. Permitir o acesso do pessoal técnico, devidamente identificado, necessário à execução dos serviços às instalações físicas onde serão executados os serviços, observando os preceitos legais, regulamentos e normas que disciplinam a segurança e o sigilo da informação e do ambiente;

5.1.13. Acompanhar, fiscalizar e avaliar a prestação dos serviços não obstante a fiscalização da CONTRATADA;

5.1.14. Fiscalizar e acompanhar a execução do contrato, de acordo com as obrigações assumidas no contrato e na sua proposta de preços, por meio dos servidores designados, não eximindo a contratada de suas obrigações por eventual omissão na fiscalização;

5.1.15. Rejeitar, no todo ou em parte, os serviços que sejam executados em desacordo com o Contrato, aplicando as penalidades cabíveis;

5.1.16. Colocar à disposição da CONTRATADA equipe responsável pela administração de sistemas e dados para acompanhamento;

5.1.17. Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte da contratada, com base em pesquisas de mercado, quando aplicável;

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

5.1.19. Fazer a transição contratual, quando for o caso.

5.2. **Obrigações da CONTRATADA:**

5.2.1. Comunicar à Administração, no prazo máximo de 12 (doze) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

5.2.2. Garantir o funcionamento e disponibilidade do objeto durante toda a vigência do contrato;

5.2.3. Indicar formalmente preposto apto a representá-la junto à contratante, que deverá responder pela fiel execução do contrato;

5.2.4. Atender prontamente quaisquer orientações e exigências do gestor do contrato, inerentes à execução do objeto contratual;

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

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

5.2.7. Fornecer, sempre que solicitado pelo Gestor do Contrato, os esclarecimentos e as informações técnicas pertinentes;

5.2.8. Manter, durante toda a execução do contrato, compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

5.2.9. Quando especificada, manter, durante a execução do Contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da Solução de Tecnologia da Informação;

5.2.10. Manter a produtividade ou a capacidade mínima de fornecimento da Solução de Tecnologia da Informação durante a execução do contrato;

5.2.11. Impor, a todos os serviços executados, rigoroso padrão de qualidade, segurança e eficiência, com estrita observância dos prazos;

5.2.12. Ceder os direitos de propriedade intelectual e direitos autorais da Solução de Tecnologia da Informação sobre os diversos artefatos e produtos produzidos ao longo do contrato, incluindo a documentação, os modelos de dados e as bases de dados, à Administração, quando aplicável;

5.2.13. Corrigir os serviços, desde que fique comprovada a existência de fato que impeça sua regular utilização, mesmo após o aceite, cuja a verificação da inconformidade dos serviços com a especificação do Termo de Referência fique comprovada ou até mesmo a substituição de material utilizado e não previsto;

5.2.14. Exigir que seus funcionários:

5.2.14.1. Apresentem-se e identifiquem-se ao responsável pela Unidade de lotação solução beneficiada pelo contrato, antes de iniciar a execução de qualquer serviço;

5.2.14.2. Usem crachá quando estiverem efetuando qualquer serviço na Unidade da CONTRATANTE;

5.2.14.3. Colaborem com os servidores da CONTRATANTE que forem acompanhar os serviços, fornecendo as informações pertinentes.

5.2.14.4. Levar imediatamente ao conhecimento da CONTRATANTE qualquer fato extraordinário ou anormal que ocorrer em suas áreas de trabalho, para adoção das medidas cabíveis;

5.2.15. Em nenhuma hipótese haverá vínculo empregatício dos funcionários da CONTRATADA com a CONTRATANTE;

5.2.16. Não permitir a utilização de qualquer trabalho do menor de dezesesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos; nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;

5.2.17. Responder por todos os encargos trabalhistas, previdenciários, fiscais e comerciais, resultantes da execução do objeto deste instrumento;

5.2.18. Responsabilizar-se por todos os impostos incidentes sobre o contrato, bem como as despesas gerais efetuadas por seus agentes de serviço;

5.2.19. Observar os preceitos legais, regulamentos e normas que disciplinam a segurança e o sigilo da informação e do ambiente da PCDF;

5.2.20. A inadimplência da licitante vencedora, com referência aos encargos sociais, comerciais e fiscais não transfere a responsabilidade por seu pagamento à Administração da PCDF, nem poderá onerar o objeto desta contratação, razão pela qual a licitante vencedora renuncia expressamente a qualquer vínculo de solidariedade, ativa ou passiva, com a PCDF.

5.2.21. Executar as obrigações contratuais conforme especificações deste Termo de Referência e de sua Proposta;

5.2.22. Informar prontamente ao CONTRATANTE sobre fatos e/ou situações relacionadas à prestação dos serviços contratados que representem risco ao êxito da contratação ou ao cumprimento de prazos exigidos além de responsabilizar-se pelo conteúdo e veracidade das informações prestadas, sob pena de incorrer em situações de dolo ou omissão e comunicar ao gestor do contrato, no prazo de 24 horas, qualquer ocorrência anormal que se verifique durante a prestação dos serviços;

5.2.23. Solicitar em tempo hábil, todas as informações de que necessitar para o cumprimento das suas obrigações contratuais, exceto aquelas que já forem de responsabilidade da CONTRATANTE fornecer, nos termos do instrumento contratual;

5.2.24. Não transferir a terceiros, por qualquer forma, nem mesmo parcialmente, as obrigações assumidas, nem subcontratar qualquer das prestações a que está obrigada;

5.2.25. Utilizar as melhores práticas, capacidade técnica, materiais, equipamentos, recursos humanos e supervisão técnica e administrativa, para garantir a qualidade do serviço e o atendimento às especificações contidas no Contrato;

5.2.26. Responsabilizar-se integralmente pela sua equipe técnica, primando pela qualidade, desempenho, eficiência e produtividade, visando à execução dos trabalhos durante todo o Contrato, dentro dos prazos estipulados, sob pena de ser considerada infração passível de aplicação de penalidades

previstas, caso os prazos e condições não sejam cumpridas;

5.2.27. A ação da fiscalização não exonera a CONTRATADA de suas responsabilidades contratuais;

5.2.28. A fiscalização exercida pela CONTRATANTE não exclui e nem reduz a responsabilidade da CONTRATADA, inclusive, por danos que possam ser causados ao CONTRATANTE ou a terceiros, por qualquer irregularidade decorrente de culpa ou dolo da CONTRATADA na execução do contrato;

5.2.29. Responsabilizar-se pelos vícios e danos decorrentes do produto, de acordo com os artigos 12, 13, 18 e 26, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

5.2.30. Aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessárias, nos termos do art. 125 da Lei 14.133/21.

6. MODELO DE EXECUÇÃO DO CONTRATO

6.1. Prazos e Condições de Entrega do objeto/execução do serviço

6.1.1. A CONTRATADA deverá prover garantia de 12 (doze) meses, contados do recebimento definitivo da solução.

6.1.2. O contratado terá o prazo de 10 (dez) dias úteis, contado a partir da data de sua convocação, para aceitar o Contrato, sob pena de decair do direito à contratação, sem prejuízo das sanções previstas.

6.1.3. A CONTRATADA deverá disponibilizar as licenças da solução ofertada, no prazo de máximo 15 (quinze) dias corridos, podendo ser prorrogado por igual período caso haja justificativa plausível, a partir do recebimento da Ordem de Fornecimento de Serviço.

6.1.4. Os serviços de suporte técnico, garantia e atualização de versões terão início a partir do recebimento definitivo da solução e vigorarão pelo período de 12 (doze) meses.

6.1.5. O treinamento será ministrado em até 30 dias após a emissão do TRD.

6.1.6. O gestor do contrato emitirá a Ordem de Serviço para a entrega dos bens especificados e/ou início da execução dos serviços.

6.1.7. A solução deverá ser entregue na Divisão de Tecnologia da Polícia Civil - DITEC, situada no SPO Conjunto A, Lote 23, Centro Tecnológico, Térreo – Complexo da PCDF – Brasília/DF, CEP: 70.610-907, contato pelo telefone (61) 3207-5023/4667 (SSTI/DITEC), ou poderá ser disponibilizada para a PCDF pela Internet, através do site do fabricante, quando viável.

6.1.8. A entrega/disponibilização com atraso sujeitará a CONTRATADA à multa moratória, conforme estabelecido no item 8 deste documento. A CONTRATANTE se reserva o direito de recusar o recebimento quando o atraso for superior a 30 (trinta) dias.

6.1.9. Caberá à equipe de fiscalização nomeada pela CONTRATANTE o acompanhamento das entregas e solicitação de eventuais penalidades.

6.1.10. A PCDF rejeitará, no todo ou em parte, os serviços executados em desacordo com os termos do Contrato.

6.2. Mecanismos Formais de Comunicação

6.2.1. São definidos como mecanismos formais de comunicação, entre a Contratante e a Contratada, os seguintes:

6.2.1.1. Ordem de Serviço;

6.2.1.2. Ata de reunião;

6.2.1.3. Ofício;

6.2.1.4. Sistema de abertura de chamados;

6.2.1.5. E-mail.

6.2.1.6. Outras formas de comunicação aplicáveis.

6.3. Manutenção de Sigilo e Normas de Segurança

6.3.1. A CONTRATADA ficará proibida de veicular e comercializar os produtos e informações geradas, relativas à prestação dos serviços, salvo se houver a prévia autorização por escrito da PCDF.

6.3.2. A CONTRATADA deverá manter sigilo absoluto sobre quaisquer dados, informações, códigos fonte ou artefatos contidos em quaisquer documentos/mídias de que venha a ter conhecimento durante a execução dos trabalhos, não podendo sob qualquer pretexto divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pela PCDF a tais documentos, sob pena de responsabilidade civil, penal e administrativa.

6.3.3. Poderá ser exigido do profissional da Contratada que tiver acesso aos sistemas/dependências da CONTRATANTE a assinatura de Termo de Responsabilidade e Sigilo, comprometendo-se a não divulgar nenhum assunto tratado nas dependências da PCDF ou a serviço desta, salvo se expressamente autorizado.

6.3.4. O profissional da Contratada que tiver acesso à estrutura computacional disponibilizada pela PCDF deverá assinar termo declarando estar ciente de que esta não poderá ser utilizada para fins particulares e que a navegação em sítios da Internet e as correspondências em meio eletrônico utilizando endereço da PCDF ou acessadas a partir dos seus equipamentos poderão ser auditadas.

6.3.5. O profissional da Contratada que prestar serviços na PCDF deverá assinar Termo de Compromisso declarando total obediência aos preceitos legais, regulamentos e normas que disciplinam a segurança e o sigilo da informação e do ambiente da PCDF vigentes, ou que venham a ser implantadas, a qualquer tempo, no âmbito da PCDF.

6.3.6. O Termo de Compromisso e Manutenção de Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal do Contratado, e Termo de Ciência, a ser assinado por todos os empregados do Contratado diretamente envolvidos na contratação, encontram-se nos ANEXOS.

6.4. Forma de pagamento

6.4.1. O pagamento será realizado após aceite da entrega do objeto, mediante apresentação da nota fiscal ou instrumento de cobrança equivalente correspondente aos serviços executados.

6.4.2. O pagamento será realizado após aceite da entrega do objeto, mediante apresentação da nota fiscal ou instrumento de cobrança equivalente correspondente aos serviços executados.

6.4.3. O pagamento será feito de acordo com as Normas de Execução Orçamentária, Financeira e Contábil do Distrito Federal, em parcela (s), mediante a apresentação de Nota Fiscal, liquidada até 30 (trinta) dias de sua apresentação, devidamente atestada pelo Gestor/Fiscal do Contrato e acompanhada da Certidão Negativa de Débitos emitida pelo INSS, do Certificado de Regularidade do Fundo de Garantia por Tempo de Serviço e Certidão de Regularidade com a Fazenda do Distrito Federal e da Certidão Conjunta Negativa de Débitos Relativos aos Tributos Federais e à Dívida Ativa da União, Certidão Negativa de Débitos Trabalhistas – CNDT (em www.tst.gov.br), em cumprimento à Lei nº 12.440/2011 e em observância ao Decreto nº 32.767/2011, visando comprovar a inexistência de débitos inadimplidos perante a Justiça do Trabalho.

6.4.4. Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como o prazo de validade, a data da emissão, os dados do contrato e do órgão contratante, o período respectivo de execução do contrato, o valor a pagar e eventual destaque do valor de retenções tributárias cabíveis.

6.4.5. A nota fiscal ou instrumento de cobrança equivalente deverá conter a descrição do objeto e quantitativo, em atendimento à Ordem de Fornecimento de Bens expedida, comprovado por meio de relatório ou listagem que será encaminhado ao Gestor do Contrato.

6.4.6. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que a Contratada providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao contratante.

6.4.7. Juntamente com a nota fiscal a Contratada deverá apresentar:

- 6.4.7.1. Documento comprovando a disponibilização das licenças no site da fabricante;
- 6.4.7.2. Outros documentos não listados, exigidos pelo Gestor do Contrato;
- 6.4.7.3. Documentação comprobatória da regularidade fiscal.
- 6.4.7.4. Outros documentos pertinentes.

6.4.8. Administração realizará consultas ao SICAF, STC/GDF, CEIS/CGU e ao CNJ (condenações cíveis por atos de Impropriedade Administrativa) para:

- 6.4.8.1. Verificar a manutenção das condições de habilitação exigidas no edital;
- 6.4.8.2. Identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas (IN nº 3, de 26 de abril de 2018).

6.4.9. Constatando-se, junto ao SICAF, a situação de irregularidade do contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da contratante.

6.4.10. Não havendo regularização ou sendo a defesa considerada improcedente, a contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

6.4.11. Persistindo a irregularidade, a contratante adotará as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.

6.4.12. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o contratado não regularize sua situação junto ao SICAF.

6.4.13. As multas que porventura forem aplicadas ao contratado serão, inicialmente, descontadas da garantia eventualmente prestada e, na hipótese de valor remanescente, debitadas nas parcelas a receber.

6.4.14. Quando o contratado não providenciar o reforço da garantia ou não revalidá-la, os pagamentos ficarão retidos até a regularização da situação.

6.4.15. Os pagamentos às empresas com sede ou domicílio no Distrito Federal, referentes a créditos de valores iguais ou superiores a R\$5.000,00, serão feitos, exclusivamente, mediante crédito em conta corrente, em nome do beneficiário junto ao Banco de Brasília S/A- BRB, na forma do Decreto-DF nº 32.767/2011, no prazo de 30 (trinta) dias corridos contados da data de apresentação pela Contratada da documentação fiscal correspondente devidamente atestada pelo executor do contrato, excluindo:

- 6.4.15.1. Os pagamentos a empresas vinculadas ou supervisionadas pela Administração Pública federal;
- 6.4.15.2. Os pagamentos efetuados à conta de recursos originados de acordos, convênios ou contratos que, em virtude de legislação própria, só possam ser movimentados em instituições bancárias indicadas nos respectivos documentos;
- 6.4.15.3. Os pagamentos a empresas de outros Estados da federação que não mantenham filiais e/ ou representações no DF e que venceram processo licitatório no âmbito deste ente federado.

6.4.16. Nenhum pagamento será efetuado ao contratado enquanto pendente de liquidação 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 (quando for o caso).

6.4.17. Nenhum pagamento será feito ao contratado caso o(s) serviço(s) seja(m) rejeitado(s) pela fiscalização do contrato, devendo esses serem refeito(s) pelo contratado de modo a obter a aprovação da fiscalização, quando for o caso.

6.4.18. Caso a Contratada seja optante pelo Sistema Integrado de Pagamento de Impostos e Contribuições (SIMPLES), deverá apresentar Declaração (modelo do Anexo IV da IN RFB nº 1234 de

11/01/2012, alterada pela IN RFB ° 1244 de 30/01/2012) juntamente com a Nota Fiscal ou Fatura. Não sendo optante, será efetuada a retenção de Impostos e Contribuições, observadas as disposições do Art. 64 da Lei 9.430/96 e Instrução Normativa SRF nº 539, de 25/04/2005 ou outra que por ventura vier a substituí-la.

6.4.19. O pagamento obedecerá ao cronograma de execução físico-financeira.

6.4.20. Quaisquer dúvidas poderão ser dirimidas na Divisão de Orçamento e Finanças – DOF/PCDF, localizada no SPO, Edifício Sede do Complexo da Polícia Civil do Distrito Federal, ou ainda pelo telefone (61) 3207-4058 ou pelo endereço eletrônico: dof@pcdf.df.gov.br.

7. MODELO DE GESTÃO DO CONTRATO

7.1. Critérios de Acompanhamento e Fiscalização do Contrato

7.1.1. O acompanhamento e a fiscalização da execução do Contrato serão realizados por servidores da CONTRATANTE, designados como Gestor e Fiscais Requisitante, Técnico e Administrativo do Contrato, os quais obedecerão às disposições de normas e resoluções internas do órgão, e ao contido no art. 33 da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022.

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

7.1.3. A reunião será realizada em conformidade com o previsto no inciso I do Art. 31 da [IN SGD/ME nº 94, de 2022](#), e ocorrerá em até 5 (cinco) dias úteis contados da data de assinatura do contrato, podendo ser prorrogada a critério da Contratante.

7.1.4. A pauta desta reunião observará, pelo menos:

7.1.4.1. Presença do representante legal da contratada, que apresentará o seu preposto;

7.1.4.2. Entrega, por parte da Contratada, do Termo de Compromisso e dos Termos de Ciência;

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

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

7.1.4.5. Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste termo de referência.

7.1.5. No recebimento do objeto observar-se-á a especificação técnica entregue com a prevista no Termo de Referência, conforme as especificações contidas no subitem 4.3. O recebimento provisório ficará a cargo dos fiscais técnico, administrativo ou setorial e o recebimento definitivo, do gestor do contrato ou da comissão designada pela autoridade competente., nos termos do art. 27 do Decreto Distrital nº 44.330/2023.

7.1.6. Para os serviços de suporte técnico e garantia, o fiscal técnico deverá acompanhar o atendimento das solicitações de chamado de suporte técnico para garantir o cumprimento da solução definitiva dentro dos limites e prazos estabelecidos nos Níveis Mínimos de Serviço (subitem 7.4).

7.1.7. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas neste Termo de Referência e no Contrato, e as normas do Decreto Distrital nº 44.330/2023, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

7.1.8. Caberá ao fiscal administrativo, dentre outras atividades, prestar apoio técnico e operacional ao gestor do contrato, com a realização das tarefas relacionadas ao controle dos prazos relacionados ao contrato e à formalização de apostilamentos e de termos aditivos, ao acompanhamento do empenho e do pagamento e ao acompanhamento de garantias e glosas, bem como examinar a regularidade no

recolhimento das contribuições fiscais, trabalhistas e previdenciárias e, na hipótese de descumprimento, relatar ao gestor do contrato para as providências pertinentes.

7.1.9. Os fiscais técnico e administrativo deverão auxiliar o gestor do contrato com as informações necessárias, na elaboração do documento comprobatório da avaliação realizada na fiscalização do cumprimento de obrigações assumidas pelo contratado, conforme o disposto no inciso VIII do caput do art. 23 Decreto Distrital nº 44.330/2023.

7.1.10. As comunicações entre o órgão ou entidade e o CONTRATADO devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

7.1.11. Quaisquer exigências da fiscalização, inerentes ao objeto da licitação, deverão ser prontamente atendidas pela CONTRATADA, sem quaisquer ônus para a CONTRATANTE.

7.1.12. O descumprimento total ou parcial das obrigações e responsabilidades assumidas pela CONTRATADA ensejará a aplicação de sanções administrativas, previstas neste Termo de Referência e na legislação vigente, podendo culminar em rescisão contratual.

7.1.13. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade da CONTRATANTE ou de seus agentes, gestores e fiscais.

7.2. Recebimento e Critérios de Aceitação do Objeto

7.2.1. As licenças descritas nos itens 1, 2 e 3 da tabela deverão ser disponibilizadas em, no máximo 15 (quinze dias) corridos, podendo ser prorrogado por igual período caso haja justificativa plausível, a partir do recebimento da Ordem de Fornecimento de Serviço.

7.2.2. A instalação e configuração da solução serão feitas pela equipe técnica da CONTRATADA.

7.2.3. O **Termo de Recebimento Provisório - TRP** da solução será emitido pela CONTRATANTE no prazo máximo de 10 (dez) dias úteis a contar da disponibilização das licenças no ambiente tecnológico da CONTRANTE, mediante a verificação da conformidade com as especificações técnicas definidas neste documento.

7.2.4. O **Termo de Recebimento Definitivo – TRD** da solução, será emitido ao final da instalação e configuração da solução no ambiente tecnológico da CONTRATADA, que se dará no prazo máximo de 30 (trinta) dias corridos após a emissão do TRP, e será classificado como ACEITO ou REJEITADO segundo os seguintes critérios:

7.2.4.1. **Aceito** – quando toda a solução estiver instalada e configurada no ambiente da PCDF, não cabendo nenhum ajuste, apenas a garantia de funcionamento e demais serviços associados, após a emissão do Termo de Recebimento Definitivo, que se dará no prazo de até 15 dias úteis a contar da finalização da instalação e configuração.

7.2.4.2. **Rejeitado** – quando o objeto contratado não for aceito pela PCDF, sujeitando-se a CONTRATADA às penalidades estabelecidas para o caso.

7.2.5. O recebimento definitivo do treinamento será classificado como ACEITO ou REJEITADO segundo os seguintes critérios:

7.2.5.1. **Aceito** – quando o serviço de treinamento cumprir devidamente todos os requisitos de capacitação previstos no subitem 3.4 deste TR;

7.2.5.2. **Rejeitado** – quando o serviço de treinamento técnico deixar de cumprir integralmente os requisitos de treinamento previstos no subitem 3.4 deste documento, sujeitando-se a CONTRATADA a fornecer novo treinamento.

7.2.6. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, por 30 (trinta) dias corridos, de forma justificada, quando houver necessidade de diligências para a aferição do atendimento das exigências deste instrumento.

7.2.7. No caso de controvérsia sobre a execução do objeto, 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 diz respeito à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

7.2.8. O prazo para a solução, pelo PCDF, 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.

7.2.9. O recebimento definitivo não excluirá a responsabilidade civil nem a responsabilidade ético-profissional pela perfeita execução do objeto.

7.3. NÍVEIS MÍNIMO DE SERVIÇO – NMS

7.3.1. Durante toda a vigência contratual, a CONTRATADA deverá disponibilizar para a CONTRATANTE todas as atualizações de versões, releases e patches dos softwares fornecidos.

7.3.2. Juntamente com as licenças, a CONTRATADA deverá entregar documentação comprobatória da contratação de suporte técnico junto ao fabricante da solução ofertada.

7.3.3. Será aplicada multa de 1% do valor total das licenças entregues por dia de não apresentação do documento que ateste que a CONTRATADA possui contrato de garantia/suporte com o fabricante das licenças vinculadas ao contrato com a PCDF.

7.3.4. O suporte técnico deverá ser prestado pelo fabricante da solução ou pela CONTRATADA, sempre em nome da CONTRATADA.

7.3.5. A contratação do suporte técnico junto ao fabricante não exime a CONTRATADA das responsabilidades contratuais.

7.3.6. **Os chamados técnicos serão categorizados nas severidades descritas abaixo, devendo ser atendidos nos prazos especificados:**

7.3.6.1. **Severidade CRÍTICA:** nível aplicado quando há comprometimento imediato do funcionamento da solução (indisponibilidade) da CONTRATANTE;

7.3.6.1.1. **Prazo de início de atendimento:** Até 01 (uma) hora.

7.3.6.1.2. **Prazo limite de resolução:** Até 24 (vinte e quatro) horas após abertura do chamado remoto

7.3.6.1.3. **Sanção em caso de não resolução no prazo determinado:** Glosa de 2% do valor do contrato, por ocorrência, em caso de descumprimento

7.3.6.2. **Severidade ALTA:** nível aplicado quando a funcionalidade principal é afetada ou ocorre degradação significativa do desempenho;

7.3.6.2.1. **Prazo de início de atendimento:** Até 04 (quatro) horas.

7.3.6.2.2. **Prazo limite de resolução:** Até 72 (setenta e duas) horas após abertura do chamado remoto.

7.3.6.2.3. **Sanção em caso de não resolução no prazo determinado:** Glosa de 1,5% do valor do contrato, por ocorrência, em caso de descumprimento

7.3.6.3. **Severidade NORMAL :** nível aplicado quando há perda parcial ou intermitente de funcionalidades não críticas da solução, sem há comprometimento imediato do seu funcionamento.

7.3.6.3.1. **Prazo de início de atendimento:** Até 8 (oito) horas.

7.3.6.3.2. **Prazo limite de resolução:** Até 8 (oito) dias após abertura do chamado remoto.

7.3.6.3.3. **Sanção em caso de não resolução no prazo determinado:** Glosa de 0,5% do valor do contrato, por ocorrência, em caso de descumprimento

7.3.6.4. **Severidade BAIXA :** nível aplicado quando há solicitação de esclarecimentos técnicos relativos às ocorrências, ao uso e ao aprimoramento dos serviços ofertados;

7.3.6.4.1. **Prazo de início de atendimento:** Até 24 (vinte e quatro) horas.

7.3.6.4.2. **Prazo limite de resolução:** Até 10 (dez) dias após abertura do chamado remoto.

7.3.6.4.3. **Sanção em caso de não resolução no prazo determinado:** Glosa de 0,25% do valor do contrato, por ocorrência, em caso de descumprimento

7.5. Garantia Contratual

7.3.7. Como garantia da execução plena do objeto e fiel cumprimento dos termos do contrato, a Contratada, de acordo com o disposto no art. 147 do Decreto nº 44.330/2023 e no art. 96 da Lei 14.133/2021, deverá prestar garantia contratual de 5% (cinco por cento) do valor contratado à Contratante, até 10 (dez) dias úteis após a assinatura do contrato, mediante comprovante de uma das seguintes modalidades:

- 7.3.7.1. Caução em dinheiro ou títulos da dívida pública;
- 7.3.7.2. Seguro – garantia;
- 7.3.7.3. Fiança Bancária, ou
- 7.3.7.4. Título de capitalização custeado por pagamento único.

7.3.8. A garantia nas modalidades caução e fiança bancária deverá ser prestada em até 15 (quinze) dias após a assinatura do contrato, prorrogável por igual período.

7.3.9. No caso de seguro-garantia, sua apresentação deverá ocorrer antes da assinatura do contrato, como condição indispensável para sua formalização.

7.3.10. A CONTRATADA deverá repor, no prazo de 15 (quinze) dias, o valor da garantia eventualmente utilizada pela CONTRATANTE.

7.3.11. A garantia prestada pela CONTRATADA deverá ser renovada a cada prorrogação, e deverá ser prestada por todo o prazo de execução do contrato, e mais 90 (noventa) dias após o término da vigência contratual, prazo este correspondente ao período de garantia da execução dos serviços, nos termos do art. 97, I da Lei nº 14.133/2021.

7.3.12. A garantia, qualquer que seja a modalidade escolhida, assegurará o pagamento de:

- 7.3.12.1. Prejuízo advindo do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;
- 7.3.12.2. Prejuízos diretos causados à Administração decorrentes de culpa ou dolo durante a execução do contrato;
- 7.3.12.3. Multas moratórias e punitivas aplicadas pela Administração à CONTRATADA;
- 7.3.12.4. Obrigações trabalhistas, fiscais e previdenciárias de qualquer natureza, não honradas pela CONTRATADA.

7.3.13. **Será considerada extinta a garantia:**

- 7.3.13.1. Com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da CONTRATANTE, mediante termo circunstanciado, de que a CONTRATADA cumpriu todas as cláusulas do contrato;
- 7.3.13.2. No prazo de 90 (noventa) dias após o término da vigência, caso a CONTRATANTE não comunique ocorrências detectadas até esse prazo.
- 7.3.13.3. Para prestação da garantia contratual, fica vedado à CONTRATADA, pactuar com terceiros (segurados, instituições financeiras, etc.), cláusulas de não ressarcimento ou não liberação do valor dado à garantia para o pagamento de multas por descumprimento contratual.

8. SANÇÕES APLICÁVEIS

8.1. Em atendimento ao disposto no art. 19, inciso IV da Instrução Normativa SGD/ME nº 94/2022, fica estabelecido que os licitantes estarão sujeitos às sanções administrativas previstas na Lei nº 14.133, de 2021, e às demais cominações previstas em regulamento específico que trata dos procedimentos de aplicação de sanções, resguardado o direito à ampla defesa e ao contraditório.

8.2. Com fundamento na Lei nº 14.133 de 2021, comete infração administrativa a CONTRATADA que:

- 8.2.1. Der causa à inexecução parcial do contrato;
- 8.2.2. Der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;
- 8.2.3. Der causa à inexecução total do contrato;
- 8.2.4. Ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;
- 8.2.5. Apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;
- 8.2.6. Praticar ato fraudulento na execução do contrato;
- 8.2.7. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- 8.2.8. Praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

8.3. Serão aplicadas a CONTRATADA que incorrer nas infrações acima descritas as seguintes sanções:

- 8.3.1. Advertência, quando o contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei nº 14.133, de 2021);
- 8.3.2. Impedimento de licitar e contratar, quando praticadas as condutas descritas nos subitens 8.3.2, 8.3.3 e 8.3.4, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);
- 8.3.3. Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nos subitens 8.3.5, 8.3.6, 8.3.7 e 8.3.8, bem como nos subitens 8.2.2, 8.2.3 e 8.2.4, que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei nº 14.133, de 2021).

8.4. **Multa:**

- 8.4.1. Moratória para o atraso na entrega do objeto ou obrigação acessória, calculada sobre a fração inadimplida do contrato, de 0,25% (vinte e cinco centésimos por cento) por dia ou hora de atraso, até o limite de 20% (vinte por cento). O atraso de até 10 (dez) dias úteis poderá ser relevado, desde que não tenha gerado grave risco à Administração ou à continuidade dos serviços da PCDF, conforme despacho fundamentado do fiscal do contrato;
- 8.4.2. No caso de atraso superior a 45 (quarenta e cinco) dias corridos e não havendo mais interesse no recebimento do objeto, o fiscal do contrato poderá requerer a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133, de 2021. Havendo interesse no recebimento, mesmo que em atraso superior a 45 (quarenta e cinco dias), caberá ao fiscal do contrato emitir relatório fundamentado;
- 8.4.3. Moratória de 0,05% (cinco centésimos por cento) por dia de atraso injustificado sobre o valor total do contrato, até o máximo de 3% (três por cento), pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia, quando exigida em edital. O atraso de até 5 (cinco) dias úteis poderá ser relevado, desde que não tenha gerado grave risco à Administração ou à continuidade dos serviços da PCDF.
- 8.4.4. Compensatória, no caso de inexecução parcial do contrato ou retardamento da execução ou entrega do objeto, infrações descritas nas alíneas 8.3.2 e 8.3.4 do subitem 8.3, de 0,5% (cinco décimos por cento) a 20% (vinte por cento) calculada sobre a fração inadimplida do contrato. Havendo grave risco ou dano à Administração ou ao funcionamento dos serviços da PCDF, a multa incidirá sobre o valor total do Contrato.
- 8.4.5. Compensatória, para a inexecução total do contrato, infração prevista na alínea 8.2.2 e 8.2.3 do subitem 8.2, de 20% (vinte por cento) do valor do Contrato. Havendo grave risco ou dano à Administração ou ao funcionamento dos serviços da PCDF, a multa será de até 30% (trinta por cento) do valor do contrato.

- 8.4.6. Para infração descrita na alínea 8.2.2 do subitem 8.2, a multa será de 10% a 50% do valor do Contrato.
- 8.4.7. Compensatória, para as infrações descritas nas alíneas 8.2.5 a 8.2.8 do subitem 8.2, de 20% (vinte por cento) a 30% (trinta por cento) do valor do Contrato;
- 8.4.8. A aplicação de multa de mora não impedirá que a administração a converta em compensatória e promova a rescisão unilateral do contrato com a aplicação cumulada de outras sanções;
- 8.4.9. A Administração pode, ad cautelam, efetuar a retenção do valor presumido da multa concomitantemente à instauração do regular procedimento administrativo sancionatório, no qual será assegurado à contratada o direito ao contraditório e à ampla defesa. Havendo provimento da defesa, o valor retido será devolvido em até 10 (dez) dias úteis.
- 8.5. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante (art. 156, §9º, da Lei nº 14.133, de 2021).
- 8.6. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei nº 14.133, de 2021).
- 8.7. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157, da Lei nº 14.133, de 2021).
- 8.8. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente (art. 156, §8º, da Lei nº 14.133, de 2021).
- 8.9. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 15 (quinze) dias úteis, a contar da data do recebimento da comunicação enviada pela autoridade competente.
- 8.10. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.
- 8.11. Na aplicação das sanções, serão considerados (art. 156, §1º, da Lei nº 14.133, de 2021):
- 8.11.1. A natureza e a gravidade da infração cometida;
 - 8.11.2. As peculiaridades do caso concreto;
 - 8.11.3. As circunstâncias agravantes ou atenuantes;
 - 8.11.4. Os danos que dela provierem para a CONTRATANTE;
 - 8.11.5. A implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.
- 8.12. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159).
- 8.13. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160, da Lei nº 14.133, de 2021).
- 8.14. O Contratante deverá, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal. (Art. 161, da

Lei nº 14.133, de 2021).

8.15. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/21.

8.16. Os débitos do contratado para com a Administração contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o contratado possua com o mesmo órgão ora contratante, na forma da Instrução Normativa SEGES/ME nº 26, de 13 de abril de 2022.

9. ESTIMATIVA DE CUSTOS

9.1. A metodologia utilizada para a composição dos preços e obtenção do preço de referência fundamentou-se nos arts. 99 a 104 do Decreto Distrital nº 44.330/2023, cujo detalhamento da pesquisa e dos cálculos constam na Estimativa de Custo e Orçamento 14 (188091105) e Memória de Cálculo (189017505), artefatos integrantes do processo de planejamento da contratação.

9.2. Com base nos valores obtidos, o preço de referência para contratação de serviços para fornecimento de Solução de Segurança para Microsegmentação, incluindo instalação, implantação, treinamento, garantia e suporte técnico por 12 (doze) meses, perfaz o total de **4.644.213,31 (quatro milhões, seiscientos e quarenta e quatro mil, duzentos e treze reais e trinta e um centavos)**, conforme demonstrado na tabela a seguir.

Item	Objeto	U.M.	Qtd.	Valor Médio Unitário	Valor Total
1	Fornecimento de Solução de segurança para microssegmentação de ambiente corporativo com licenciamento para Servidores	Licença	516	R\$ 2.988,73	R\$ 1.542.184,68
2	Fornecimento de Solução de microssegmentação de ambiente corporativo com licenciamento para Endpoints	Licença	5000	R\$ 496,23	R\$ 2.481.150,00
3	Fornecimento de Solução de microssegmentação de ambiente corporativo com licenciamento para Kubernetes.	Licença	21	R\$ 13.498,43	R\$ 283.467,03
4	Serviço de Instalação da solução	Serviço	1	R\$ 217.500,00	R\$ 217.500,00
5	Serviço de Treinamento/ Capacitação para 5 pessoas	Serviço	5	R\$ 23.982,32	R\$ 119.911,60
VALOR DE REFERÊNCIA TOTAL DA CONTRATAÇÃO					R\$ 4.644.213,31

10. ADEQUAÇÃO ORÇAMENTÁRIA

10.1. Fonte de Recursos

10.1.1. As despesas resultantes desta contratação estão inicialmente previstas no Programa de Trabalho 28.845.0903.00NR.0053 – Manutenção da Polícia Civil do Orçamento da União, fonte 100 (PCDF), cuja fonte de recursos será ratificada quando da reserva orçamentária feita pela Divisão de Orçamento de Finanças – DOF.

10.2. Cronograma de execução físico-financeira

Item	Descrição	Percentual Pago	Valor (R\$)	Prazo
1	Fornecimento de Solução de segurança para microssegmentação de ambiente corporativo com licenciamento para Servidores.	100%	R\$ 1.542.184,68	Em até 30 dias a contar do recebimento definitivo.
2	Fornecimento de Solução de microssegmentação de ambiente corporativo com licenciamento para Endpoints.	100%	R\$ 2.481.150,00	Em até 30 dias a contar do recebimento definitivo.

3	Fornecimento de Solução de microssegmentação de ambiente corporativo com licenciamento para Kubernetes.	100%	R\$ 283.467,03	Em até 30 dias a contar do recebimento definitivo.
4	Serviço de Instalação da solução	100%	R\$ 217.500,00	Em até 30 dias a contar do recebimento definitivo.
5	Serviço de Treinamento para 5 pessoas	100%	R\$ 119.911,60	Em até 30 dias a contar do aceite do treinamento.

10.3. Tipo de empenho

10.3.1. O empenho será **ordinário**, tendo em vista que a despesa advinda da contratação possui valor total conhecido e será pago em parcela única.

11. CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

11.1. Organização da Proposta

11.1.1. Ter prazo de validade não inferior a 90 (noventa) dias corridos, a contar da data de sua apresentação;

11.1.2. Descrever de forma clara as especificações do objeto e outros dados que facilitem a análise e o julgamento;

11.1.3. As propostas deverão ser apresentadas com as quantidades, contemplando o valor unitário de cada item e o valor global. Os valores deverão estar atualizados, em moeda nacional, em algarismo e por extenso, conforme modelo de proposta;

11.1.4. Indicar de forma expressa que o preço cotado inclui todos os custos e despesas inerentes ao objeto licitado, tais como: tributos, impostos, contribuições fiscais, parafiscais ou taxas, inclusive, porventura, com serviços de terceiros, que incidam direta ou indiretamente no valor dos serviços cotados que venham a onerar o objeto desta licitação;

11.1.5. Declarar que concorda e cumprirá todas as condições que constarão do Termo de Referência;

11.1.6. Informar dados da empresa como: razão social, endereço completo, telefone/fax, número do CNPJ, banco, agência, número da conta corrente e endereço eletrônico;

11.1.7. Apresentar valores atualizados expressos em Reais, em algarismo e por extenso, conforme modelo de proposta;

11.1.8. Indicar de forma detalhada as especificações da solução cotada, marca e modelo (quando cabíveis), e outros dados que facilitem a análise e o julgamento.

11.2. Apresentação das Propostas de Preços

11.2.1. No preço cotado, deverão ser incluídas todas as despesas com mão-de-obra, auxílio alimentação ou refeição, transporte, fretes, taxas, serviços de suporte, tributos, garantia e quaisquer outras vantagens pagas aos colaboradores, prêmio de seguro e taxas, inclusive de administração, emolumentos e quaisquer despesas operacionais, ICMS, viagens de colaboradores, bem como todos os encargos sociais, trabalhistas, previdenciários, fiscais, comerciais, despesas e obrigações financeiras de qualquer natureza e outras despesas, diretas e indiretas, ou seja, todos os componentes de custos agregados ao fornecimento das licenças de renovação de garantia e suporte técnico, inclusive o lucro, necessários à perfeita execução do objeto da licitação e todas as demais despesas necessárias à execução do objeto.

11.2.2. Será considerada vencedora do grupo a empresa que apresentar a proposta com menor valor unitário, desde que atenda as exigências contidas neste Termo de Referência e no edital do Pregão, em razão das características e peculiaridades, conforme descrito nas especificações técnicas.

11.2.3. A proposta deverá ser apresentada conforme modelo do Anexo I.

11.3. Qualificação Técnica

11.3.1. Deverá apresentar comprovação relativa à qualificação técnica, para fins de habilitação

técnica, 01 (um) ou mais ATESTADO(S) DE CAPACIDADE TÉCNICA, a ser(em) fornecido(s) por pessoa jurídica de direito público ou privado, em documento timbrado, que comprove que a licitante prestou serviços em características, quantidades e prazos compatíveis com o objeto desta licitação, mediante a apresentação de atestado(s) fornecido(s) por pessoas jurídicas de direito público ou privado, de acordo com o art. 156 do Decreto Distrital nº 44.330/2023 e art. 67 da Lei Federal nº 14.133/2021, devendo manter, durante toda a execução do contrato, em compatibilidade com as obrigações por ele assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

11.3.2. Consideram-se pertinentes e compatíveis os atestados que, em sua individualidade ou somatório, comprovem que a empresa já executou ou esteja executando, de forma satisfatória, o fornecimento de licenciamentos similares aos descritos neste TR, pelo período mínimo de 12 (doze) meses, junto a empresa ou órgão da Administração Pública. Será considerado suficiente o atendimento aos requisitos citados nos itens 11.3.2.1 ou 11.3.2.2, a seguir.

11.3.2.1. No mínimo 258 licenças de solução de segurança para microssegmentação de ambiente corporativo para Servidores;

11.3.2.2. No mínimo 2500 licenças da solução de segurança para microssegmentação de ambiente corporativo para Endpoints.

11.3.3. O documento apresentado pela licitante para comprovação de sua qualificação técnica, além de possuir informações técnicas e operacionais suficientes para qualificar o escopo realizado, incluindo-se os serviços de assistência técnica, deverá conter dados que possibilitem à contratante confirmar sua veracidade junto ao cedente emissor.

11.3.4. A CONTRATANTE reserva-se o direito de promover diligências por meio de contato com as pessoas jurídicas emitentes dos atestados com o intuito de obter informações complementares ou certificar-se da exatidão das informações constantes nos atestados apresentados.

11.3.5. Deverão constar do(s) atestado(s) de capacidade técnica os seguintes dados: razão social, CNPJ, endereço, telefone e identificação dos responsáveis pelas informações, especificação completa do fornecimento, prazo de vigência do contrato, local e data de expedição.

11.3.6. Ressalta-se que será aceito somatório de atestados que comprovem o fornecimento de licenças de solução de segurança para microssegmentação de ambiente corporativo para Servidores e Endpoints e Kubernetes, conforme item 11.3.2, mesmo que em projetos diferentes.

11.3.7. Somente poderão ser aceitos atestados de capacidade técnica expedidos após a conclusão do contrato ou, no caso de contratos vigentes, se decorrido período suficiente que comprove a execução satisfatória, observando-se que o prazo mínimo de 12 (doze) meses exigido no item 11.3.2 refere-se à experiência acumulada da licitante, podendo ser comprovado pelo somatório de diferentes atestados, em observância à jurisprudência do TCU.

11.3.8. O(s) atestado(s) de capacidade técnica será(ão) submetido(s) a Divisão de Tecnologia da Informação – DITEC/DGI para validação técnica.

11.4. **Qualificação econômico-financeira**

11.4.1. Deverá ser apresentada certidão negativa de falência expedida pelo distribuidor da sede do licitante.

11.4.2. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos.

11.4.3. No caso de empresa constituída no exercício social vigente, admite-se a apresentação de balanço patrimonial e demonstrações contábeis referentes ao período de existência da sociedade.

11.4.4. É admissível o balanço intermediário, se decorrer de lei ou contrato social/estatuto social.

11.4.5. Comprovação da boa situação financeira da empresa mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), obtidos pela aplicação das seguintes fórmulas:

	Ativo Circulante + Realizável a Longo Prazo
--	---

LG =	Passivo Circulante + Passivo Não Circulante
------	---

SG =	Ativo Total
	Passivo Circulante + Passivo Não Circulante

LC =	Ativo Circulante
	Passivo Circulante

11.4.6. As empresas, cadastradas ou não no SICAF, que apresentarem resultado inferior ou igual a 1(um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), deverão comprovar patrimônio líquido de 10 % (dez por cento) do valor estimado da contratação ou do item pertinente, na forma do §4º do art. 69 da Lei nº 14.133/2021.

11.5. Critérios de Seleção

11.5.1. **Caracterização da Solução** - Por se tratar de bens e serviços usuais no mercado e passíveis de serem definidos de forma objetiva, o objeto em questão se enquadra na definição de bens e serviços comuns, conforme art. 6º, inciso XIII da Lei 14.133/2021.

11.5.2. **Tipo de Licitação:** o critério de julgamento das propostas que deverá ser levado em conta é o de MENOR PREÇO dentre os fornecedores que apresentarem condições de realizar o serviço conforme art. 33, inciso I, da Lei 14.133/2021 e art. 115 do Decreto Distrital nº 44.330/2023.

11.5.3. **Modalidade de Licitação:** Por se tratar de bens e serviços comuns e como existem no mercado diversas empresas capazes de atender as necessidades da Contratante, sendo que a escolha pode ser feita baseada somente no preço ofertado, a seleção do fornecedor deve dar-se-á por meio de Pregão Eletrônico, conforme art. 6º, inciso XLI, da Lei 14.133/2021 e art. 114 do Decreto Distrital nº 44.330/2023.

11.5.4. **Regime de execução:** O objeto da contratação contempla o regime de execução indireta com fornecimento e prestação de serviço associado, na forma de empreitada por preço global.

11.5.5. **Tratamento Diferenciado a Microempresas e Empresas de Pequeno Porte – ME/EPP:** Não será aplicado o tratamento diferenciado, segundo determinações da Lei Complementar nº 123/2006 e da Lei Distrital 4.611/2011 em razão do valor estimado da contratação, e por não haver viabilidade técnica para a divisibilidade do objeto em lotes ou itens de cotas, considerando-se que a divisão poderia ocasionar datas de entregas e características diferentes para o mesmo produto licitado, bem como descaracterização da solução a ser adquirida. Além disso, a divisão dos itens em cotas reservadas abre a possibilidade para que o produto seja arrematado por duas empresas diferentes, podendo causar grandes problemas na execução contratual. Corre-se ainda o risco de se ter itens desertos ou fracassados, o que afetaria diretamente no atendimento da necessidade da contratação. Importante ressaltar que não há também como se garantir a quantidade mínima de 3 (três) fornecedores competitivos enquadrados como microempresas ou empresas de pequeno porte sediados local ou regionalmente e capazes de cumprir as exigências estabelecidas no instrumento convocatório, nos termos do art. 49, II da LC nº 123/2006.

11.5.6. **Subcontratação, Subcontratação Compulsória:** Não será admitida na presente contratação em razão da não possibilidade de fracionamento do objeto e por não se tratar de objeto complexo ou de grande vulto.

11.5.7. **Consórcio e Cooperativa:** Não serão admitidos na presente contratação em razão da não possibilidade de fracionamento do objeto, que não é complexo e tampouco de grande vulto, e dadas as características específicas da contratação dos produtos a serem fornecidos, uma vez que não pressupõem multiplicidade de atividades empresariais distintas (heterogeneidade de atividades empresariais) para o fornecimento do objeto deste TR. Há diversas empresas do mercado que fornecem o objeto a ser contratado. Nessa situação, caso a participação do consórcio fosse permitida, estaria limitando a concorrência, pois as empresas poderiam deixar de ser concorrentes com objetivo de se unir, reduzindo a oportunidade de oferta de um preço mais justo pelo serviço.

11.5.8. **Justificativa para Contratação Direta:** Não se aplica devido à realização de Pregão Eletrônico e por haver no mercado diversas empresas especializadas e capazes de prestar os serviços objeto deste termo de referência.

- 11.5.9. **Critérios Técnicos Pontuáveis:** Não se aplicam devido à realização de Pregão Eletrônico.
- 11.5.10. **Critério de Julgamento:** O critério de julgamento será o de menor preço.

12. VISTORIA

- 12.1. Em razão do objeto da contratação (Solução de Segurança para Microsegmentação de rede), não será necessária vistoria.

13. DO REAJUSTE

- 13.1. Os preços inicialmente contratados são fixos e irrevogáveis, no prazo de um ano contado da data do orçamento estimado.
- 13.2. Após o interregno de um ano, e independentemente de pedido do contratado, os preços iniciais serão reajustados, mediante a aplicação, pelo contratante, do Índice de Custos de Tecnologia da Informação – ICTI, na forma do art. 24 da Instrução Normativa SGD/ME nº 94/2022, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.
- 13.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.
- 13.4. No caso de atraso ou não divulgação do(s) índice(s) de reajustamento, o contratante pagará ao contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).
- 13.5. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).
- 13.6. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.
- 13.7. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.
- 13.8. O reajuste será realizado por apostilamento.
- 13.9. Por fim, cumpre esclarecer que pagamento do contrato ocorrerá em parcela única, no início da execução do contrato, na forma do subitem 10.2, não incidindo reajustamento de preços durante os 12 (doze) meses de fornecimento da subscrição.

14. VIGÊNCIA DO CONTRATO

- 14.1. O contrato vigorará por 12 (doze) meses, contados a partir da data da assinatura do contrato, podendo ser prorrogado nos termos dos artigos 106 e 107 da Lei nº 14.133/2021, e do §20, artigo 179, do Decreto Distrital nº 44.330/2023.
- 14.2. O prazo de vigência contratual não se confunde com o prazo de prestação dos serviços de suporte técnico, manutenção e garantia, que serão prestados pelo período de 12 (doze) meses, mas contados a partir do Termo de recebimento definitivo.

15. DISPOSIÇÕES GERAIS

- 15.1. Caso os prazos definidos no Termo de Referência não estejam expressamente indicados nas propostas, eles serão considerados como aceitos pela CONTRATADA;
- 15.2. Em caso de divergência entre normas infralegais e as contidas no Termo de Referência, prevalecerão as últimas;
- 15.3. Nos termos do artigo 1º da Lei Distrital 5.061/2013, c/c o artigo 7º, inciso XXXIII da

Constituição Federal, é estritamente vedado o uso de mão de obra infantil;

15.4. Havendo irregularidades no instrumento, deve-se entrar em contato com a Ouvidoria de Combate à Corrupção, no telefone 0800-6449060;

15.5. Nos termos do artigo 1º da Lei Distrital 5.448/2015, fica proibido qualquer conteúdo discriminatório contra a mulher, que incentive a violência contra a mulher, que exponha a mulher a constrangimento, de natureza homofóbico ou que represente qualquer tipo de discriminação.

16. DOCUMENTOS ANEXOS

- 16.1. Anexo I – Modelo de Proposta de preços
- 16.2. Anexo II – Modelo de Termo de Responsabilidade, Compromisso e Sigilo.
- 16.3. Anexo III – Modelo de Termo de Ciência
- 16.4. Anexo IV – Modelo de Termo de Recebimento Provisório
- 16.5. Anexo V – Modelo de Termo de Recebimento Definitivo
- 16.6. Anexo VI – Modelo de Ordem de Serviço

17. DESPACHOS FINAIS E ENCAMINHAMENTOS

Equipe de Planejamento da Contratação:

Integrante Requisitante: Carlos Said Oiticica Bandeira, matrícula nº 78.156-8

Integrante Técnico: Luiz Eduardo Paes Salomão, matrícula nº 1.721.179-4

Integrante Administrativo: Renata Sousa Pinto de Abreu - Matrícula: 77.432-4

Autoridade Competente:

Simone Pereira Duarte

Matrícula nº 78.526-1

Diretor da DITEC/DGI/PCDF

ANEXO I - MODELO DE PROPOSTA DE PREÇOS

(Em papel timbrado da empresa)

À
Polícia Civil do Distrito Federal – PCDF

Proposta que faz a empresa _____ inscrita no CNPJ nº _____ e Inscrição Estadual nº _____ estabelecida no (a) _____, para Contratação de serviços para fornecimento de Solução de Segurança para Microsegmentação, incluindo instalação, implantação, treinamento, garantia e suporte técnico por 12 (doze) meses, conforme especificações técnicas descritas no Termo de Referência.

ITEM	QTD	DESCRIÇÃO	U.M	VALOR UNITÁRIO	VALOR TOTAL
1	516	Fornecimento de Solução de segurança para microsegmentação de ambiente corporativo com licenciamento para Servidores.			

2	5000	Fornecimento de Solução de microssegmentação de ambiente corporativo com licenciamento para Endpoints.			
3	21	Fornecimento de Solução de microssegmentação de ambiente corporativo com licenciamento para Kubernetes.			
4	1	Serviço de Instalação da solução			
5	5	Serviço de Treinamento para 5 pessoas			
	TOTAL				

O valor total de proposta é de _____ (em algarismo e por extenso).

O valor apresentado engloba todas as despesas com tributos, impostos, contribuições fiscais, parafiscais ou taxas, inclusive, porventura, com serviços de terceiros, que incidam direta ou indiretamente no valor dos serviços cotados que venham a onerar o objeto desta licitação.

O prazo de validade desta proposta é de 90 (noventa) dias, contados a partir da data do seu envio à PCDF.

Declaramos que estamos de pleno acordo com todas as condições estabelecidas no Termo de Referência e seus Anexos.

Observação: A proposta deve indicar de forma detalhada as especificações da solução cotada, marca e modelo (quando cabíveis), e outros dados que facilitem a análise e o julgamento.

Dados da empresa:

Razão Social: _____

CNPJ/MF: _____

Endereço: _____

Tel/Fax: _____

e-mail: _____

CEP: _____ Cidade: _____ UF: _____

Dados do Representante Legal da Empresa:

Nome: _____

Cargo/Função: _____

Brasília, _____ de _____ de 2025.

Atenciosamente,

Proponente

Assinatura(s) do(s) representante(s) legal (is) do proponente

Nome(s), endereço, Fax e telefone para contato

ANEXO II - MODELO DE TERMO DE RESPONSABILIDADE, CONFIDENCIALIDADE E SIGILO

PROTOCOLO Nº <<>>

<<Número de Identificação Termo>>

Eu <<XXXX>> CPF nº <<000.000.000-00>> matrícula nº <<000.000>>, vinculado ao quadro do(a) <<unidade de lotação>> onde exerço o cargo/função de <<>>

DECLARO estar ciente das credenciais de acesso aos ativos de tecnologia da Polícia Civil do Distrito Federal, para acesso ou alteração de informações do(s) sistema(s) informatizado(s) desta instituição, que a mim são concedidas através da inclusão no módulo/grupo/perfil do sistema de trabalho descrito no protocolo vinculado, bem como nas disposições contidas no instrumento Políticas e Diretrizes de Segurança da Informação da Polícia Civil do Distrito Federal, e com base no disposto:

ASSUMO o compromisso de manter confidencialidade e sigilo sobre todas as informações [1] constantes nos Sistemas Corporativos da Polícia Civil do Distrito Federal às quais terei acesso.

Por este Termo de Responsabilidade, Confidencialidade e Sigilo, comprometo-me:

- A não utilizar QUAISQUER informações (Estratégicas, Técnicas Administrativas, Táticas ou Operacionais), confidenciais ou não, a que tiver acesso, para gerar benefício próprio exclusivo e/ou unilateral, presente ou futuro, ou para o uso de terceiros;
- A não efetuar nenhuma gravação ou cópia da documentação a que tiver acesso;
- A não apropriar para mim ou para outrem de QUALQUER material técnico, gerencial ou administrativo que venha a ser disponível;
- A não repassar o conhecimento das informações, responsabilizando-me por todas as pessoas que vierem a ter acesso às informações, por meu intermédio, e obrigando-me, assim, a estar sujeito a qualquer apuração de ocorrência de qualquer dano e/ou prejuízo oriundo de uma eventual quebra de sigilo ou confidencialidade de todas as informações fornecidas;
- Em tomar os cuidados que a mim são incumbidos no dever laboral para que as informações confidenciais fiquem restritas ao conhecimento tão somente das pessoas que estejam diretamente envolvidas nas discussões, análises, reuniões e negócios, devendo cientificá-las da existência deste Termo e da natureza confidencial destas informações.

DECLARO, por fim, ter pleno conhecimento do conteúdo deste Termo de Responsabilidade, Confidencialidade e Sigilo em sua íntegra.[2]

Brasília <<dd>> de <<mês>> de <<yyyy>>.

<<NOME DO USUÁRIO>>

<<MATRÍCULA>>

[1] Informação inclui, mas não se limita a, informação relativa às documentações técnicas, relatórios técnicos, operações, instalações, equipamentos, segredos de negócio, segredo de fábrica, dados, habilidades especializadas, projetos, métodos e metodologia, sistemas, softwares, bases de dados, fluxogramas, especializações, componentes, fórmulas, produtos, amostras, diagramas, desenhos de esquema, oportunidades de mercado e questões relativas a negócios revelados no âmbito de serviço.

A vigência da obrigação de confidencialidade e sigilo, assumida pela minha pessoa por meio deste Termo, terá a validade enquanto a informação não for tornada de conhecimento público por qualquer outra pessoa, ou mediante autorização escrita, concedida à minha pessoa pelas partes interessadas neste Termo. Pelo não cumprimento do presente Termo de Responsabilidade, Confidencialidade e Sigilo, fico ciente de todas as sanções judiciais que poderão advir.

[2] O presente documento se fundamenta no Procedimento de Segurança da Informação de Gestão de Controle de Acesso Lógico dos Recursos Computacionais no âmbito da PCDF, aprovado pela Resolução CGSIC nº 25, de 10/08/2022, publicado no Boletim de Serviço de 13/09/2022.

ANEXO III - MODELO DE TERMO DE CIÊNCIA

O Termo de Ciência visa obter o comprometimento formal dos empregados da Contratada diretamente envolvidos na contratação quanto ao conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes no órgão/entidade.

No caso de substituição ou inclusão de empregados da contratada, o preposto deverá entregar ao Fiscal Administrativo do Contrato os Termos de Ciência assinados pelos novos empregados envolvidos na execução dos serviços contratados.

1 – IDENTIFICAÇÃO

CONTRATO Nº	xxxx/aaaa		
OBJETO	<objeto do contrato>		
CONTRATADA	<nome da contratada>	CNPJ	xxxxxxxxxxxxx
PREPOSTO	<Nome do Preposto da Contratada>		
GESTOR DO CONTRATO	<Nome do Gestor do Contrato>	MATR.	xxxxxxxxxxxxx

2 – CIÊNCIA

Por este instrumento, os empregados da prestadora de serviços abaixo-assinados declaram ter ciência e conhecimento do Termo de Compromisso de Manutenção de Sigilo e da estrutura normativa de Segurança da Informação vigentes na Contratante (PDSI, PSI, PCI, normas e procedimentos de segurança da informação).

Funcionários da Contratada		
Nome	Matrícula	Assinatura
<Nome do(a) Funcionário(a)>	<xxxxxxxxxxx>	
<Nome do(a) Funcionário(a)>	<xxxxxxxxxxx>	
...	...	...

_____ de _____ de 20_____

ANEXO IV - MODELO DE TERMO DE RECEBIMENTO PROVISÓRIO

O Termo de Recebimento Provisório declarará, de forma sumária, que as compras foram entregues, para verificação posterior da conformidade do material com as exigências contratuais, baseada nos requisitos e nos critérios de aceitação definidos no Modelo de Gestão do Contrato.

1 – IDENTIFICAÇÃO

CONTRATO/NOTA DE EMPENHO Nº	xx/aaaa		
CONTRATADA	<Nome da Contratada>	CNPJ	xxxxxxxxxxxxx
Nº DA OFB	<xxxx/aaaa>		
DATA DA EMISSÃO	<dd/mm/aaaa>		

2 – ESPECIFICAÇÃO DOS PRODUTO(S)/BEM(S) E VOLUMES DE EXECUÇÃO			
SOLUÇÃO DE TIC			
<Descrição da solução de TIC solicitada relacionada ao contrato anteriormente identificado>			
ITEM	DESCRIÇÃO DO BEM OU SERVIÇO	MÉTRICA	QUANTIDADE
1	<Descrição igual ao da OFB de abertura>	<Ex.: UNID.>	<n>
...	...	...	...
...	...	...	...
...	...	...	...
TOTAL DE ITENS			

3 – RECEBIMENTO

Para fins de cumprimento do disposto no art. 33, inciso II, alínea “i”, da IN SGD/ME nº 94/2022, por este instrumento ATESTO que os <bem(s)/produto(s)> correspondentes à <OFB> acima identificada, conforme definido no Modelo de Execução do contrato supracitado, foram entregues, estando sujeitos à avaliação específica para verificação do atendimento às demais exigências contratuais, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do contrato.

Ressaltamos que o recebimento definitivo destes <bem(s)/produto(s)> ocorrerá somente após a verificação desses requisitos e das demais condições contratuais, desde que não se observem inconformidades ou divergências quanto às especificações constantes do Termo de Referência e do Contrato acima identificado que ensejem correções por parte da **CONTRATADA**. Por fim, reitera-se que o objeto poderá ser rejeitado, no todo ou em parte, quando estiver em desacordo com o contrato.

4 – ASSINATURA

FISCAL TÉCNICO

<Nome do Fiscal Técnico do Contrato>
Matrícula: xxxxxx
<Local>, <dia> de <mês> de <ano>.

PREPOSTO

<Nome do Preposto do Contrato>
Matrícula: xxxxxx
<Local>, <dia> de <mês> de <ano>.

ANEXO V - MODELO DE TERMO DE RECEBIMENTO DEFINITIVO

O Termo de Recebimento Definitivo declarará formalmente à Contratada que os serviços prestados ou que os bens fornecidos foram devidamente avaliados e atendem às exigências contratuais, de acordo com os requisitos e critérios de aceitação estabelecidos.

1 – IDENTIFICAÇÃO			
CONTRATO/NOTA DE EMPENHO Nº	xx/aaaa		
CONTRATADA	<Nome da Contratada>	CNPJ	xxxxxxxxxxxxxx
Nº DA OS/OFB	<xxxx/aaaa>		
DATA DA EMISSÃO	<dd/mm/aaaa>		

2 – ESPECIFICAÇÃO DOS PRODUTO(S)/BEM(S)/SERVIÇOS E VOLUMES DE EXECUÇÃO				
SOLUÇÃO DE TIC				
<descrição da solução de TIC solicitada relacionada ao contrato anteriormente identificado>				
ITEM	DESCRIÇÃO DO BEM OU SERVIÇO	MÉTRICA	QUANTIDADE	TOTAL
1	<descrição igual à da OS/OFB de abertura>	<Ex.: PF>	<n>	<total>
...				
TOTAL DE ITENS				

3 – ATESTE DE RECEBIMENTO

Para fins de cumprimento do disposto no art. 33, inciso II, alínea “h”, da IN SGD/ME nº 94/2022, por este instrumento ATESTO/ATESTAMOS que o(s) <serviço(s)/ bem(s)> correspondentes à <OS/OFB> acima identificada foram <prestados/entregues> pela **CONTRATADA** e ATENDEM às exigências contratuais, discriminadas abaixo, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do Contrato acima indicado.

ITEM	EXIGÊNCIA CONTRATUAL	ATENDIMENTO	OBSERVAÇÃO
1	<exigência contratual estabelecida no TR >	...	
...	...	...	
...	...	...	

4 – DESCONTOS EFETUADOS E VALOR A LIQUIDAR

De acordo com os critérios de aceitação e demais termos contratuais, <não> há incidência de descontos por desatendimento dos indicadores de níveis de serviços definidos.

<Não foram / Foram> identificadas inconformidades técnicas ou de negócio que ensejam indicação de glosas e sanções, <cuja instrução corre em processo administrativo próprio (nº do processo)>.

Por conseguinte, o valor a liquidar correspondente à <OS/OFB> acima identificada monta em R\$ <valor> (<valor por extenso>).

Referência: <Relatório de Fiscalização nº xxxx ou Nota Técnica nº yyyy>.

5 – ASSINATURA

GESTOR DO CONTRATO

<Nome do Gestor do Contrato>

Matrícula: xxxxxxxx

<Local>, <dia> de <mês> de
<ano>.

ANEXO VI - MODELO DE ORDEM DE SERVIÇO OU FORNECIMENTO DE BENS

Por intermédio da Ordem de Serviço (OS) ou Ordem de Fornecimento de Bens (OFB) será solicitado formalmente à Contratada a prestação de serviço ou o fornecimento de bens relativos ao objeto do contrato.

O encaminhamento das demandas deverá ser planejado visando a garantir que os prazos para entrega final de todos os bens e serviços estejam compreendidos dentro do prazo de vigência contratual.

1 – IDENTIFICAÇÃO

Nº da OS/OFB	xxxx/aaaa	Data emissão	de	<dd/mm/aaaa>
CONTRATO/NOTA DE EMPENHO nº	xx/aaaa			
Objeto do Contrato	<Descrição do objeto do contrato>			
Contratada	<Nome contratada>	da	CNPJ	99.999.999/9999-99
Preposto	<Nome do preposto>			
Início vigência	<dd/mm/aaaa>	Fim vigência	<dd/mm/aaaa>	
ÁREA REQUISITANTE				
Unidade	< Sigla – Nome da unidade>			
Solicitante	<Nome solicitante>	do	E-mail	xxxxxxxxxxxxxx

2 – ESPECIFICAÇÃO DOS BENS/SERVIÇOS E VOLUMES ESTIMADOS					
Item	Descrição do bem ou serviço	Métrica	Valor unitário (R\$)	Qtde/Vol.	Valor Total (R\$)
1	...	...	...	...	...
...	...	...	...	...	...
Valor total estimado da OS/OFB					

3 – <INSTRUÇÕES/ESPECIFICAÇÕES> COMPLEMENTARES
<Incluir instruções complementares à execução da OS/OFB> <Ex.: Contatar a área solicitante para agendamento do horário de entrega> <Ex.: Conforme consta no Termo de Referência, o recebimento provisório está condicionado à entrega do código no ambiente de homologação, e a documentação do software no repositório oficial de gestão de projetos>

4 – DATAS E PRAZOS PREVISTOS			
Data de Início:	<dd/mm/aaaa>	Data do Fim:	<dd/mm/aaaa>
CRONOGRAMA DE EXECUÇÃO/ENTREGA			

Item	Tarefa/entrega	Início	Fim
1		<dd/mm/aaaa>	<dd/mm/aaaa>
...		<dd/mm/aaaa>	<dd/mm/aaaa>

5 – ARTEFATOS / PRODUTOS	
Fornecidos	A serem gerados e/ou atualizados

6 – ASSINATURA E ENCAMINHAMENTO DA DEMANDA

Autoriza-se a <execução dos serviços / entrega dos bens> correspondentes à presente <OS/OFB>, no período e nos quantitativos acima identificados.

<Nome >

<Responsável pela demanda/ Fiscal Requisitante>

Matr.: <Nº da matrícula>

<Nome >

Gestor do Contrato

Matr.: <Nº da matrícula>

<Local>, xx de xxxxxxxxxx de xxxx



Documento assinado eletronicamente por **RENATA SOUSA PINTO DE ABREU - Matr.0077432-4, Chefe do Serviço de Governança de Projetos**, em 11/02/2026, às 19:30, conforme art. 6º do Decreto nº 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.



Documento assinado eletronicamente por **SIMONE PEREIRA DUARTE FERREIRA - Matr.0078526-1, Diretor(a) da Divisão de Tecnologia**, em 12/02/2026, às 12:47, conforme art. 6º do Decreto nº 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.



Documento assinado eletronicamente por **LUIZ EDUARDO PAES SALOMAO - Matr.1721179-4, Agente de Polícia Civil**, em 12/02/2026, às 14:00, conforme art. 6º do Decreto nº 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.



A autenticidade do documento pode ser conferida no site:
[http://sei.df.gov.br/sei/controlador_externo.php?](http://sei.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0verificador=194459148)
[acao=documento_conferir&id_orgao_acesso_externo=0](http://sei.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0verificador=194459148)
[verificador= 194459148](http://sei.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0verificador=194459148) código CRC= **B961C111**.

"Brasília - Patrimônio Cultural da Humanidade"

SPO, Lote 23, Conjunto A, Bloco H, Centro Tecnológico, Térreo - Bairro Setor Policial - CEP 70610-907 - DF
Telefone(s): (61) 3207-5147
Sítio - www.pcdf.df.gov.br

00052-00026224/2024-94

Doc. SEI/GDF 194459148