Termo de Referência n.º 95/2026 - DETRAN/DG/DIRTEC

1. DAS CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Do Objeto

1.1.1. O presente Termo de Referência tem por objeto a pretensa contratação, **REGISTRO DE PREÇO PARA EVENTUAL CONTRATAÇÃO DE SERVIÇO DE PLATAFORMA DE SEGURANÇA PARA DEFESA CIBERNÉTICA QUE AUXILIE NA DETECÇÃO, INVESTIGAÇÃO E RESPOSTA ÀS AMEAÇAS AVANÇADAS COM EXTENSA AUTOMAÇÃO DO CICLO DE RESPOSTA A INCIDENTES ATRAVÉS DE TECNOLOGIA BASEADA EM INTELIGÊNCIA ARTIFICIAL PARA PARALISAR IMEDIATAMENTE A AMEAÇA EM ANDAMENTO, EM VELOCIDADE DE MÁQUINA, REDUZINDO COM EFETIVIDADE O RISCO CIBERNÉTICO. A SOLUÇÃO DEVE MANTER ANÁLISE CONTÍNUA, VISIBILIDADE GRANULAR EM TEMPO REAL E SERVIÇO ININTERRUPTO DE NOTIFICAÇÕES PROATIVAS DE AMEAÇAS, 24 HORAS POR DIA E 7 DIAS POR SEMANA, PARA A EQUIPE DE SEGURANÇA DESIGNADA, A FIM DE MANTER A CONFIDENCIALIDADE, A DISPONIBILIDADE E A INTEGRIDADE DAS INFORMAÇÕES, PELO PERÍODO DE 24 MESES, para atender as demandas do DETRAN/DF**, conforme condições e exigências estabelecidas neste instrumento.

1.2. Da natureza e classificação do objeto

1.2.1. Nos termos do Inciso XIII do art. 6º da Lei n. 14.133/2021, informamos que o objeto é classificado com bem comum, por possuir padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado.

1.3. Da vigência do contrato

1.3.1. O prazo de vigência da contratação é de 24 (vinte e quatro) meses contados da assinatura do Termo de Contrato, prorrogável para até 10 anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

"Os contratos de serviços e fornecimentos contínuos poderão ser prorrogados sucessivamente, respeitada a vigência máxima decenal, desde que haja previsão em edital e que a autoridade competente ateste que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com o contratado ou a extinção contratual sem ônus para qualquer das partes."

1.3.2. A definição do prazo de vigência contratual é elemento determinante para a segurança jurídica e operacional da contratação, especialmente quando se trata de solução tecnológica integrada de segurança da informação e defesa cibernética, com natureza contínua, dependente de monitoramento ininterrupto, evolução tecnológica constante e suporte técnico especializado. Em observância ao art. 107 da Lei nº 14.133/2021, os contratos administrativos que envolvem prestação de serviços contínuos podem ter vigência superior a um exercício financeiro, desde que expressamente prevista no edital e mantida a vantajosidade da relação contratual para a Administração.

1.3.3. As empresas/licitantes deverão cotar a quantidades previstas neste instrumento.

1.3.4. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. Finalidade

2.2. O objeto da contratação tem como finalidade elevar o nível de segurança da informação institucional, garantir a proteção de dados sensíveis e prevenir incidentes capazes de comprometer a continuidade dos serviços públicos de trânsito. A adoção de uma solução integrada de cibersegurança responde diretamente aos desafios decorrentes da crescente interconexão de sistemas administrativos, plataformas digitais e aplicações em nuvem, exigindo mecanismos unificados de controle, resposta e visibilidade. Trata-se, assim, de medida estratégica de governança digital que contribui para a preservação da integridade, disponibilidade e confidencialidade das informações sob guarda do DETRAN-DF, assegurando aderência aos princípios da Lei nº 13.709/2018 (LGPD) e da Lei nº 14.129/2021 (Governo Digital).

2.3. Motivação/Justificativa

2.3.1. A justificativa da necessidade da contratação parte do reconhecimento de que o Departamento de Trânsito do Distrito Federal – DETRAN-DF, autarquia integrante do Sistema Nacional de Trânsito, criada originalmente no âmbito da Secretaria de Segurança Pública (Decreto-Lei nº 315/1967) e transformada em autarquia pela Lei nº 6.296/1975, exerce função essencial à segurança viária, à regulação da frota e à prestação de serviços críticos à população do Distrito Federal.

2.3.2. Ao longo de sua trajetória institucional, consolidou-se como autoridade pública responsável por políticas de educação, fiscalização, registro e controle de veículos e condutores, por integrações com bases nacionais e distritais e pela disponibilização de serviços digitais que permitem ampla fruição de direitos pelo cidadão. A natureza e a criticidade dessas atribuições, executadas sobre ecossistema tecnológico cada vez mais distribuído e interconectado, impõem a adoção de padrões elevados de segurança cibernética, governança de dados e resiliência operacional, sob pena de comprometer a continuidade do serviço público, a proteção de informações pessoais e sensíveis e a confiança social nos serviços prestados.

2.3.3. No plano das responsabilidades finalísticas, o DETRAN-DF estrutura e operacionaliza serviços de registro, licenciamento, transferência e fiscalização de veículos, habilitação de condutores, educação para o trânsito, atendimento ao público e integração de dados com órgãos do Governo do Distrito Federal, com o Departamento Nacional de Trânsito, com forças de segurança e com demais entes do Sistema Nacional de Trânsito. Para tornar isso possível, mantém ambientes transacionais de alta demanda, integrações em tempo real com repositórios críticos (multas, pontuação, restrições administrativas, vistorias, arrecadação), serviços digitais em múltiplos canais, atendimento remoto e presencial e operações que, por sua própria natureza, exigem disponibilidade contínua, confiabilidade das informações e proteção contra incidentes cibernéticos ao longo de toda a cadeia de valor do serviço público.

2.3.4. A expansão do portfólio digital, a multiplicidade de atores que interagem com os sistemas e a intensificação do uso de dados para tomada de decisão reclamam, com urgência, arcabouço tecnológico capaz de detectar, investigar e responder a ameaças com rapidez e precisão, em conformidade com a Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/2018), o Marco Civil da Internet (Lei nº 12.965/2014, art. 13 e §1º), a Política Nacional de Segurança da Informação (Decreto nº 9.637/2018), a Estratégia Nacional de Segurança Cibernética (Decreto nº 10.222/2020) e as boas práticas de gestão de segurança da informação (ISO/IEC 27001, 27002 e correlatas).

2.3.5. A missão institucional do DETRAN-DF, orientada à promoção da segurança, da fluidez e da cidadania no trânsito, demanda que a tomada de decisão seja suportada por evidências confiáveis, tempestivas e íntegras; que a visão de longo prazo – consolidar-se como referência nacional em gestão, governança e educação para o trânsito – seja sustentada por plataformas tecnológicas resilientes; e que os valores institucionais – probidade, transparência, respeito à vida, inovação e educação – se traduzam em serviços digitais estáveis, auditáveis e seguros.

2.3.6. Esses pressupostos, inerentes ao interesse público, conectam-se diretamente à governança digital e às contratações de TIC regidas pela Lei nº 14.133/2021, pela IN SEGES/ME nº 94/2022 e pelo Decreto Distrital nº 44.330/2023, que exigem planejamento robusto, motivação adequada, análise de riscos e definição precisa do problema a ser solucionado antes da escolha do arranjo de contratação e da solução tecnológica.

2.3.7. A estrutura institucional necessária para cumprir tais responsabilidades envolve unidades finalísticas e de apoio, governança de TIC, segurança da informação, atendimento, fiscalização, arrecadação e educação, articuladas por fluxos decisórios e controles internos que viabilizam a segregação de funções, a rastreabilidade de atos e a conformidade com as diretrizes de planejamento e orçamento (PAC/PGC, PPA, LDO e LOA).

2.3.8. Em termos de infraestrutura, o órgão opera data centers e serviços em nuvem, redes corporativas, estações de trabalho, serviços de diretório e identidade, bases relacionais e não relacionais, integrações por APIs, mensageria, serviços críticos de arrecadação e de atendimento digital, além de camadas de monitoramento e de proteção já implantadas (firewalls, VPN, segmentação, antivírus/EDR, cópias de segurança).

2.3.9. Esse conjunto, embora relevante, mostra-se insuficiente diante do cenário atual de ameaças avançadas e do crescimento de dependência digital dos serviços do órgão.

2.3.10. No estado atual, observam-se problemas estruturais típicos de ambientes em expansão contínua: fragmentação de visibilidade sobre tráfego leste-oeste e ativos fora de padrão; baixa integração entre telemetrias de rede, endpoints e aplicações; lacunas de correlação em tempo real; resposta a incidentes eminentemente reativa; e insuficiência de mecanismos para conter, de forma autônoma e em velocidade de máquina, movimentos laterais, exfiltração e campanhas coordenadas (ransomware, BEC, abuso de credenciais, uso indevido de SaaS).

2.3.11. Esse contexto expõe a organização a riscos de indisponibilidade de serviços essenciais, de vazamento de dados pessoais e sensíveis, de deterioração da confiança social, de impacto financeiro e de responsabilização administrativa, inclusive à luz da LGPD e do Marco Civil da Internet, cujo art. 13 e §1º exigem guarda, sigilo e controle dos registros de conexão em ambiente seguro sob responsabilidade do administrador do sistema autônomo, o que demanda governança e controle interno efetivos sobre o ciclo de vida desses registros.

2.3.12. Com vistas a mitigar tais riscos, o órgão adotou medidas paliativas e corretivas pontuais, porém insuficientes para enfrentar a escala e a sofisticação das ameaças contemporâneas. Entre essas medidas, destacam-se: reforço de regras de perímetro em firewalls legados, sem cobertura comportamental abrangente; campanhas periódicas de conscientização de usuários e ajustes de política de senha; ampliação manual de listas de controle de acesso e endurecimento de configurações sem automação de verificação contínua; contratação fragmentada de serviços de suporte reativo para análise de incidentes após a ocorrência; substituição ad hoc de equipamentos e atualizações de assinatura antivírus/EDR sem correlação avançada com telemetria de rede e de SaaS; integrações pontuais com ferramentas de monitoramento que não atendem plenamente a requisitos de detecção comportamental e de resposta automática.

2.3.13. Tais iniciativas, embora necessárias, mantêm a defesa em patamar aquém do requerido, pois permanecem dependentes de intervenção humana, escalonamento manual e janelas de reação que não coíbem a progressão de ataques em curso.

2.3.14. Os impactos acumulados desse cenário são verificáveis em múltiplas dimensões: aumento do tempo médio de detecção e de resposta a incidentes; esforço operacional elevado para triagem de alertas com alto índice de falsos positivos; janelas de indisponibilidade não planejadas e degradação de desempenho em sistemas críticos; risco de exposição de dados pessoais e sensíveis com potenciais sanções regulatórias; necessidade recorrente de retrabalho em investigações forenses; atraso na entrega de serviços digitais ao cidadão; impactos reputacionais por notícias adversas sobre incidentes setoriais; pressão sobre equipes técnicas e sobre a cadeia decisória; riscos orçamentários decorrentes de mitigações emergenciais; e vulnerabilidade ampliada em integrações com terceiros e serviços em nuvem.

2.3.15. Esse quadro, somado à evolução do crime cibernético e ao histórico de incidentes no setor público, reforça a urgência de abandonar o ciclo estritamente reativo e adotar postura preventiva, detectiva e responsiva de alta automação.

2.3.16. Diante disso, identifica-se a necessidade de ampliar, com prioridade, a capacidade institucional de observar e compreender comportamentos anômalos em toda a superfície de ataque (rede, endpoints, IoT/OT, aplicações e SaaS), correlacionar telemetrias em tempo real, reduzir drasticamente o tempo de contenção e executar respostas proporcionais de forma automática, com governança e auditabilidade.

2.3.17. O objetivo é evoluir do modelo fragmentado para um ecossistema integrado de defesa que opere com análise comportamental e inteligência artificial aplicada à detecção, investigação e resposta a ameaças, com mecanismos de contenção autônoma e orquestrada, relatórios executivos e trilhas de auditoria, integração com SIEM/SOAR, APIs e padrões abertos, sem identificação de fabricante no instrumento convocatório, em observância à isonomia e à competitividade previstas na Lei nº 14.133/2021 e na IN nº 94/2022.

2.3.18. A solução a ser contratada deve contemplar, entre outras capacidades, a observação contínua do ambiente para construção de perfis comportamentais basais; a detecção de anomalias e de cadeias táticas, técnicas e procedimentos (TTPs) independentemente de assinaturas; a investigação assistida por IA para priorização de eventos e redução de falsos positivos; a resposta automática e proporcional para isolar dispositivos, neutralizar comunicações maliciosas e impedir movimento lateral; a cobertura de ambientes híbridos e de aplicações SaaS relevantes ao órgão; a integração com diretórios de identidade e mecanismos de autenticação; a geração de trilhas de auditoria e relatórios de conformidade; e a preservação da guarda e do sigilo dos registros sob controle da Administração, em atendimento ao art. 13 e §1º do Marco Civil da Internet.

2.3.19. Esses requisitos almejam um patamar de proteção compatível com a criticidade do serviço público, alinhado à Política e à Estratégia Nacional de Segurança Cibernética e às melhores práticas de segurança da informação.

2.3.20. Espera-se, com a contratação, benefícios tangíveis e mensuráveis: redução do tempo médio de detecção e de resposta; aumento da taxa de contenção antes de impacto operacional; melhoria da disponibilidade de serviços digitais e da experiência do usuário; proteção reforçada de dados pessoais e sensíveis com reflexos diretos na conformidade à LGPD; racionalização do esforço operacional por redução de falsos positivos e automação de triagem; evidências auditáveis para órgãos de controle; maior previsibilidade orçamentária por mitigação de perdas associadas a incidentes; e reforço da confiança social no serviço público.

2.3.21. De igual modo, a não contratação mantém elevado o risco de incidentes graves, indisponibilidades prolongadas, vazamento de dados e responsabilizações institucionais, com custos financeiros e reputacionais significativamente superiores aos investimentos planejados.

2.3.22. Sob o ponto de vista jurídico-administrativo, a presente justificativa está em consonância com os deveres de planejamento e motivação das contratações (Lei nº 14.133/2021), com a exigência de análise de risco e definição do problema público antes da escolha da solução (IN nº 94/2022), com as diretrizes distritais de governança e segregação de funções (Decreto Distrital nº 44.330/2023), com a proteção de dados pessoais (LGPD) e com a guarda de registros sob responsabilidade do administrador do sistema autônomo (Marco Civil da Internet).

2.3.23. A etapa ora documentada não define marca ou fornecedor, mantendo o foco no resultado pretendido e nos requisitos funcionais e não funcionais essenciais à proteção do interesse público, preservando a competitividade e a isonomia na fase externa da contratação.

2.3.24. Em síntese, a contratação é decorrente de estudo de viabilidade técnica e econômica voltado à contratação de empresa especializada para fornecimento de plataforma integrada de defesa cibernética baseada em inteligência artificial, com serviços correlatos de implantação, operação assistida, suporte, treinamento e transferência de conhecimento, capaz de prover detecção comportamental, investigação assistida e resposta autônoma em tempo de máquina, assegurando guarda e sigilo de registros sob controle do órgão, integridade e disponibilidade dos serviços críticos, conformidade regulatória e transparência para fins de auditoria. Essa solução, delineada em termos de capacidades e resultados e não de marcas, materializa a transição necessária do modelo reativo para uma postura preventiva e responsiva de alta maturidade, compatível com as responsabilidades institucionais do DETRAN-DF e com as expectativas do cidadão por serviços públicos digitais seguros, estáveis e confiáveis.

2.4. Riscos da não contratação

2.4.1. A ausência de uma solução tecnológica avançada de defesa cibernética coloca o DETRAN-DF em situação de vulnerabilidade crítica, expondo a Autarquia a riscos operacionais, jurídicos e institucionais de grande magnitude. O risco mais sensível reside na violação de dados pessoais e sensíveis, cuja guarda é responsabilidade direta do órgão, conforme a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD). Um eventual vazamento de informações pode gerar sanções administrativas severas, multas expressivas e perda de credibilidade institucional, comprometendo a confiança dos cidadãos e o cumprimento do dever de proteção da informação pública.

2.4.2. A ausência de mecanismos automatizados de detecção e resposta também eleva substancialmente a probabilidade de indisponibilidade dos sistemas críticos que sustentam os serviços de trânsito, como licenciamento, habilitação, arrecadação e fiscalização. Um ataque bem-sucedido, mesmo que pontual, tem potencial para paralisar operações essenciais, afetar a arrecadação, gerar filas e atrasos em larga escala e causar prejuízos financeiros e reputacionais irreversíveis. Cada hora de inatividade representa perdas diretas para a Administração e transtornos para milhares de cidadãos que dependem dos serviços digitais da Autarquia.

2.4.3. Há ainda o risco de espionagem cibernética e vazamento de informações estratégicas, uma vez que o DETRAN-DF processa dados com alto valor informacional e sensibilidade pública. A inexistência de monitoramento comportamental contínuo e de mecanismos autônomos de resposta facilita o acesso indevido por agentes mal-intencionados, podendo comprometer não apenas a integridade das bases de dados, mas também a segurança de outros órgãos interconectados.

2.4.4. Outro aspecto relevante diz respeito ao risco de perda de confiança institucional. Em uma era em que a transparência e a confiança são pilares da governança pública, qualquer incidente de segurança afeta diretamente a imagem do órgão perante a sociedade. O cidadão, ao perceber falhas de proteção, tende a questionar a capacidade do Estado em resguardar seus dados, o que fragiliza a credibilidade institucional e prejudica o relacionamento entre o Departamento e a população.

2.4.5. Adicionalmente, a ausência de solução específica para segurança cibernética compromete o atendimento a normas e exigências regulatórias, especialmente aquelas que tratam de auditoria, rastreabilidade e conformidade técnica (ISO 27001, Decreto nº 9.637/2018 e Decreto nº 10.222/2020). A não observância desses requisitos pode acarretar apontamentos de órgãos de controle, sanções administrativas e até responsabilização de gestores públicos por omissão na adoção de medidas preventivas.

2.4.6. Outro fator de risco relevante é a obsolescência tecnológica. Sem atualizações contínuas e recursos modernos de análise e mitigação, o ambiente tecnológico do DETRAN-DF tende a operar com ferramentas ultrapassadas, incapazes de acompanhar a evolução das ameaças. Essa condição fragiliza as defesas do órgão e dificulta a implementação de medidas corretivas tempestivas, aumentando o tempo de exposição a vulnerabilidades conhecidas.

2.4.7. A inexistência de uma solução capaz de oferecer visibilidade integral do ambiente de rede e dos ativos críticos impede a detecção antecipada de anomalias e o tratamento proativo de falhas. A falta de gestão de vulnerabilidades e de automação de resposta torna o DETRAN-DF altamente suscetível a ataques sofisticados, como ransomware e invasões persistentes, podendo resultar em perda de dados, paralisação de serviços e danos irreparáveis à infraestrutura tecnológica. Diante de um cenário cada vez mais dinâmico e agressivo em matéria de ameaças digitais, não investir em defesa cibernética equivale a aceitar um risco institucional inaceitável, incompatível com os deveres de segurança, continuidade e eficiência que regem a Administração Pública.

2.5. Resultados esperados

2.5.1. São resultados esperados com a pretendida contratação:

2.5.1.1. Redução substancial dos riscos de indisponibilidade e perda de dados sensíveis, assegurando a continuidade dos serviços essenciais e a resiliência operacional do

DETRAN-DF diante de ameaças cibernéticas cada vez mais sofisticadas;

2.5.1.2. Implementação de mecanismos de detecção e correção automática de vulnerabilidades, possibilitando uma postura proativa de segurança e eliminando brechas antes que possam ser exploradas por agentes mal-intencionados;

2.5.1.3. Resposta autônoma e em tempo real a incidentes de segurança, com apoio de algoritmos de inteligência artificial capazes de identificar e conter comportamentos anômalos, evitando a propagação de ataques e o comprometimento de sistemas críticos;

2.5.1.4. Conformidade integral com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e com os normativos de segurança da informação aplicáveis à Administração Pública, assegurando o tratamento adequado das informações pessoais sob a custódia do órgão;

2.5.1.5. Ampliação da capacidade de auditoria e rastreabilidade de eventos, facilitando a atuação dos órgãos de controle e reforçando a governança e a transparência das operações tecnológicas do DETRAN-DF;

2.5.1.6. Garantia de integridade, sigilo e proteção dos registros de conexão e demais dados sob guarda institucional, em consonância com o art. 13 e §1º do Marco Civil da Internet (Lei nº 12.965/2014), preservando-os em ambiente seguro e controlado;

2.5.1.7. Adoção de postura preventiva, inteligente e automatizada no enfrentamento de ameaças cibernéticas, com aumento da visibilidade sobre todo o ecossistema digital e maior agilidade na identificação de comportamentos suspeitos;

2.5.1.8. Modernização e evolução contínua da infraestrutura tecnológica, com implantação de uma solução escalável e aderente às futuras demandas de transformação digital do órgão, assegurando longevidade e eficiência dos investimentos públicos;

2.5.1.9. Integração simplificada com outras tecnologias e sistemas corporativos, permitindo interoperabilidade segura e reforçando a governança sobre os ativos digitais do DETRAN-DF;

2.5.1.10. Reforço na confiança social e na credibilidade institucional, evidenciando o compromisso do DETRAN-DF com a segurança das informações, a continuidade dos serviços e a proteção dos dados dos cidadãos, em conformidade com os princípios da legalidade, eficiência e transparência que regem a Administração Pública.

2.6. Nível de Maturidade do Detran-DF frente ao tipo de tecnologia

2.6.1. Encontra-se descrito junto aos Estudos Técnicos Preliminares.

2.7. Planejamento de Contratação Anual:

2.7.1. Em conformidade com o Planejamento de Contratações Anual (PCA), os itens previstos são: 29248

2.7.2. Para garantir a qualidade e eficácia da solução no decorrer da fase de elaboração, realizamos um ajuste, adicionando e separando os itens conforme o novo planejamento.

2.8. Integração da solução à Plataforma gov.br

2.8.1. Não se aplica.

2.8.2. A análise e justificativa encontram-se descritas junto aos Estudos Técnicos Preliminares.

2.9. Alinhamento ao Parecer Referencial nº 66/2024 – PGDF/PGCONS

2.9.1. A presente contratação encontra-se alinhada às diretrizes e premissas estabelecidas no Parecer Referencial nº 66/2024 – PGDF/PGCONS, aplicável às contratações de serviços sob a égide da Lei nº 14.133/2021, especialmente quanto à caracterização do objeto como serviço comum, à adoção do critério de julgamento compatível, à definição dos requisitos de habilitação e à adequada instrução processual.

2.9.2. O referido parecer foi juntado integralmente aos autos, servindo como fundamento jurídico referencial para a modelagem do Termo de Referência.

2.10. Cumprimento do Anexo I da IN SGD nº 94/2022 (art. 269-A do Decreto nº 44.330/2023)

2.10.1. A presente contratação enquadra-se nas hipóteses previstas no art. 269-A do Decreto nº 44.330/2023, por tratar-se de licenciamento de software.

2.10.2. Em observância ao referido dispositivo e ao Anexo I da IN SGD nº 94/2022, foram atendidas as diretrizes de planejamento, modelagem, gestão de riscos, governança contratual e definição de métricas de desempenho, conforme demonstrado no Estudo Técnico Preliminar, Termo de Referência e matriz de riscos juntados aos autos.

2.10.3. Consta no processo a comprovação do atendimento às exigências estruturantes do Anexo I, inclusive quanto à justificativa da solução, análise comparativa de alternativas, modelo de execução, modelo de fiscalização e gestão contratual.

2.11. Demais justificativas encontram-se dispostas junto ao Documento de Formalização da Demanda (DFD).

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTOS

3.1. Registro de preço para eventual contratação de serviço de plataforma de segurança para defesa cibernética que auxilie na detecção, investigação e resposta às ameaças avançadas com extensa automação do ciclo de resposta a incidentes através de tecnologia baseada em inteligência artificial para paralisar imediatamente a ameaça em andamento, em velocidade de máquina, reduzindo com efetividade o risco cibernético. a solução deve manter análise contínua, visibilidade granular em tempo real e serviço ininterrupto de notificações proativas de ameaças, 24 horas por dia e 7 dias por semana, para a equipe de segurança designada, a fim de manter a confidencialidade, a disponibilidade e a integridade das informações, pelo período de 24 meses.

3.2. Com base na estimativa da futura demanda, conforme estudo técnico preliminar realizado, foi projetado um consumo aproximado de:

Item	Descrição	CATMAT/CATSER	Licenças/ Quantidade	Métrica	Modelo
01	Solução de previsão, monitoramento, detecção, notificação, investigação e resposta autônoma a ataques cibernéticos para 2.611 dispositivos em análise de rede.	27502	1	Unidade	Subscrição
02	Expansão de Solução de previsão, monitoramento, detecção, notificação, investigação e resposta autônoma a ataques cibernéticos dispositivos em análise de rede – 100 dispositivos	27502	20	Unidade	Subscrição
03	Expansão de Solução de previsão, monitoramento, detecção, notificação, investigação e resposta autônoma a ataques cibernéticos dispositivos em análise local com agente	27502	500	Unidade	Subscrição
04	Solução de monitoramento, detecção, notificação, investigação e resposta autônoma a ataques cibernéticos em plataforma Microsoft 365.	27502	2.248	Unidade	Subscrição

05	Solução de previsão, monitoramento, detecção, notificação, e investigação em plataforma aberta	27502	2	Unidade	SaaS
06	Serviço ininterrupto de Notificações Proativas e de Ameaças de alto grau de criticidade e impacto em caráter 24x7	21202	24	Mensal	Serviço
07	Serviço de Instalação e Configuração da Plataforma de Segurança para Defesa Cibernética.	27260	1	Unidade	Serviço

3.3. A oferta deverá se basear na estimativa anual, ainda que a vigência seja definida para 24 meses.

3.4. Itens que compõem a solução

3.4.1. A solução a ser contratada é composta pelos seguintes itens:

3.4.1.1. Item 01: Formado por uma solução de previsão, monitoramento, detecção, notificação, investigação e resposta autônoma a ataques cibernéticos para dispositivos em análise de rede.

3.4.1.2. Item 02: Formado por uma solução de previsão, monitoramento, detecção, notificação, investigação e resposta autônoma a ataques cibernéticos para dispositivos em análise de rede.

3.4.1.3. Item 03: Formado por uma solução de previsão, monitoramento, detecção, notificação, investigação e resposta autônoma a ataques cibernéticos dispositivos em análise local com agente.

3.4.1.4. Item 04: Formado por uma solução de monitoramento, detecção, notificação, investigação e resposta autônoma a ataques cibernéticos em plataforma Microsoft 365.

3.4.1.5. Item 05: Formado por uma solução de previsão, monitoramento, detecção, notificação, e investigação em plataforma aberta.

3.4.1.6. Item 06: Formado por um serviço ininterrupto de Notificações Proativas e de Ameaças de alto grau de criticidade e impacto em caráter 24x7.

3.4.1.7. Item 07: Formado por serviço de instalação e configuração da plataforma de segurança para defesa cibernética.

4. ESTIMATIVA DA DEMANDA DE BENS E SERVIÇOS

4.1. Conforme o inciso I, do art. 11 da IN SGD/ME n° 94 DE 2022, o órgão demandante deve descrever de forma detalhada, motivada e justificada, inclusive quanto à forma de Cálculo, o quantitativo de bens e serviços necessários para sua composição.

4.2. A definição dos quantitativos anuais estimados para cada subitem da solução foi realizada a partir do Estudo Técnico Preliminar, apêndice deste Termo de Referência, documento que tem por objetivo analisar a viabilidade técnica, econômica e operacional da contratação, fundamentando a escolha da solução mais adequada.

4.3. Item 01: 01 unidade de subscrição

4.3.1. Solução Única contemplando todo o conjunto de dispositivos atualmente existentes e que serão monitorados, conforme levantamento de dispositivos constantes do Estudo Técnico Preliminar.

4.4. Item 02: 20 unidades de subscrição

4.4.1. Subscrições específicas para fins de expansão de monitoramento de ambiente, considerando um possível crescimento e novos ativos IoT. Separamos em 20 unidades para possibilitar crescimento gradativo e orgânico, afastando risco de contratações desnecessárias.

4.5. Item 03: 500 unidades de subscrição

4.5.1. Refere-se a quantidade de dispositivos que serão monitorados, de pessoas (remotos e em home office), como desktops.

4.6. Item 04: 2.248 unidades de subscrição

4.6.1. Refere-se a quantidade de contas existentes, junto à plataforma Microsoft365

4.7. Item 05: 02 unidades SaaS

4.7.1. Estimativa de expansão futura para outras áreas que podem ser definidas como prioritárias e necessitarem utilizar os recursos da solução.

4.8. Item 06: 24 unidades mensais

4.8.1. Quantidade correspondente ao número de meses de vigência do contrato.

4.9. Item 07: 01 unidade de serviço

4.9.1. Serviço inicial único de instalação.

5. DO REGISTRO DE PREÇOS

5.1. Em conformidade e aderência ao Estudo Técnico Preliminar, será adotado o procedimento auxiliar de registro de preços, na presente contratação.

5.2. Do Órgão Gerenciador

5.2.1. Caberá à AUTARQUIA, na qualidade de **Órgão Gerenciador** da Ata de Registro de Preços, a prática de todos os atos de controle, administração e coordenação do certame e das contratações decorrentes, em estrita observância às competências fixadas pelo art. 192 do Decreto Distrital nº 44.330/2023, competindo-lhe especificamente:

5.2.2. Dos Mecanismos de Controle de Fornecimento e Atas

I - Gestão Prévias das Obrigações: Apoiar os órgãos e entidades participantes na execução dos atos preparatórios e na consolidação das demandas, bem como gerenciar a Ata de Registro de Preços, controlando os saldos de quantitativos disponíveis para cada item da Solução de TIC registrado;

II **- Controle de Penalidades e Cadastros:** Conduzir os procedimentos administrativos para a aplicação de eventuais penalidades decorrentes do descumprimento do pactuado na ata de registro de preços, promovendo o registro das sanções no Sistema de Cadastramento Unificado de Fornecedores (SICAF) e nos demais cadastros oficiais de fornecedores do Distrito Federal;

III **- Revisão e Negociação de Preços:** Realizar, periodicamente ou quando provocado, a pesquisa de mercado para comprovar a manutenção da vantajosidade dos preços registrados, promovendo as negociações necessárias com a CONTRATADA para a adequação dos valores aos novos patamares de mercado ou para a alteração de marcas/modelos por obsolescência tecnológica, se justificado;

IV **- Cancelamento do Registro:** Conduzir os atos formais de cancelamento do registro de preços da CONTRATADA ou de itens específicos nas hipóteses legais, assegurados o contraditório e a ampla defesa.

5.2.3. Dos Mecanismos de Comunicação Institucional

V **- Canal Centralizado de Demandas:** Estabelecer canal eletrônico oficial e centralizado de comunicação com os órgãos e entidades participantes, cabendo ao gerenciador receber, analisar e deliberar sobre as solicitações de liberação de cotas e autorizações para a abertura de contratos derivados da Ata;

VI **- Notificação e Alinhamento com Participantes:** Comunicar formalmente aos órgãos participantes qualquer alteração superveniente na Ata de Registro de Preços, incluindo reajustes lineares pelo ICTI, substituições homologadas de componentes de software ou aplicação de penalidades que impeçam a continuidade do fornecimento;

VII **- Mediação Técnica:** Intervir, quando provocado por órgão participante, na mediação de conflitos técnicos ou operacionais relativos à execução e entrega das subscrições e serviços por parte da CONTRATADA, visando garantir a padronização e a qualidade na entrega das Soluções de TIC especificadas neste Termo de Referência.

5.3. Da justificativa pela escolha do Sistema de Registro de Preços

5.3.1. Considerando a natureza técnica, operacional e estratégica da solução integrada de segurança da informação e defesa cibernética a ser contratada, a análise conduzida no âmbito deste Estudo Técnico Preliminar concluiu pela adequação do uso do Sistema de Registro de Preços (SRP) como procedimento auxiliar da futura licitação. A modelagem permite a implementação progressiva e sob demanda de recursos e serviços, garantindo eficiência operacional, racionalidade orçamentária e mitigação de riscos associados à subutilização de ativos tecnológicos.

5.3.2. Nos termos do art. 190, inciso II, do Decreto Distrital nº 44.330/2023, o SRP será adotado preferencialmente "quando for conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida ou tarefa", o que se coaduna perfeitamente com o modelo de consumo programado previsto para esta contratação. A dinâmica de operação das soluções de cibersegurança – baseadas em licenciamento, monitoramento contínuo, serviços mensais e expansões graduais – justifica plenamente a utilização do SRP como mecanismo de planejamento, flexibilidade e governança de consumo.

5.3.3. A adoção do SRP permite ao DETRAN-DF estruturar a contratação em formato escalável e adaptativo, possibilitando a ampliação do uso de ferramentas como monitoramento NDR, integração com Microsoft 365, análise Dark Web e alertas autônomos de ameaças apenas quando houver necessidade comprovada e capacidade de suporte operacional. Essa lógica elimina a obrigatoriedade de aquisição integral antecipada e assegura que o consumo dos recursos ocorra de forma proporcional à demanda real e ao nível de criticidade dos serviços de segurança, reforçando os princípios da economicidade e eficiência previstos no art. 11 da Lei nº 14.133/2021.

5.3.4. O modelo também contribui para racionalidade orçamentária e controle financeiro, uma vez que os empenhos e pagamentos estarão diretamente vinculados à efetiva execução e à demanda apurada. A Administração poderá, assim, ajustar o volume de contratações ao longo do exercício, evitando imobilização indevida de recursos ou ociosidade contratual. Esse arranjo é particularmente vantajoso para soluções de segurança de TIC, em que o comportamento da ameaça, o volume de tráfego e a infraestrutura de rede podem variar substancialmente em função do cenário tecnológico e das políticas públicas em vigor.

5.3.5. Além disso, o SRP reforça a prevenção de ociosidade contratual e a otimização dos custos públicos, pois os serviços de monitoramento, resposta a incidentes, threat intelligence e suporte especializado poderão ser ativados de acordo com a evolução da necessidade institucional, sem que haja oneração prematura do erário. Essa abordagem modular é reconhecida pelos órgãos de controle, como o TCU e a CGU, como prática de boa governança e maturidade contratual em contratações de TIC.

5.3.6. A natureza progressiva e contínua da solução, aliada à necessidade de atualização tecnológica constante, torna o SRP o instrumento mais compatível com o modelo de contratação sob demanda e de execução gradual, permitindo inclusive a adesão de outros órgãos públicos interessados, conforme autoriza o Decreto Distrital nº 44.330/2023. Tal possibilidade potencializa ganhos de escala, uniformização tecnológica e ampliação da economicidade, ao mesmo tempo em que fortalece o papel do DETRAN-DF como referência institucional em governança cibernética.

5.3.7. Por fim, a adoção do SRP no presente caso está alinhada às boas práticas de planejamento, transparência e sustentabilidade contratual, assegurando previsibilidade orçamentária, rastreabilidade de consumo e aderência à estratégia de segurança digital do órgão. O modelo de registro de preços, ao vincular a execução à efetiva demanda, preserva a flexibilidade gerencial, garante a vantajosidade pública e resguarda o interesse institucional, conforme os princípios previstos no art. 37 da Constituição Federal, no art. 11 da Lei nº 14.133/2021 e no art. 190, II, do Decreto Distrital nº 44.330/2023.

5.4. Da vigência da ata de registro de preços

5.4.1. O prazo de vigência da ata de registro de preços, contado a partir da publicação do extrato da ata no Portal Nacional de Contratações Públicas, será de 12 (doze) meses e poderá ser prorrogado, por igual período, desde que comprovado que as condições e o preço permanecem vantajosos, conforme dispõe o art. 198, § 1º, do Decreto Distrital 44.330, de 2023.

5.5. Da Intenção de Registro de Preços – IRP

5.5.1. A Intenção de Registro de Preços – IRP, ficará limitada a 3 (três) órgãos ou entidades participantes, devido a capacidade limitada de gerenciamento desta autarquia, conforme permissivo do art. 192, inciso I, do Decreto 44.330/2023.

5.6. Das obrigações do órgão gerenciador

5.6.1. Efetuar o registro do licitante fornecedor e firmar a correspondente Ata de Registro de Preços.

5.6.2. Conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados.

5.6.3. Aplicar as penalidades por descumprimento do pactuado na Ata de Registro de Preços.

5.6.4. Definir mecanismos de comunicação com os órgãos participantes e não participantes, contendo:

5.6.4.1. As formas de comunicação entre os envolvidos, a exemplo de ofício, telefone, e-mail, ou sistema informatizado, quando disponível; e

5.6.4.2. Definição dos eventos a serem reportados ao órgão gerenciador, com a indicação de prazo e responsável.

5.6.5. Definir mecanismos de controle de fornecimento da solução de TIC.

5.6.6. As regras para gerenciamento da fila de fornecimento da solução de TIC aos órgãos participantes e não participantes, contendo prazos e formas de negociação e redistribuição da demanda, quando está ultrapassar a produtividade definida ou a capacidade mínima de fornecimento e for requerida pelo contratado.

5.6.7. Durante a vigência da ata de registro de preços originada desta contratação, será admitida, mediante autorização prévia e expressa do DETRAN-DF, na qualidade de órgão gerenciador, a adesão de órgãos ou entidades da Administração Pública que não tenham participado do procedimento licitatório, desde que:

5.6.7.1. A possibilidade de adesão tenha sido expressamente prevista no edital e nos instrumentos convocatórios correspondentes;

5.6.7.2. Haja manifestação favorável do fornecedor ou prestador detentor da ata;

5.6.7.3. Seja demonstrada, no respectivo processo administrativo do órgão ou entidade não participante, a vantagem da adesão em relação a outros meios de contratação disponíveis.

5.6.8. As aquisições ou contratações adicionais decorrentes de adesões não poderão exceder, por órgão ou entidade não participante, a 50% (cinquenta por cento) dos quantitativos previstos para cada item registrado na ata de registro de preços, conforme originalmente definidos para o DETRAN-DF, na condição de órgão gerenciador, e para os órgãos participantes.

5.6.9. O quantitativo global das adesões de que trata esta cláusula não poderá ultrapassar, no total, o dobro do quantitativo de cada item registrado na ata de registro de preços para o DETRAN-DF e para os órgãos participantes, independentemente do número de adesões por órgãos não participantes.

5.6.10. As adesões autorizadas deverão preservar integralmente as condições técnicas, operacionais, pedagógicas e de garantia pactuadas nesta ata e no contrato dela decorrente, assegurando-se a observância da legislação aplicável, especialmente o Decreto Distrital nº 44.330/2023 e a Lei nº 14.133/2021.

5.7. Possibilidade de órgãos ou entes participantes sugerirem a inclusão de novos itens

5.7.1. Desde que não restrinja ou inviabilize o planejamento da contratação por parte deste Detran-DF e que eventuais itens tenha correlação lógica, técnica, operacional e justificável, eventuais interessados poderão sugerir a inclusão de novos itens, exigindo que sejam refeitas a pesquisa de preços e nova estimativa de custos.

5.8. Justificativa para possibilidade de adesões por entes não participantes (complementar ao ETP)

5.8.1. Preliminarmente, tem-se que a legislação vigente classifica a previsão ou não de adesão, como sendo decisão discricionária da Administração, condicionada à previsão disposta em edital. Tal previsão é condicionada à existência de justificativa, sujeita à limites quantitativos e subordinada à vantajosidade comprovada.

5.8.2. Importante destacar que órgãos de controle não vedam essa possibilidade, mas são acompanhadas pelos mesmos. O que órgãos de controle buscam combater é previsões sem justificativa, adesões sem planejamento, ilimitadas, que desvirtuem a competição ou utilizadas para contornar as exigências mínimas.

5.8.3. A definição, no instrumento convocatório e na Ata de Registro de Preços, da possibilidade de adesão por órgãos ou entidades não participantes, encontra respaldo no regime jurídico do Sistema de Registro de Preços instituído pela Lei nº 14.133/2021 e regulamentado, no âmbito da Administração Pública federal, pelo Decreto nº 11.462/2023.

5.8.4. Tal previsão não configura ampliação indevida do objeto, mas desdobramento legítimo de um procedimento auxiliar concebido para contratações futuras e eventuais de bens e serviços de natureza comum. A possibilidade de adesão qualifica-se como instrumento de racionalização das contratações públicas, especialmente adequados a objetos que demandam flexibilidade operacional, escalabilidade e contratação sob demanda, como é o caso de soluções que envolvem recursos avançados de tecnologia da informação vinculadas á demandas escalares. A lógica estrutural do SRP, ao dissociar o momento da seleção competitiva do fornecedor do momento da contratação efetiva, permite que múltiplas necessidades homogêneas sejam atendidas de forma coordenada, preservando-se a vantajosidade em cada contratação derivada e evitando a rigidez típica de contratos fechados que não acompanham a dinâmica tecnológica e operacional inerente a esse tipo de solução.

5.8.5. Sob a perspectiva da eficiência administrativa, a possibilidade de adesão evita a fragmentação de esforços e a proliferação de licitações paralelas para soluções equivalentes, que, no campo da segurança de TIC, tendem a gerar assimetrias técnicas, sobreposição de recursos, incompatibilidades e aumento do custo total de propriedade.

O compartilhamento do procedimento licitatório, aliado à contratação sob demanda, reduz custos operacionais, mitiga riscos procedimentais e assegura resposta mais célere às necessidades institucionais, em consonância com os princípios do planejamento, da eficiência e da boa administração consagrados na Lei nº 14.133/2021.

5.8.6. Do ponto de vista econômico, o compartilhamento do registro de preços potencializa ganhos de escala relevantes, ampliando o volume estimado de contratação e elevando o interesse de fornecedores qualificados. Em mercados intensivos em tecnologia e serviços especializados, como o de segurança de TIC, a previsibilidade de demanda ampliada reduz riscos comerciais, incentiva maior agressividade competitiva e favorece a apresentação de propostas mais vantajosas, refletindo positivamente na formação dos preços registrados. A vantajosidade, nesse contexto, não se limita ao momento da licitação, mas se projeta de forma dinâmica ao longo da vigência da ata, sendo reafirmada a cada contratação derivada mediante verificação de compatibilidade com o mercado.

5.8.7. Outro fundamento relevante reside na padronização técnica, funcional e contratual, essencial para soluções de segurança que demandam interações com outros recursos do mesmo segmento e consistência na gestão de serviços. A utilização compartilhada da ata contribui para reduzir riscos de dependência tecnológica, assimetria tecnológica excessiva e soluções isoladas, favorecendo a neutralidade tecnológica, a integração sistêmica e a eficiência da gestão contratual, inclusive no acompanhamento de níveis de serviço, desempenho e resultados alcançados.

5.8.8. No plano do planejamento e da governança, a abertura da ata à adesão decorre da identificação, na fase preparatória, de necessidades convergentes e previsíveis, devidamente registradas no Estudo Técnico Preliminar, sem afastar a exigência de motivação individualizada por parte dos órgãos não participantes no momento da adesão. Tal abordagem reforça a segregação de funções entre planejamento, licitação, gestão da ata e contratação derivada, reduzindo riscos decisórios e fortalecendo a rastreabilidade e a auditabilidade dos atos administrativos.

5.8.9. A permissão de adesão também se justifica como mecanismo de mitigação de riscos administrativos e orçamentários, ao reduzir a probabilidade de contratações emergenciais, soluções improvisadas ou fracionamento indevido da despesa. Ao consolidar necessidades comuns em um único procedimento estruturado, a Administração atua de forma preventiva, preservando a continuidade dos serviços e a coerência sistêmica do ordenamento jurídico das contratações públicas.

5.8.10. Sob a ótica da isonomia e da competitividade, não há qualquer prejuízo, uma vez que a disputa ocorre integralmente no certame originário, em ambiente público e competitivo, com regras claras e previamente conhecidas. A possibilidade de adesão, quando expressamente prevista, assegura previsibilidade ao mercado, igualdade de condições aos licitantes e segurança jurídica ao procedimento, não constituindo privilégio discricionário, mas faculdade condicionada a critérios objetivos e verificáveis.

5.8.11. Do ponto de vista do controle externo, a experiência consolidada demonstra que a adesão é admitida quando acompanhada de motivação específica, demonstração de vantagem, compatibilidade do objeto e verificação de preços, elementos que são preservados e reforçados quando a possibilidade de adesão é estruturada desde a origem do certame. Longe de fragilizar o controle, esse modelo amplia a transparência, facilita auditorias futuras e reduz litigiosidade decorrente de múltiplas contratações isoladas para objetos equivalentes.

5.8.12. Desta forma, podemos resumir como vantagens de tal previsão:

5.8.12.1. **Ganho de escala e economicidade**, ampliando a competição, reduzindo custos unitários, permitindo a diluição de custos administrativos comuns e evitando a multiplicidade de certames similares para o mesmo segmento;

5.8.12.2. **Racionalização administrativa**, evitando repetição de processos licitatórios, reduzindo custos operacionais, otimização de tempo e simplificação da máquina pública, atendendo o princípio da eficiência (art. 5º da 14.133);

5.8.12.3. **Padronização tecnológica ou de soluções**, garantindo maior eficiência, interoperabilidade e integração entre recursos tecnológicos, mantém padrão arquitetural e evita fragmentações contratuais;

5.8.12.4. **Previsibilidade de demandas futuras incertas**, decorrente da não definição prévia e equivocada de quantitativos, compossibilidade de expansões de acordo com a necessidade efetivamente apurada, unificada e replicável de forme escalar;

5.8.12.5. **Planejamento prévio**, demonstrado com a estruturação de estudo técnico preliminar robusto, contendo as estimativas projetadas, sem vínculo com a real situação ou construção de cenário para justificar quantidades, registrando os impactos positivos de adesões, especialmente em termos de custos unitários e sem fixação de limites;

5.8.12.6. **Limitação expressa de quantitativos**, em termos de entes possivelmente aderentes, do limite global da ata e de acordo com a real capacidade do futuro fornecedor;

5.8.12.7. **Comprovação de vantajosidade na adesão**, onde serão exigidas comprovações de planejamento prévio por parte dos interessados, de vantajosidade financeira decorrente de pesquisa de preços no momento das adesões, demonstrando a existência de vantajosidade;

5.8.12.8. **Preservação da isonomia**, com ampla divulgação das regras e possibilidades, estimativas, hipóteses e condições, afastando risco de alegações futuras de surpresas concorrenciais.

5.9. Vedação

5.9.1. É vedada a participação do órgão ou entidade em mais de uma ata de registro de preços com o mesmo objeto no prazo de validade daquela de que já tiver participado, salvo na ocorrência de ata que tenha registrado quantitativo inferior ao máximo previsto no edital.

6. MARCA

6.1. A presente contratação não considera a possibilidade de indicar ou vedar qualquer marca, fabricante ou produto.

7. REQUISITOS DA CONTRATAÇÃO

7.1. Requisitos Funcionais

7.1.1. São requisitos funcionais indispensáveis ao atendimento das necessidades:

REQUISITOS FUNCIONAIS DA SOLUÇÃO		
1.	Monitoramento contínuo e automatizado	A solução deverá permitir a supervisão ininterrupta das atividades de rede, com capacidade de identificar, em tempo real, comportamentos anômalos e potenciais incidentes de segurança que comprometam a confidencialidade, integridade ou disponibilidade das informações do órgão.
2.	Detecção e análise de anomalias	Deve prover mecanismos de análise comportamental que permitam a identificação autônoma de desvios de padrão em dispositivos e usuários, sem depender de listas de assinaturas ou de pré-configurações específicas, possibilitando correlação entre eventos e priorização de riscos.
3.	Resposta automatizada a incidentes	O sistema deverá permitir a execução automática de ações corretivas em caso de detecção de ameaças, reduzindo o tempo de exposição e o impacto sobre o ambiente computacional, mediante registro e rastreabilidade de todas as ações executadas.
4.	Correlação integrada de dados	Deve viabilizar a correlação entre eventos provenientes de diferentes camadas tecnológicas — rede, nuvem e dispositivos locais — de forma a propiciar visão unificada do ambiente e maior assertividade no diagnóstico de incidentes.

5.	Visibilidade e auditoria centralizada	A plataforma deverá fornecer painéis executivos e técnicos com visão consolidada das ocorrências e indicadores de segurança, permitindo rastreabilidade e exportação de relatórios com trilhas de auditoria para fins de controle e conformidade institucional.
6.	Capacidade de integração	O sistema deverá dispor de interfaces padronizadas (API ou equivalentes) que possibilitem integração com demais soluções tecnológicas da instituição, garantindo interoperabilidade e continuidade operacional, sem alterar a topologia existente de rede.
7.	Suporte a ambientes híbridos	A solução deverá permitir o monitoramento simultâneo de ativos locais e em nuvem, assegurando a análise integrada de dados provenientes de ambientes físicos, virtuais e SaaS utilizados pela Administração.
8.	Inteligência analítica e aprendizado adaptativo	A solução deverá empregar mecanismos analíticos de evolução contínua, capazes de aprimorar automaticamente a identificação de ameaças e reduzir falsos positivos, mediante análise histórica e contextual do ambiente monitorado.
9.	Capacidade de pesquisa e rastreamento externo	O sistema deverá permitir a coleta e análise de informações públicas e subterrâneas (fontes abertas e não indexadas) relacionadas a ameaças ou vazamentos de dados vinculados ao órgão, com capacidade de geração de alertas proativos.
10.	Gestão de incidentes e relatórios	Deve contemplar funcionalidades de registro, acompanhamento e encerramento de incidentes, geração automática de relatórios técnicos e executivos e mecanismos de priorização e atribuição de responsabilidade, em consonância com as boas práticas de governança de TIC (IN SEGES/ME nº 94/2021).
11.	Serviço contínuo e suporte especializado	O provedor deverá garantir operação ininterrupta (24x7x365) do ambiente contratado, com equipe especializada para acompanhamento, suporte técnico, comunicação de incidentes críticos e emissão de relatórios periódicos de desempenho e segurança.

7.1.2. Requisitos Legais

7.1.3. A pretendida contratação deverá observar, naquilo que couber, as seguintes legislações e normas:

REQUISITOS LEGAIS		
Id	**Norma**	**Descrição**
1.	Lei nº 14.133, de 1º de abril de 2021	Estabelece a Nova Lei de Licitações e Contratos Administrativos, dispondo sobre normas gerais para licitações e contratos no âmbito da Administração Pública direta, autárquica e fundacional de todos os entes da Federação, consolidando os princípios do planejamento, eficiência, economicidade e gestão de riscos.
2.	Decreto Distrital nº 44.330, de 18 de setembro de 2023	Regulamenta a aplicação da Lei nº 14.133/2021 no âmbito do Distrito Federal, estabelecendo regras específicas sobre planejamento das contratações, elaboração de ETP, gestão de riscos e execução contratual.
3.	Instrução Normativa SEGES/ME nº 94, de 23 de dezembro de 2022	Dispõe sobre o planejamento das contratações de Tecnologia da Informação e Comunicação (TIC) na Administração Pública Federal, definindo diretrizes e modelos para elaboração do Documento de Formalização da Demanda (DFD), do Estudo Técnico Preliminar (ETP) e do Termo de Referência (TR).
4.	Instrução Normativa SEGES/ME nº 58, de 8 de agosto de 2022	Institui a metodologia de Avaliação de Maturidade Institucional em Governança de TIC, estabelecendo parâmetros e níveis de evolução organizacional a serem considerados no planejamento e execução de contratações tecnológicas.
5.	Decreto Federal nº 10.747, de 28 de junho de 2021	Institui a Política de Governança de Tecnologia da Informação e Comunicação da Administração Pública Federal, com foco em princípios de integridade, eficiência, transparência e efetividade na gestão dos recursos digitais.
6.	Decreto Federal nº 10.947, de 25 de janeiro de 2022	Dispõe sobre o Plano de Contratações Anual (PCA) e o Sistema de Planejamento e Gerenciamento de Contratações (PGC), estabelecendo procedimentos para o planejamento e alinhamento das contratações às metas estratégicas institucionais.
7.	Decreto Federal nº 10.222, de 5 de fevereiro de 2020	Aprova a Estratégia Nacional de Segurança Cibernética (E-Ciber), definindo princípios, objetivos e diretrizes para o fortalecimento da resiliência cibernética da Administração Pública e a proteção das infraestruturas críticas de informação.

8.	Decreto Federal nº 9.637, de 26 de dezembro de 2018	Institui a Política Nacional de Segurança da Informação (PNSI), estabelecendo fundamentos e diretrizes para a governança e a proteção dos ativos informacionais da Administração Pública Federal.
9.	Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD)	Dispõe sobre o tratamento de dados pessoais e sobre a proteção da privacidade e dos direitos fundamentais de liberdade e de desenvolvimento da personalidade, aplicando-se a todos os órgãos e entidades da Administração Pública.
10.	Lei nº 14.129, de 29 de março de 2021 (Lei do Governo Digital)	Estabelece princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública, promovendo a transformação digital dos serviços públicos e a inovação tecnológica no setor público.
11.	Portaria SGD/MGI nº 1.070, de 1º de junho de 2023	Dispõe sobre a Política de Segurança da Informação e Cibernética da Administração Pública Federal, definindo diretrizes para gestão de riscos, governança de segurança digital, monitoramento contínuo e resposta a incidentes cibernéticos.
12.	Portaria SGD/MGI nº 852, de 28 de março de 2023	Dispõe sobre a Política de Governança Digital da Administração Pública Federal, estabelecendo princípios, objetivos e diretrizes para planejamento, interoperabilidade, dados e contratações digitais.
13.	Portaria SGD/MGI nº 778, de 4 de abril de 2019	Institui a Política de Segurança da Informação e Comunicações (POSIC) no âmbito da Administração Pública Federal, definindo responsabilidades, níveis de classificação da informação e diretrizes gerais de proteção e controle.
14.	Decreto-Lei nº 315, de 13 de março de 1967	Cria o Departamento de Trânsito do Distrito Federal (DETRAN-DF) no âmbito da Secretaria de Segurança Pública, estabelecendo sua natureza e competências institucionais originais.
15.	Lei Distrital nº 6.296, de 15 de janeiro de 1975	Transforma o Departamento de Trânsito do Distrito Federal em autarquia, vinculando-o ao Governo do Distrito Federal e conferindo-lhe autonomia administrativa, financeira e patrimonial.
16.	Normas Técnicas Complementares (Boas Práticas e Padrões de Governo Eletrônico)	Incluem os referenciais ISO/IEC 27001 e 27002 (segurança da informação), COBIT e ITIL (governança e gestão de serviços de TI), e os padrões e-Ping, e-MAG, e-PWG, ICP-Brasil e e-ARQ Brasil, aplicáveis a interoperabilidade, acessibilidade e conformidade técnica de sistemas públicos.

7.2. Requisitos Temporais

7.2.1. Para fins de execução contratual, ficam estabelecidos os seguintes critérios gerais aplicáveis à contagem de prazos, agendamento de eventos e atendimento de obrigações pelas partes envolvidas:

7.2.1.1. Nos termos do art. 6º do Decreto Distrital nº 44.330/2023, na contagem dos prazos previstos neste instrumento ou em quaisquer outros artefatos vinculados ao contrato, excluir-se-á o dia do começo e incluir-se-á o do vencimento, salvo disposição em contrário. Todos os prazos mencionados, salvo se expressamente definidos de outra forma, serão contados em dias corridos, inclusive aqueles relacionados à entrega de produtos, à resposta de chamados ou ao cumprimento de obrigações acessórias.

7.2.1.2. Os eventos presenciais, reuniões de acompanhamento, sessões de homologação e quaisquer atividades que demandem a participação de representantes do DETRAN-DF ocorrerão, via de regra, em dias úteis, de segunda a sexta-feira, das 08h às 18h, excluídos os feriados do Distrito Federal, salvo se pactuado de forma diversa entre as partes.

7.2.1.3. Da mesma forma, os eventos que envolvam a presença de integrantes da empresa contratada em ambientes do DETRAN-DF, deverão ocorrer dentro da mesma janela institucional (dias úteis, das 08h às 18h), ressalvados os casos em que houver acordo expresso entre as partes, devidamente formalizado.

7.2.1.4. O prazo para início da execução das Ordens de Serviço emitidas pelo DETRAN-DF será contado a partir do primeiro dia útil subsequente à formalização da Ordem, a qual poderá ser transmitida por qualquer dos meios oficiais de comunicação estabelecidos neste instrumento ou em documento posterior acordado entre as partes.

7.2.1.5. Excepcionalmente, poderá ser indicada outra data de início diretamente na própria Ordem de Serviço, desde que fundamentada pelo DETRAN-DF.

7.2.1.6. Abaixo, detalham-se os principais eventos contratuais e seus prazos de cumprimento, com base no cronograma e modelo de governança definido no planejamento:

EVENTO	**PRAZOS APLICÁVEIS**
Assinatura do Contrato	Deverá ocorrer no prazo de até 10 (dez) dias úteis contados do recebimento da convocação formal.
Reunião Inicial de Alinhamento	Deverá ocorrer no prazo de até 5 (cinco) dias úteis a contar da assinatura do contrato.
Disponibilização da Solução	Deverá ocorrer no prazo previsto no cronograma contratual, contados da assinatura do contrato.
Implantação / Customização / Integrações	Conforme Plano de Implantação a ser apresentado pela contratada e aprovado pelo DETRAN-DF.
Ordens de Serviço (acompanhamentos formais)	O prazo de resposta e execução será definido na própria OS, conforme sua gravidade e criticidade.
Recebimento Provisório	Após entrega formal da solução e validação funcional inicial, conforme critérios definidos no edital.
Recebimento Definitivo	Após decurso do prazo de observação e homologação técnica da solução, nos termos do art. 140 da Lei nº 14.133/2021.
Prazo de Pagamento	Efetuado conforme cláusula contratual específica, observando o disposto no art. 143 da Lei nº 14.133/2021.

Atendimento de Chamados / Suporte	Conforme matriz de severidade e níveis de serviço definidos no contrato ou plano de suporte técnico.
Janelas de Manutenção	Devem ser previamente acordadas com o DETRAN-DF e ocorrer preferencialmente fora do horário comercial.

7.2.1.7. Nos casos de urgência grave, especialmente aqueles que comprometam a segurança da informação, integridade de dados ou disponibilidade dos serviços essenciais, os prazos convencionais para atendimento poderão ser superados ou antecipados, conforme critério técnico e decisão fundamentada da fiscalização do contrato.

7.3. Requisitos de Ambientação Inicial

7.3.1. A contratada disporá de um prazo máximo de até 90 (noventa) dias corridos, contados a partir da data de conclusão da entrega inicial da solução, para fins de ambientação técnica, calibração operacional, integração sistêmica e adequação processual ao ambiente tecnológico do DETRAN-DF. Esse período terá por objetivo assegurar a correta assimilação dos fluxos de informação, protocolos de segurança, mecanismos de correlação de eventos, rotinas de monitoramento, e demais parâmetros técnicos necessários à execução plena e estável dos serviços contratados.

7.3.2. Durante essa fase, deverão ser conduzidas as ações de configuração de sensores, ajustes de coleta de telemetria, definição de perfis de análise e validação de integrações, sob supervisão da área técnica do DETRAN-DF, assegurando que a infraestrutura de defesa cibernética alcance sua capacidade operacional plena dentro dos padrões de desempenho esperados.

7.3.3. No período de ambientação, os níveis mínimos de serviço (SLAs) previstos contratualmente não serão exigidos em sua integralidade, sendo facultado ao DETRAN-DF o acompanhamento técnico orientativo das medições parciais. A suspensão temporária das métricas de desempenho não exime a contratada da observância de todas as demais obrigações contratuais, especialmente aquelas relacionadas à entrega tempestiva dos componentes da solução, à integridade das configurações e à qualidade dos registros e relatórios técnicos.

7.3.4. Caso sejam identificadas falhas que comprometam a operação ou a segurança do ambiente, a contratada deverá adotar, de imediato, as medidas corretivas necessárias, sob pena de aplicação das sanções previstas em contrato, conforme as disposições da Lei nº 14.133/2021 e do Decreto Distrital nº 44.330/2023.

7.3.5. Concluído o período de ambientação e não havendo manifestação expressa em sentido contrário pela fiscalização contratual, considerar-se-á plenamente iniciado o ciclo de exigibilidade dos SLAs, devendo tais parâmetros ser observados de forma rigorosa em todas as medições subsequentes. A partir deste marco, o desempenho da contratada será avaliado de acordo com as métricas de eficiência, eficácia e continuidade dos serviços de segurança cibernética, conforme disposto nos instrumentos de governança contratual e nos planos de monitoramento técnico validados pela Administração.

7.4. Requisitos da Reunião Inicial

7.4.1. A Reunião Inicial de Alinhamento deverá ser convocada e realizada pelo DETRAN-DF no prazo máximo de 10 (dez) dias úteis contados da assinatura do contrato, conforme o disposto no art. 132, §1º, do Decreto Distrital nº 44.330/2023, com a finalidade de garantir o nivelamento técnico e procedimental entre as partes, promover a integração das equipes envolvidas, validar os instrumentos de governança contratual e planejar a execução inicial das etapas do projeto.

7.4.2. A reunião terá caráter técnico-operacional e estratégico, devendo contemplar, no mínimo, os seguintes pontos:

7.4.2.1. Apresentação formal dos fiscais técnico e administrativo, bem como do gestor do contrato, designados pelo DETRAN-DF, e entrega do respectivo Plano de Fiscalização, elaborado nos termos do art. 63 do Decreto nº 44.330/2023, contendo metodologia, instrumentos de acompanhamento, frequência de verificação e matriz de responsabilidades.

7.4.2.2. Apresentação formal do preposto da contratada, devidamente indicado por carta assinada pelo representante legal, contendo nome completo, CPF e cargo do profissional que atuará como interlocutor técnico e administrativo junto ao DETRAN-DF, com poderes para receber comunicações, responder diligências e coordenar a execução operacional do contrato.

7.4.2.3. Entrega do Termo de Compromisso de Sigilo e do Termo de Ciência em Segurança da Informação, assinados pelo representante legal da contratada, pelo preposto designado e por todos os profissionais envolvidos na execução contratual, em conformidade com as normas internas do DETRAN-DF, a Lei nº 13.709/2018 (LGPD) e os princípios da Política Nacional de Segurança da Informação (Decreto nº 9.637/2018).

7.4.2.4. Apresentação do plano preliminar de implantação técnica, contemplando cronograma indicativo de configuração do ambiente, etapas de calibração dos mecanismos de segurança, definição de fluxos de comunicação com a equipe de resposta a incidentes e procedimentos de homologação.

7.4.2.5. Definição consensual das prioridades operacionais iniciais, com identificação de marcos críticos, pontos de controle e ações de mitigação de risco, assegurando alinhamento entre a contratada e as unidades técnicas do DETRAN-DF quanto às metas e resultados esperados.

7.4.2.6. Planejamento das atividades de integração e parametrização da solução contratada, incluindo definição de perfis de acesso, credenciais de autenticação, políticas de controle de usuários e critérios de interoperabilidade com sistemas preexistentes.

7.4.2.7. Apresentação do programa de transferência de conhecimento, com indicação de datas, conteúdos e metodologia de capacitação da equipe técnica do DETRAN-DF, priorizando a formação operacional e o domínio dos mecanismos de monitoramento, notificação e resposta a incidentes.

7.4.2.8. Análise conjunta do contrato, edital e anexos técnicos, com o objetivo de prevenir interpretações divergentes, garantir conformidade entre as partes e assegurar execução harmônica, contínua e alinhada aos objetivos estratégicos da Administração.

7.4.2.9. Esclarecimento de dúvidas administrativas e técnicas, inclusive quanto aos procedimentos de comunicação formal, critérios de aceitação de entregas, fluxo de aprovações e aplicação de penalidades, em conformidade com a Lei nº 14.133/2021.

7.4.2.10. Estabelecimento de prazo para apresentação da documentação comprobatória da qualificação técnica da equipe, incluindo currículos, certificados de capacitação e declarações de experiência compatíveis com as exigências do edital e da legislação vigente.

7.4.2.11. Todos os temas tratados deverão ser registrados em ata circunstanciada, lavrada e assinada por representantes de ambas as partes, a qual constituirá marco formal do início da execução contratual, servindo de referência para a contagem dos prazos de implantação e início da aferição dos indicadores de desempenho.

7.5. Requisitos de Aderência Técnica

7.5.1. O processo de seleção e futuro fornecimento deverão obedecer às seguintes diretrizes:

7.5.2. Cada proponente deverá indicar em sua proposta a solução (ões) ofertada (s), seus respectivos fabricantes, versões, Partnumbers, entre outros;

7.5.3. Tanto um eventual check-list, declaração do fabricante, ponto-a-ponto ou evento de amostra, deverão se referir a mesma solução informada;

7.5.4. A solução a ser fornecida deverá ser a mesma informada junto a proposta e aprovada no evento de amostra.

7.6. Requisitos de Padronização

7.6.1. As contratações públicas realizadas no âmbito do Distrito Federal devem observar o disposto no Decreto Distrital nº 44.330, de 16 de março de 2023, que regulamenta a aplicação da Lei Federal nº 14.133/2021 no território distrital. Nos termos do art. 81 do referido Decreto, a Administração deve, sempre que possível, adotar o princípio da padronização, assegurando a compatibilidade das especificações técnicas, funcionais e de desempenho dos bens e serviços, bem como a coerência quanto às condições de manutenção, suporte e garantias ofertadas.

7.6.2. No que tange ao segmento de segurança da informação e defesa cibernética, verifica-se que, até o presente momento, não há norma distrital de padronização vigente que discipline requisitos técnicos uniformes para este tipo de solução. Assim, inexiste impedimento jurídico para a definição das especificações com base em critérios técnicos usuais de mercado, desde que observadas as diretrizes de interoperabilidade, conformidade normativa e alinhamento às políticas de segurança da informação da Administração Pública.

7.6.3. O objeto em estudo constitui-se de serviços tecnológicos especializados de monitoramento e resposta a incidentes cibernéticos, enquadrando-se, portanto, como bem e serviço comum de tecnologia, conforme as definições da Instrução Normativa SEGES/ME nº 94/2022, cuja descrição técnica pode ser padronizada por meio de requisitos de desempenho, capacidade e confiabilidade, sem vinculação a fabricantes, modelos ou marcas específicas.

7.6.4. Ainda que inexista padronização formal instituída pelo Governo do Distrito Federal para esta categoria tecnológica, a presente contratação observará, como diretriz técnica e estratégica, a necessidade de uniformidade operacional e coerência arquitetural entre os componentes da solução. Essa medida visa assegurar compatibilidade funcional, facilidade de integração, homogeneidade na experiência de uso e racionalização de custos de operação, capacitação e manutenção, alinhando-se ao princípio da eficiência administrativa e aos objetivos institucionais do DETRAN-DF, especialmente no tocante à proteção de dados, continuidade dos serviços e resguardo da

infraestrutura tecnológica crítica da Autarquia.

7.7. Requisitos de Projeto de Implementação

7.7.1. Compete à empresa contratada a execução integral de todas as etapas do projeto de implementação da solução tecnológica, abrangendo atividades de disponibilização, configuração, integração, parametrização e ativação operacional, de modo a assegurar o funcionamento pleno e contínuo de todos os componentes, módulos, serviços e funcionalidades previstos. Todas as ações deverão observar os requisitos técnicos, cronogramas e padrões de desempenho definidos no Termo de Referência, nos anexos contratuais e nas normas aplicáveis da Lei nº 14.133, de 1º de abril de 2021, e do Decreto Distrital nº 44.330, de 16 de março de 2023.

7.7.2. A execução da implantação dependerá de manifestação técnica formal do DETRAN-DF, emitida após a aprovação do Plano de Implementação submetido pela contratada. Nenhum procedimento que envolva acesso ao ambiente de produção, manipulação de dados institucionais ou emissão de credenciais de acesso poderá ser iniciado sem o ateste prévio da Administração, em observância ao art. 71 da Lei nº 14.133/2021 e às diretrizes de controle de segurança da informação vigentes.

7.7.3. Todos os recursos tecnológicos e operacionais indispensáveis ao desempenho contratual, inclusive ferramentas auxiliares, componentes de hardware e software ou integrações complementares, ainda que não expressamente descritos na proposta técnica, integram o escopo de responsabilidade da contratada. Tais elementos deverão ser fornecidos de forma regularizada, licenciada e plenamente funcional, sem ônus adicional ao erário, em consonância com o princípio da responsabilidade integral da execução contratual previsto no art. 117 da Lei nº 14.133/2021.

7.7.4. A contratada deverá manter documentação técnica completa e continuamente atualizada sobre todas as fases da implementação, incluindo planos de trabalho, cronogramas, atas técnicas, registros de testes, homologações, relatórios de acompanhamento e manuais operacionais. Ao término da implantação, deverá ser apresentado à fiscalização o dossiê técnico consolidado (“as built”), contendo a totalidade dos registros, diagramas, certificações e demais evidências comprobatórias da conformidade do projeto, conforme as exigências do art. 141, §1º, do Decreto Distrital nº 44.330/2023.

7.7.5. Durante a execução da implementação, caberá exclusivamente à contratada identificar, diagnosticar e corrigir eventuais falhas, inconsistências ou incidentes técnicos, inclusive aqueles decorrentes da integração entre módulos e componentes da solução. Caso, após análise técnica fundamentada e aceita pela fiscalização, seja constatado que o evento decorre de causas externas ou de responsabilidade do DETRAN-DF, a Administração adotará as providências corretivas sob sua competência, observando-se a boa-fé contratual e a repartição de responsabilidades prevista no art. 137 da Lei nº 14.133/2021.

7.7.6. A presente contratação não contempla o desenvolvimento de software sob demanda, razão pela qual não se aplicam metodologias típicas de engenharia de software, tais como modelagens, versionamento contínuo (CI/CD) ou processos ágeis de desenvolvimento. O objeto contratual restringe-se à implantação de solução de mercado pronta (COTS – Commercial Off-The-Shelf), configurável e parametrizável conforme as necessidades operacionais do DETRAN-DF.

7.7.7. Concluída a etapa de implementação, a contratada deverá entregar a solução totalmente instalada, configurada e operacional, com todos os módulos integrados, funcionalidades ativas e documentação validada, apta ao início da execução regular dos serviços e à aferição dos indicadores de desempenho e níveis de serviço (SLAs) previstos nos instrumentos de governança contratual, em conformidade com o art. 132 do Decreto Distrital nº 44.330/2023 e as boas práticas de gestão de contratos de tecnologia da informação.

7.8. Requisitos de Arquitetura

7.8.1. A arquitetura tecnológica da solução deverá observar integralmente as diretrizes técnicas e de segurança definidas pela área responsável do DETRAN-DF, em conformidade com o Termo de Referência, o art. 6º, inciso XXIV, da Lei nº 14.133/2021, e as disposições correlatas do Decreto Distrital nº 44.330/2023, assegurando compatibilidade, interoperabilidade e aderência às políticas institucionais de tecnologia da informação e governança digital.

7.8.2. A utilização de arquitetura, componentes ou tecnologias distintas das aprovadas pela Administração dependerá de autorização técnica formal do DETRAN-DF. Na ausência dessa autorização, fica vedada qualquer modificação na arquitetura validada, sob pena de caracterizar inexecução contratual, conforme o art. 137 da Lei nº 14.133/2021.

7.9. Requisitos de Implantação

7.9.1. A implantação da solução deverá observar o uso de tecnologias, padrões e diretrizes estabelecidos no Documento de Arquitetura de Sistemas do DETRAN-DF, em conformidade com as normas internas de tecnologia da informação e com o disposto no art. 6º, inciso XXIV, da Lei nº 14.133/2021, que exige a descrição precisa e suficiente dos requisitos técnicos.

7.9.2. Todas as etapas de implantação deverão ser conduzidas segundo as orientações técnicas da área de tecnologia da informação do DETRAN-DF, assegurando conformidade com os padrões de interoperabilidade, segurança, autenticação e rastreabilidade definidos pela instituição e previstos no Decreto Distrital nº 44.330/2023.

7.9.3. O processo de implantação deverá seguir as diretrizes específicas do Termo de Referência e seus anexos, garantindo a aderência entre o planejamento técnico, as especificações contratuais e os parâmetros de governança estabelecidos pela Administração.

7.10. Requisitos de Sustentabilidade

7.10.1. A futura CONTRATADA deverá declarar que atende aos requisitos de sustentabilidade previstos no art. 2º, da Lei Distrital nº 4.770/2012, em conformidade com o Decreto nº 7.746/2012 ou outro que vier a substituí-lo, estabelece a implementação de critérios, práticas e ações de logística sustentável no âmbito da Administração Pública do Distrito Federal direta, autárquica e fundacional e das empresas estatais dependentes, devendo ser observados os requisitos ambientais com menor impacto ambiental em relação aos seus similares.

7.11. Requisitos de Capacitação e Transferência de Conhecimento

7.11.1. A transferência de conhecimento técnico decorrente da execução contratual tem por finalidade assegurar a assimilação, pela equipe do DETRAN-DF, das informações e procedimentos técnicos essenciais à operação, supervisão e evolução da solução implantada, de modo a garantir autonomia institucional na gestão e continuidade do serviço, em conformidade com o art. 11, inciso IV, da Lei nº 14.129/2021 (Lei do Governo Digital), que prevê a promoção da capacitação e da gestão do conhecimento no âmbito da administração pública digital.

7.11.2. O Termo de Referência deverá prever o processo de transferência de conhecimento técnico, contemplando a documentação dos procedimentos realizados, a entrega de relatórios explicativos, manuais e registros operacionais, e a realização de reuniões técnicas de nivelamento, quando necessário, observando o disposto no art. 6º, inciso XXIV, da Lei nº 14.133/2021 e no Decreto Distrital nº 44.330/2023, quanto à precisão e rastreabilidade das informações geradas durante a execução contratual.

7.12. Requisitos de Metodologia de Trabalho

7.12.1. A execução do contrato somente poderá iniciar-se após a assinatura do instrumento contratual e a publicação de seu extrato no Diário Oficial do Distrito Federal, conforme o disposto no art. 94, inciso III, da Lei nº 14.133/2021 e no art. 130 do Decreto Distrital nº 44.330/2023, que condicionam a eficácia dos contratos administrativos à respectiva publicação oficial.

7.12.2. O início do fornecimento da solução tecnológica — compreendendo a disponibilização dos componentes, serviços e recursos contratados — ocorrerá automaticamente após a assinatura do contrato, dispensada a emissão de Ordem de Serviço inicial, salvo se a Administração determinar de forma diversa por justificativa técnica formal.

7.12.3. As obrigações contratuais de natureza continuada, como suporte técnico, manutenção, relatórios, atualização de componentes e demais serviços correlatos, deverão observar os prazos e condições fixados neste instrumento e em seus anexos, podendo ser formalmente acionadas por Ordem de Serviço emitida pelo gestor ou fiscais do contrato, em conformidade com o art. 117 da Lei nº 14.133/2021.

7.12.4. Após a designação do gestor e dos fiscais, deverá ser realizada a Reunião Inicial de Alinhamento, nos termos do art. 132, §1º, do Decreto Distrital nº 44.330/2023, para nivelar entendimentos sobre as condições contratuais, apresentar as equipes envolvidas, esclarecer dúvidas e pactuar os fluxos formais de comunicação e fiscalização.

7.12.5. Demandas complementares dentro do escopo contratual deverão ser formalizadas pelo DETRAN-DF ao preposto da contratada, com indicação técnica, prazos e critérios de entrega. A contratada deverá responder oficialmente quanto à viabilidade e cronograma de execução. O não atendimento injustificado poderá ensejar a aplicação das sanções previstas nos arts. 156 e 157 da Lei nº 14.133/2021.

7.12.6. A empresa a ser contratada, executará os serviços, seguindo os processos, padrões, modelos, normas e procedimentos definidos e autorizados por este Órgão e especificados em anexo.

7.12.7. A CONTRATADA deverá fornecer meios para contato e registro de ocorrências do funcionamento do serviço contratado, funcionando 24 horas por dia e 7 dias por semana por via telefônica ou meios eletrônicos.

7.12.8. A empresa a ser contratada, deverá produzir toda a documentação em conformidade com os critérios de aceitação solicitados por este Órgão, de acordo com as definições e padrões mínimos.

7.12.9. A empresa a ser contratada, não poderá se negar ou deixar de executar nenhuma Ordem de Serviço demandada que esteja prevista no escopo da contratação.

7.12.10. Quando houver impedimentos ou fatos alheios à responsabilidade da contratada que possam inviabilizar ou retardar a execução, esta deverá notificar imediatamente a Administração, relatando as circunstâncias e seus reflexos sobre o cronograma, conforme o princípio da boa-fé contratual previsto no art. 137 da Lei nº 14.133/2021.

7.12.11. A empresa a ser contratada, deverá apresentar justificativa formal sobre eventuais atrasos ou paralisação dos serviços, cabendo ao Gestor do Contrato acatar ou não a justificativa.

7.12.12. As manutenções corretivas e atualizações evolutivas vinculadas à garantia deverão ser prestadas sem custo adicional à Administração, dentro dos prazos fixados contratualmente. A contratada deverá manter canal de atendimento técnico ininterrupto (24 x 7) por meios eletrônicos e telefônicos, com registro formal das ocorrências, observando as regras de rastreabilidade definidas no Decreto Distrital nº 44.330/2023.

7.12.13. A contratada deverá elaborar e manter atualizada toda a documentação técnica e operacional pertinente à execução contratual, incluindo manuais, relatórios, registros de entregas e materiais de apoio, conforme os padrões exigidos pelo DETRAN-DF e o disposto no art. 141 do Decreto Distrital nº 44.330/2023.

7.12.14. É vedado à contratada recusar o cumprimento de obrigações relacionadas ao objeto contratual. Em caso de impossibilidade técnica comprovada, deverá comunicar formalmente o gestor do contrato, apresentando justificativa detalhada para deliberação administrativa, nos termos do art. 138 da Lei nº 14.133/2021.

7.12.15. O DETRAN-DF poderá convocar reuniões técnicas a qualquer tempo, a fim de discutir desempenho, propor melhorias ou tratar de eventuais ajustes operacionais, garantindo a melhoria contínua da execução e a eficiência do serviço.

7.12.16. As atividades deverão ser executadas, preferencialmente, em instalações da contratada, salvo quando a natureza do serviço exigir atuação presencial nas dependências do DETRAN-DF, hipótese em que serão definidos local e cronograma específicos, mediante agendamento prévio entre as partes.

7.12.17. O endereço para prestação dos serviços presenciais constará no futuro edital.

7.13. Requisitos de Garantia

7.13.1. Durante toda a vigência contratual, a contratada permanecerá integral e exclusivamente responsável pela garantia da solução fornecida, devendo corrigir, sem ônus adicional para o DETRAN-DF, quaisquer falhas, defeitos técnicos, erros de configuração ou inconformidades operacionais que afetem o desempenho, a estabilidade, a integridade funcional ou a qualidade dos serviços contratados, em conformidade com o art. 137 da Lei nº 14.133/2021 e com as condições estabelecidas no contrato.

7.13.2. A garantia compreenderá a sustentação técnica plena da solução, abrangendo suas funcionalidades, dados processados, fluxos de operação, mecanismos de autenticação, recursos analíticos e demais componentes necessários ao adequado funcionamento do serviço, de forma a assegurar disponibilidade, confiabilidade e continuidade durante todo o período contratual, observando o disposto no Decreto Distrital nº 44.330/2023 quanto às obrigações de desempenho e continuidade da execução.

7.13.3. A contratada deverá apresentar à Administração processo formal de acionamento de suporte e garantia, com definição de canais de atendimento, fluxos de registro e triagem, classificação de incidentes, critérios de prioridade e prazos máximos de resposta e resolução, conforme níveis de severidade. O suporte técnico deverá operar ininterruptamente (24x7), por meios eletrônicos e telefônicos, para atendimento de ocorrências críticas, em conformidade com o princípio da eficiência previsto no art. 5º do Decreto Distrital nº 44.330/2023.

7.13.4. A contratada deverá designar formalmente equipe técnica qualificada para o atendimento de chamados e suporte à operação, informando nomes, funções e contatos atualizados. Deverá ainda garantir a rastreabilidade integral das ações corretivas, assegurando comunicação direta e tempestiva com o DETRAN-DF sempre que houver impacto na prestação dos serviços.

7.13.5. Todos os procedimentos de correção e atendimento realizados no âmbito da garantia deverão ser documentados e auditáveis, mediante emissão de relatórios técnicos contendo descrição das falhas, ações executadas, logs de sistema e comprovação da regularização. Esses registros deverão ser disponibilizados à fiscalização contratual, para verificação e arquivamento, conforme o art. 141 do Decreto Distrital nº 44.330/2023.

7.14. Requisitos de Manutenção

7.14.1. A solução contratada deverá incluir, sem qualquer custo adicional para o DETRAN-DF, os serviços de manutenção técnica e operacional durante toda a vigência contratual, com o objetivo de garantir funcionalidade, disponibilidade, desempenho, atualização e segurança contínua da plataforma e de seus componentes tecnológicos, conforme os princípios da Lei nº 14.133/2021 e as disposições do Decreto Distrital nº 44.330/2023.

7.14.2. Para os efeitos deste contrato, entende-se por manutenção toda intervenção técnica — preventiva, corretiva ou evolutiva — destinada a assegurar o funcionamento adequado da solução, a correção de falhas e a mitigação de riscos operacionais, conforme diretrizes da área técnica do DETRAN-DF.

7.14.3. As atividades de manutenção contratual serão classificadas da seguinte forma:

7.14.3.1. Preventiva: ações proativas voltadas à prevenção de falhas, indisponibilidades e vulnerabilidades, incluindo inspeções periódicas, atualizações de segurança e testes de integridade;

7.14.3.2. Evolutiva: aperfeiçoamentos e atualizações decorrentes da evolução tecnológica, de mudanças normativas ou de requisitos operacionais;

7.14.3.3. Corretiva: intervenções destinadas à correção de falhas, defeitos ou comportamentos indevidos, a serem tratadas dentro dos prazos definidos nos acordos de nível de serviço (SLA).

7.14.4. Não serão consideradas manutenções — devendo ser tratadas como novas demandas ou alterações de escopo — as intervenções que impliquem reengenharia da solução, integração com sistemas não previstos ou reconfiguração total do ambiente, salvo se decorrerem de obrigação legal, contratual ou de necessidade institucional de continuidade, conforme o art. 137 da Lei nº 14.133/2021, se couber.

7.14.5. Todos os serviços de manutenção deverão ser executados diretamente pela contratada, sendo vedada a terceirização dessa atividade. A contratada será plenamente responsável pelos profissionais envolvidos, pelos acessos concedidos e pela rastreabilidade das ações realizadas, em observância ao art. 117 da Lei nº 14.133/2021.

7.14.6. Qualquer manutenção que envolva potencial impacto operacional deverá ser previamente comunicada e autorizada pela Administração, mediante solicitação formal de janela de manutenção, contendo, no mínimo: data e horário previstos, justificativa técnica, atividades a serem executadas, identificação dos profissionais responsáveis (nome e CPF) e os acessos necessários.

7.14.7. A autorização de execução dependerá de análise técnica da área de tecnologia da informação do DETRAN-DF, podendo ser negada ou reagendada por motivos de conveniência administrativa, indisponibilidade operacional ou riscos à continuidade dos serviços, conforme o art. 141 do Decreto Distrital nº 44.330/2023.

7.14.8. Durante toda a execução contratual, a contratada deverá manter base histórica e auditável das manutenções realizadas, contendo relatórios técnicos, logs, registros de testes e evidências de correções, a serem apresentados à fiscalização sempre que requisitado, para fins de controle e auditoria contratual.

7.14.9. Em razão da natureza crítica do objeto, que envolve a continuidade de serviços públicos essenciais, os níveis de serviço (SLAs) deverão refletir a gravidade e a urgência dos incidentes, assegurando resposta prioritária e resolução imediata para ocorrências de alta severidade, preferencialmente por atendimento remoto ininterrupto (24x7), com acionamento presencial quando necessário.

7.15. Requisitos específicos aplicáveis ao objeto

7.15.1. Gestão de Vulnerabilidades

7.15.1.1. A contratada deverá manter processo contínuo de identificação e análise de vulnerabilidades em superfície de ataque, com relatórios técnicos periódicos à fiscalização.

7.15.2. Resposta a Incidentes de Segurança

7.15.2.1. Deverá ser estruturado plano formal de resposta a incidentes, em conformidade com o Guia de Resposta a Incidentes (SGD/2024), a Portaria SGD/MGI nº 852/2023 e o Decreto nº 10.748/2021, contendo fluxos de comunicação, papéis, prazos e relatórios de conclusão.

7.15.3. Gestão de Controle de Acesso

7.15.3.1. Os acessos deverão seguir os princípios de menor privilégio e necessidade de saber, com autenticação multifatorial e rastreabilidade de ações, conforme o Modelo de Política de Controle de Acesso (SGD/2023) e o art. 46 da Lei nº 13.709/2018 (LGPD).

7.15.4. Registro e Rastreabilidade de Eventos

7.15.4.1. Todos os eventos e acessos deverão ser registrados em logs protegidos e auditáveis, em conformidade com o Guia de Requisitos e Obrigações (SGD/2024) e com o art. 141 do Decreto Distrital nº 44.330/2023.

7.15.5. Proteção de Dados Pessoais

7.15.5.1. O tratamento de dados deverá observar o art. 46 da LGPD, aplicando controles técnicos e administrativos para prevenir acesso indevido, perda ou comunicação não autorizada.

7.15.6. Gestão de Mudanças e Atualizações

7.15.6.1. Qualquer alteração em componentes ou configurações deverá ser precedida de análise de impacto, aprovação técnica e registro formal, conforme a ABNT NBR ISO/IEC 27005:2011 e o Decreto Distrital nº 44.330/2023.

7.15.7. Backup e Continuidade Operacional

7.15.7.1. Deverão ser mantidas cópias de segurança e plano de recuperação em conformidade com o Guia de Requisitos e Obrigações (SGD/2024) e o art. 117 da Lei nº 14.133/2021.

7.15.8. Segurança das Interfaces e APIs

7.15.8.1. As integrações deverão cumprir o Guia de Requisitos Mínimos para APIs Públicas (SGD/2024), com possibilidade de realizar integrações.

7.15.9. Auditoria e Conformidade Técnica

7.15.9.1. A contratada deverá disponibilizar evidências auditáveis que comprovem conformidade com os controles da ISO/IEC 27001:2013 e ISO/IEC 27701:2019, conforme o art. 50 da LGPD.

7.15.10. Governança de TIC e Responsabilidade Institucional

7.15.10.1. A solução deverá seguir as diretrizes da Portaria nº 778/2019, com gestão por resultados, transparência e controle de desempenho, alinhada ao PDTIC do DETRAN-DF e ao Decreto Distrital nº 44.330/2023.

7.15.11. Conformidade com o PPSI – Programa de Privacidade e Segurança da Informação

7.15.11.1. Deverão ser observados os controles definidos na Portaria SGD/MGI nº 852/2023, garantindo disponibilidade, integridade, confidencialidade e autenticidade das informações tratadas.

7.15.12. Gestão de Ativos de Informação

7.15.12.1. Os ativos físicos, lógicos e digitais deverão ser classificados e protegidos segundo o Modelo de Política de Gestão de Ativos (SGD/2023) e o art. 46 da LGPD.

7.15.12.2. Deverão ser aplicadas práticas de segurança cibernética alinhadas à Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC) e ao Centro Integrado de Segurança Cibernética do Governo Digital, conforme o Decreto nº 10.748/2021.

7.15.13. Gestão de Dados e Privacidade

7.15.13.1. O tratamento de dados institucionais deverá seguir as diretrizes do Guia de Governança de Dados Pessoais (SGD/2023) e os princípios da Lei nº 13.709/2018.

7.15.14. Resposta a Incidentes e Comunicação de Ocorrências

7.15.14.1. Deverá existir plano de resposta e comunicação de incidentes, com classificação de severidade e prazos de resolução, conforme o art. 14 da Portaria SGD/MGI nº 852/2023.

7.15.15. Rastreabilidade e Evidência Técnica

7.15.15.1. Todas as ações de segurança deverão gerar evidências documentadas, disponíveis à fiscalização, conforme o art. 141 do Decreto Distrital nº 44.330/2023.

7.16. Requisitos de Segurança

7.16.1. A execução contratual deverá observar as políticas e normas de segurança da informação adotadas pelo DETRAN-DF, incluindo a POSIC, a Política de Governança Digital, as diretrizes do DSI/GSI-PR, e as Instruções Normativas SEGES/ME nº 94/2021 e nº 1/DSIC/GSIPR, conforme o Decreto Distrital nº 44.330/2023.

7.16.2. A contratada deverá assegurar a confidencialidade, integridade, disponibilidade, autenticidade e não repúdio das informações tratadas, implementando controles técnicos e organizacionais compatíveis com os riscos, conforme os arts. 6º e 46 da Lei nº 13.709/2018 (LGPD).

7.16.3. Todos os dados e informações processados deverão estar protegidos contra perda, alteração, vazamento, uso indevido ou destruição, sendo vedada qualquer exploração econômica ou científica desses registros.

7.16.4. Ao término do contrato ou em caso de rescisão, os dados sob custódia da contratada deverão ser devolvidos ao DETRAN-DF de forma íntegra e auditável, com termo formal de transferência de guarda, vedado o armazenamento posterior sem autorização da Administração.

7.16.5. Os serviços deverão ser executados em conformidade com os procedimentos de segurança e controle de acesso do DETRAN-DF, observando segregação de funções, perfis de usuários, criptografia e registros de log auditáveis.

7.16.6. O representante legal da contratada e todos os colaboradores designados deverão assinar Termo de Compromisso e de Ciência em Segurança da Informação, condição indispensável para acesso a dados institucionais.

7.16.7. A contratada deverá manter Plano de Continuidade e Recuperação de Desastres, prevendo estratégias e recursos para restabelecimento de serviços e dados em caso de incidentes, com testes periódicos e supervisão da fiscalização.

7.16.8. Recomenda-se que a contratada utilize soluções com certificações ISO/IEC 27001 e ISO/IEC 27701 ou equivalentes, em conformidade com as boas práticas do Programa de Privacidade e Segurança da Informação – Portaria SGD/MGI nº 852/2023.

7.17. Requisitos de segurança da informação e privacidade

7.17.1. A solução contratada deverá atender integralmente às normas nacionais de proteção de dados pessoais e segurança da informação, observando os princípios e disposições da Lei nº 13.709/2018 (LGPD), especialmente no tratamento de dados de servidores, colaboradores, estudantes e usuários vinculados ao DETRAN-DF.

7.17.2. Considerando que a execução contratual poderá envolver armazenamento remoto, processamento e tráfego de dados institucionais, deverão ser rigorosamente cumpridas as seguintes diretrizes:

7.17.2.1. Fixação de foro brasileiro para solução de eventuais controvérsias contratuais, com renúncia expressa a qualquer outro;

7.17.2.2. As análises de Inteligência Artificial da dados de rede deverão ser realizadas 100% de forma local, sem envio de dados para nuvem;

7.17.2.3. Licenciamento pleno e contínuo da solução, sem restrições técnicas ou comerciais que limitem as prerrogativas legais da Administração;

7.17.2.4. Garantia de titularidade e domínio exclusivo do DETRAN-DF sobre os dados, sendo vedada qualquer forma de uso, cópia, monetização ou mineração pela contratada;

7.17.2.5. Disponibilidade de criptografia de Estado ou equivalente, conforme os níveis de sigilo e inviolabilidade exigidos pelo DETRAN-DF;

7.17.2.6. Proibição expressa de replicação, espelhamento ou uso indevido de dados sob gestão da contratada;

7.17.2.7. Implementação de controles de acesso segregados, rastreabilidade de logs e proteção de dados sensíveis, conforme os arts. 46 e 49 da LGPD.

7.17.3. A contratada deverá firmar Termo de Confidencialidade Institucional, subscrito por seu representante legal, comprometendo-se a não divulgar, transferir ou permitir acesso a dados e registros produzidos durante a execução, salvo mediante autorização formal do DETRAN-DF.

7.17.4. Todos os profissionais vinculados à execução deverão assinar Termo de Ciência e Responsabilidade, declarando conhecimento das normas e obrigações relativas à proteção de dados, sigilo e segurança da informação, os quais deverão permanecer arquivados e disponíveis à fiscalização.

7.17.5. A contratada deverá notificar imediatamente o DETRAN-DF em caso de desligamento de qualquer colaborador envolvido no contrato, para que sejam providenciados bloqueio de acessos e revogação de credenciais eletrônicas, em conformidade com o art. 46 da LGPD.

7.17.6. Deverá também colaborar com as políticas internas de segurança, sugerindo e aplicando boas práticas como limitação de tentativas de login, renovação periódica de senhas, autenticação multifatorial e monitoramento automatizado de acessos não autorizados, em conformidade com a IN GSI/PR nº 1/2020 e a Portaria SGD/MGI nº 852/2023.

7.18. Requisitos de Qualidade

7.18.1. A solução de segurança cibernética a ser contratada deverá manter, durante toda a vigência, conformidade plena com os requisitos técnicos e operacionais definidos

neste artefato, assegurando desempenho estável, cobertura integral do ambiente monitorado e aderência aos objetivos estratégicos do DETRAN-DF em proteção da informação e continuidade dos serviços públicos.

7.18.2. Deverão ser formalizados Acordos de Nível de Serviço (SLAs) que estabeleçam parâmetros claros de disponibilidade, tempo de resposta, resolução de incidentes e atualização de ameaças, permitindo aferição objetiva e responsabilização contratual, conforme o art. 115 da Lei nº 14.133/2021 e o Decreto Distrital nº 44.330/2023.

7.18.3. A qualidade da execução será verificada por meio de relatórios técnicos periódicos, contendo evidências automáticas da efetiva operação da solução, da precisão dos alertas, da estabilidade do ambiente e do cumprimento dos indicadores de desempenho definidos pela Administração.

7.18.4. A contratada deverá implantar e acompanhar Acordos de Nível de Serviço (SLAs) específicos para segurança da informação, tais como taxa de detecção, tempo médio de resposta, redução de falsos positivos e disponibilidade dos painéis de monitoramento.

7.18.5. Os mecanismos da solução deverão possibilitar avaliação periódica da eficácia dos controles de segurança, gerando relatórios quantitativos e qualitativos que subsidiem a fiscalização na mensuração da maturidade cibernética do órgão.

7.18.6. A contratada deverá assegurar emissão automatizada de registros técnicos e evidências de conformidade, com integridade criptográfica e rastreabilidade completa, permitindo verificação independente pela fiscalização.

7.18.7. A aferição de qualidade considerará a atualização contínua das bases de ameaça, a eficiência dos mecanismos de correlação e análise de eventos, a conformidade com a Política de Segurança da Informação do DETRAN-DF, e o alinhamento às diretrizes do Programa de Privacidade e Segurança da Informação – Portaria SGD/MGI nº 852/2023.

7.18.8. O não atingimento dos níveis mínimos de desempenho e confiabilidade técnica, comprovado por registros objetivos ou auditoria contratual, ensejará aplicação das sanções previstas nos arts. 156 e 157 da Lei nº 14.133/2021 e no Decreto Distrital nº 44.330/2023, incluindo glosas, advertência e eventual rescisão contratual.

7.19. Requisitos sociais, ambientais e culturais

7.19.1. Tanto a futura CONTRATADA quanto seus funcionários e colaboradores, deverão se submeter às diretrizes, padrões e requisitos de segurança da informação em uso ou futuramente adotados pelo DETRAN-DF;

7.19.2. Os funcionários e colaboradores deverão se comportar de forma educada e respeitosa, quando estiver no ambiente do DETRAN-DF ou em qualquer tipo de contato a ser realizado;

7.19.3. No que se refere aos aspectos culturais e sociais, os funcionários e colaboradores deverão atender somente demandas relacionadas com o objeto a ser contratado;

7.19.4. Não poderão se comportar de forma a criar ou modificar regras e protocolos existentes, nem criar novos serviços que possam ocasionar mudanças culturais na instituição;

7.19.5. Toda e qualquer comunicação deverá ser realizada ou redigida em língua portuguesa, escrita e falada no Brasil, em conformidade com as normas técnicas e jurídicas aplicáveis;

7.19.6. Os profissionais designados para prestar serviços no ambiente do DETRAN-DF deverão apresentar-se devidamente identificados e trajados de forma condizente com o ambiente de trabalho, de modo a resguardar a imagem institucional e evitar o uso de vestuário que possa comprometer a seriedade e a formalidade da instituição;

7.19.7. É imprescindível que os profissionais mantenham respeito e cordialidade com todos os colaboradores, independentemente da posição hierárquica, prezando pela comunicação eficiente e pelo relacionamento interpessoal positivo, promovendo um ambiente de trabalho harmonioso;

7.19.8. A futura CONTRATADA será responsável pelo recolhimento adequado de todos os consumíveis utilizados, bem como pelos resíduos gerados nos processos de manutenção e limpeza dos locais onde os serviços forem prestados, assegurando que esses resíduos sejam tratados de forma ambientalmente correta, conforme as normas vigentes;

7.19.9. Todos os componentes da solução ofertada deverão possuir funcionalidades que contribuam para a economia de energia elétrica, como o modo de economia de energia ou outras tecnologias sustentáveis, visando a redução do impacto ambiental das operações do DETRAN-DF.

7.20. Requisito de Experiência Profissional

7.20.1. Toda e qualquer responsabilidade pela composição, qualificação, formação e experiência dos profissionais especializados vinculados à execução do contrato caberá integralmente à futura CONTRATADA, que deverá garantir a alocação de equipe tecnicamente habilitada e dimensionada de forma compatível com a complexidade das atividades a serem desempenhadas.

7.20.2. A formação acadêmica, certificações e experiência profissional dos especialistas que venham a atuar sob responsabilidade da contratada constituem obrigação exclusiva desta, devendo atender aos padrões técnicos e éticos exigidos pela legislação aplicável e pelos normativos de segurança, tecnologia e governança previstos na Lei nº 14.133/2021 e no Decreto Distrital nº 44.330/2023.

7.20.3. O DETRAN-DF não exercerá qualquer ingerência, controle ou deliberação sobre a equipe técnica da contratada, suas funções, perfis, quantitativos ou formações, uma vez que a presente contratação não tem por objeto a prestação de serviços, mas o fornecimento de solução tecnológica com resultados definidos e responsabilidade integral da contratada pela execução e pela qualidade do produto final.

7.20.4. Eventuais substituições, remanejamentos ou desligamentos de profissionais serão de responsabilidade exclusiva da contratada, que deverá adotar as providências internas necessárias à preservação da continuidade operacional, sem impacto no cronograma ou na qualidade das entregas contratadas.

7.20.5. A contratada deverá zelar pela capacitação e atualização técnica contínua de seus colaboradores, mantendo equipe devidamente qualificada durante toda a vigência contratual, sem que qualquer custo, ônus ou encargo relativo a treinamento, certificação ou qualificação profissional recaia sobre o DETRAN-DF.

7.20.6. A ausência de profissionais qualificados, ou a insuficiência técnica da equipe alocada, caracterizará inadimplemento contratual, sujeitando a contratada às sanções cabíveis previstas na Lei nº 14.133/2021, inclusive advertência, multa ou rescisão, conforme gravidade e reincidência.

7.20.7. Dessa forma, a gestão, supervisão e responsabilidade técnica sobre os especialistas empregados na execução do contrato são atribuições exclusivas da contratada, cabendo-lhe assegurar que todos os profissionais atuem de acordo com os padrões técnicos, éticos e legais exigidos, sem qualquer transferência de responsabilidade à Administração.

7.21. Requisitos de formação de equipe

7.21.1. A formação, composição e gestão da equipe técnica vinculada à execução do contrato constituem responsabilidade integral e exclusiva da futura CONTRATADA, competindo-lhe a seleção, contratação, alocação, capacitação, substituição e dimensionamento dos profissionais necessários à plena execução das atividades sob sua responsabilidade.

7.21.2. O DETRAN-DF não exercerá qualquer ingerência sobre a equipe da contratada, seus vínculos empregatícios, modelo de contratação, regime jurídico, formas de remuneração ou estrutura interna de gestão de pessoal, cabendo à empresa observar a legislação vigente e assegurar o cumprimento de todas as obrigações trabalhistas e previdenciárias, nos termos do art. 121, §§2º e 3º, da Lei nº 14.133/2021.

7.21.3. A vedação à interferência da Administração Pública estende-se à exigência de vínculo celetista, à imposição de paridade salarial e à determinação de quantitativos ou perfis específicos de pessoal, uma vez que o presente objeto não se caracteriza como prestação de serviços com dedicação exclusiva de mão de obra, mas como fornecimento de solução tecnológica autônoma, de natureza intelectual e orientada a resultados, conforme o entendimento consolidado pelo Acórdão nº 1189/2025 – TCU – Plenário.

7.21.4. A contratada deverá garantir que os profissionais sob sua gestão possuam qualificação compatível com as atividades desempenhadas, mantendo-os tecnicamente atualizados durante a vigência contratual. O DETRAN-DF limitar-se-á à verificação dos resultados contratados, sem qualquer interferência na gestão interna de recursos humanos da contratada.

7.22. Requisitos de Severidades

7.22.1. As classificações de severidade e os respectivos prazos de resposta e solução serão definidos conforme o cenário técnico adotado e a forma de acompanhamento da execução contratual, devendo refletir a complexidade, a origem e o impacto operacional de cada ocorrência sobre o ambiente de segurança da informação do DETRAN-DF.

7.22.2. A definição de severidades deverá considerar o tipo de chamado, a natureza do incidente, os riscos associados e o grau de comprometimento dos ativos institucionais, observando prazos distintos para registro, análise preliminar, tratamento definitivo e reclassificação de ocorrências, especialmente nos casos em que a indisponibilidade de informações ou acessos pela Administração possa afetar a adequada avaliação da demanda.

7.23. Participação de empresas reunidas sob a forma de consórcio, Cooperativa e Subcontratação

7.23.1. No contexto da presente contratação, voltada à implantação de solução integrada de segurança da informação e defesa cibernética, a análise técnica, jurídica e operacional conduzida pela equipe de planejamento identificou que o objeto demanda execução direta, unificada e de alta responsabilidade técnica, o que torna inadequada a participação de consórcios empresariais, cooperativas ou subcontratadas. Tal decisão se ampara no princípio da eficiência (art. 11, Lei nº 14.133/2021), no dever de proporcionalidade e na necessidade de preservar a unicidade de comando técnico e de governança durante toda a execução contratual.

7.23.2. A estrutura contratual do projeto compreende atividades contínuas e interdependentes — como monitoramento inteligente, detecção e resposta a incidentes, integração com Microsoft 365, análise comportamental de rede (NDR), inteligência de ameaças e operação de alertas 24x7 — que requerem domínio integral do contratado sobre todos os componentes da solução. A fragmentação dessas responsabilidades entre múltiplos entes comprometeria a rastreabilidade de eventos, a integridade das correlações, o desempenho da inteligência automatizada e a segurança dos dados sensíveis, contrariando as obrigações impostas pela Lei nº 13.709/2018 (LGPD) e pelos princípios de integridade e continuidade operacional da Administração.

7.23.3. A participação de consórcios empresariais foi considerada tecnicamente desnecessária e potencialmente prejudicial, visto que acarretaria aumento da complexidade contratual, dificultando a imputação de responsabilidades diretas e a responsabilização solidária em incidentes de segurança. Além disso, a heterogeneidade de políticas e padrões de compliance entre empresas consorciadas poderia introduzir vulnerabilidades técnicas e jurídicas, em desacordo com a exigência de arquitetura coesa, interoperável e auditável. Por essas razões, restou definida a vedação expressa à participação de consórcios no certame, de modo a preservar a coerência técnica, a previsibilidade operacional e a responsabilização unívoca da contratada.

7.23.4. A mesma lógica aplica-se às sociedades cooperativas, cuja estrutura descentralizada e de gestão compartilhada é incompatível com a natureza sensível e sigilosa da execução. A contratação de entidade com múltiplos associados responsáveis pela execução direta implicaria risco elevado à governança de segurança, à confidencialidade e à rastreabilidade de logs e incidentes. Além disso, a ausência de hierarquia operacional rígida e de controle centralizado inviabilizaria o cumprimento das normas de auditoria, segregação de funções e controle de acesso exigidas para ambientes críticos de ciberdefesa.

7.23.5. No tocante à subcontratação, a diretriz institucional adotada é igualmente restritiva. A natureza do objeto requer controle técnico unificado, padrões homogêneos de configuração, suporte e monitoramento, além de garantia de confidencialidade e de resiliência dos serviços contratados. Qualquer subcontratação parcial de módulos, integrações ou serviços correlatos introduziria terceiros não supervisionados diretamente pela Administração, comprometendo a integridade da solução e criando risco de exposição indevida de informações estratégicas, violando as premissas de segurança da informação e os princípios de governança previstos na Lei nº 14.133/2021.

7.23.6. Dessa forma, a vedação à subcontratação de quaisquer parcelas do objeto justifica-se como medida preventiva de segurança institucional, destinada a assegurar que todas as obrigações técnicas e operacionais sejam executadas diretamente pela contratada, sob regime de rastreabilidade, sigilo e controle integral. Tal postura resguarda o interesse público, a continuidade dos serviços críticos, a coerência dos resultados e a responsabilização plena da executora, garantindo que a plataforma de defesa cibernética opere de modo uniforme, previsível e compatível com os padrões de conformidade e integridade exigidos pelo DETRAN-DF.

7.24. Itens de Maior Relevância

7.24.1. Analisando os itens que compõem o objeto a ser contratado, anotamos como itens de maior representatividade:

7.24.1.1. Item 01: Justifica-se a relevância tendo em vista que possui a maior quantidade de dispositivos monitorados.

7.24.1.2. Item 07: Justifica-se a importância tendo em vista que é um serviço essencial, prestado no formato 24x7.

7.25. Exclusividade

7.25.1. Em observância aos art. 25, §2º, da Lei 4.611, de 9 de agosto de 2011, e 7º, do Decreto Distrital 35.592, de 2 de julho 2014, não serão destinados itens a participação Exclusiva das entidades preferenciais.

7.26. Parcelamento do objeto

7.26.1. Não será empregado parcelamento do objeto, conforme estudo e conclusão prevista no Estudo Técnico Preliminar.

8. DAS RESPONSABILIDADES

8.1. Das obrigações da contratante

8.1.1. Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos, de acordo com as obrigações assumidas no contrato e na sua proposta de preços;

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

8.1.3. Receber o objeto fornecido pelo contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

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

8.1.5. Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;

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

8.1.7. Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

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

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

8.1.10. Permitir o acesso dos empregados da CONTRATADA, devidamente identificados, para a execução de serviços, testes, reuniões administrativas ou qualquer outra atividade relacionada ao objeto contratado, desde que autorizado pela CONTRATANTE;

8.1.11. Permitir o acesso e prestar informações que venham a ser solicitadas pelos técnicos da CONTRATADA, durante a vigência do contrato;

8.1.12. Manter a CONTRATADA informada acerca da composição da Comissão de Execução contratual, cientificando-lhe para fins de propiciar que seus Prepostos possam reportar eventuais falhas ou problemas detectados, bem como possam apresentar-lhes os faturamentos correspondentes às prestações executadas;

8.1.13. Disponibilizar o local e os meios adequados para a execução dos serviços;

8.1.14. Emitir, nas condições estabelecidas no documento contratual, o Termo de Encerramento do Contrato;

8.1.15. Emitir relatórios sobre os atos relativos à execução do contrato que vier a ser firmado, em especial, quanto ao acompanhamento e fiscalização da execução dos serviços, à exigência de condições estabelecidas e proposta de aplicação de sanções;

8.1.16. Arquivar, entre outros documentos, projetos, "as built", especificações técnicas, orçamentos, termos de recebimento, contratos e aditamentos, relatórios de inspeções técnicas após o recebimento do serviço e notificações expedidas;

8.1.17. Designar servidor como Executor para o Contrato ao qual serão incumbidas as atribuições legais;

8.1.18. Notificar a CONTRATADA, por escrito, quanto a eventuais imperfeições, falhas ou irregularidades verificadas no curso da execução dos serviços objeto da contratação, bem como, quanto a qualquer ocorrência relativa ao comportamento de seus técnicos, quando em atendimento, que venha a ser considerado prejudicial ou inconveniente pelo CONTRATANTE, para que sejam adotadas as medidas corretivas necessárias, fixando prazo para a sua correção;

8.1.19. Esclarecimentos acerca da forma de validação e aceite das entregas que serão realizadas pela CONTRATADA;

8.1.20. Não permitir que pessoas estranhas à CONTRATADA examinem ou provoquem qualquer alteração nos serviços do presente objeto;

8.1.21. Observar e pôr em prática as recomendações técnicas feitas pela CONTRATADA relacionadas às condições de funcionamento, quando julgar pertinente ou oportuno;

8.1.22. Proporcionar as condições para que a CONTRATADA possa desempenhar seus serviços de acordo com as determinações do Contrato, do Edital e seus Anexos, especialmente do Termo de Referência;

8.1.23. Disponibilizar pessoal qualificado para a passagem do conhecimento o qual é objeto da contratação;

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

8.2. Das obrigações da contratada

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

8.2.2. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

8.2.3. 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;

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

8.2.5. Manter a produtividade ou a capacidade mínima de fornecimento do objeto durante a execução do Contrato, conforme especificação;

8.2.6. Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC, nos termos definidos neste artefato;

8.2.7. Fazer a transição contratual, quando for o caso, observado o disposto no art. 35 da IN 94/2022.;

8.2.8. Comunicar imediatamente ao Contratante qualquer alteração ocorrida no endereço, conta bancária, e-mail e telefone, indicado na respectiva proposta de preços, como também, outras informações julgadas necessárias para o recebimento de correspondências encaminhadas pelos diversos órgãos integrantes da centralização de compras do Distrito Federal;

8.2.9. Cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto;

8.2.10. Planejar, mapear, desenvolver, executar e prestar os serviços conforme especificações do Termo de Referência e de sua proposta e dentro das exigências de níveis de serviços nele estabelecidos, com a alocação dos empregados necessários e com formação e conhecimento técnico condizentes para o perfeito cumprimento das cláusulas contratuais;

8.2.11. Manter e proteger, independentemente do término do serviço objeto desse documento, a condição de confidencialidade de qualquer informação considerada dessa natureza pelo DETRAN/DF;

8.2.12. Informar seus representantes acerca do sigilo a ser mantido, orientando-os a assinar o Termo de Confidencialidade Corporativo constante nos Anexos, devendo tomar todas as providências necessárias para que a referida natureza confidencial seja preservada e não seja permitida a utilização das informações disponibilizadas para fins outros que não aqueles relacionados à prestação do serviço. Em caso de inobservância deste dispositivo, poderão ser aplicadas as sanções administrativas dispostas no Art. 156, da Lei 14.133/21, além de imposição da multa prevista em Edital;

8.2.13. Cumprir e garantir que seus profissionais estejam cientes, aderentes e obedeçam rigorosamente às normas e aos procedimentos estabelecidos na Política de Segurança da Informação da CONTRATANTE;

8.2.14. Obedecer aos prazos contratuais estabelecidos;

8.2.15. Cumprir integralmente os níveis de serviço exigidos;

8.2.16. Responsabilizar-se pela conservação dos ambientes da CONTRATANTE em que desempenhe seus serviços;

8.2.17. Elaborar e apresentar à CONTRATANTE, quando solicitado, o Relatório Gerencial dos Serviços Executados, contemplando serviços executados. Outros relatórios ou evidências relacionadas ao Contrato poderão ser solicitados pela CONTRATANTE;

8.2.18. Manter seus funcionários ou representantes credenciados devidamente identificados quando da execução de qualquer serviço nas dependências do CONTRATANTE, referente ao objeto contratado, observando as normas de segurança (interna e de conduta);

8.2.19. Comunicar a CONTRATANTE, por escrito, no prazo máximo de 5 (cinco) dias úteis que antecedem o prazo de vencimento das entregas, quaisquer anormalidades que ponham em risco o êxito e o cumprimento dos prazos da execução dos serviços, propondo as ações corretivas necessárias para a execução dos mesmos;

8.2.20. Submeter à aprovação da CONTRATANTE qualquer alteração que se tornar essencial à continuação da execução ou prestação dos serviços;

8.2.21. Arcar com os eventuais prejuízos causados ao DETRAN/DF e/ou a terceiros, provocados por ineficiência ou irregularidade cometida por seus empregados ou colaboradores envolvidos na execução dos serviços, respondendo integralmente pelo ônus decorrente de sua culpa ou dolo na entrega dos itens/serviços, o que não exclui nem diminui a responsabilidade pelos danos que se constatarem, independentemente do controle e fiscalização exercidos pelo DETRAN/DF;

8.2.22. Responsabilizar-se, sempre, pelos danos causados por sua culpa ou dolo, pelos seus prepostos ou funcionários e, eventualmente, pelos prejuízos resultantes de caso fortuito e força maior, nos termos do artigo 393 do Código Civil Brasileiro. A fiscalização ou o acompanhamento da execução do contrato não exclui nem reduz essa responsabilidade;

8.2.23. Ter pleno conhecimento de todas as condições e peculiaridades inerentes aos serviços a serem executados, não podendo invocar posteriormente desconhecimento para cobrança de serviços extras;

8.2.24. Dar ciência, imediatamente e por escrito, de qualquer anormalidade que verificar na execução dos serviços, bem como prestar esclarecimentos que forem solicitados pelo DETRAN/DF;

8.2.25. Utilizar profissionais devidamente capacitados e habilitados para os serviços contratados, impondo-lhes rigoroso padrão de qualidade, segurança e eficiência, correndo por sua conta todas as despesas com salários, impostos, contribuições previdenciárias, encargos trabalhistas, seguros e outras correlatas;

8.2.26. Assumir total responsabilidade pelos atos administrativos e encargos previstos na legislação trabalhista, tais como: controle de frequência, ausências permitidas, licenças autorizadas, promoções, férias, punições, admissões, demissões, transferências, como também pelo cumprimento de todas as obrigações trabalhistas, fiscais, previdenciárias e comerciais, inclusive a responsabilidade decorrente de acidentes, indenizações e seguros e outros correlatos;

8.2.27. Não transferir a terceiros, no todo ou em parte, por qualquer forma, as obrigações assumidas oriundas do contrato, nem subcontratar, salvo se prévia e expressamente autorizadas pela instituição competente;

8.2.28. Comprovar que possui profissionais com habilitação para executar os serviços técnicos especializados, apresentando certificado técnico/treinamento emitido pelo fabricante ou distribuidor da solução;

8.2.29. Aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, no montante de até 25% (vinte e cinco por cento), do valor inicialmente contratado, nos termos do Art. 125, da Lei 14.133/21;

8.2.30. Não permitir a utilização de qualquer trabalho do menor de dezesseis 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;

8.2.31. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento ao objeto da licitação;

8.2.32. Respeitar os termos estipulados no Decreto nº 38.365, publicado no Diário Oficial do Distrito Federal nº 143, de 27 de julho de 2017, que regulamenta a Lei Distrital nº 5.448/2015, o qual proíbe conteúdo discriminatório contra a mulher;

8.2.33. Entregar ao CONTRATANTE toda e qualquer documentação fornecida e produzida durante vigência da prestação de serviços, em conformidade com as exigências contidas no Termo de Referência, tais como: estudos, relatórios, especificações, descrições técnicas, protótipos, dados, artefatos, códigos- fonte, banco de dados, scripts, plantas, desenhos, diagramas, base de conhecimentos, manuais, guias, dentre outros, em papel ou mídia digital;

8.2.34. Fornecer à CONTRATANTE relação nominal dos técnicos que atuarão no cumprimento do objeto contratado, atualizando-a sempre que necessário;

8.2.35. Utilizar padrões de atendimento definidos em conjunto com a CONTRATANTE (nomenclaturas, metodologias, entre outros);

8.2.36. Responsabilizar-se integralmente pela sua equipe técnica, primando pela qualidade, desempenho, eficiência e produtividade, visando à execução dos trabalhos durante toda a vigência do Contrato, dentro dos prazos e condições estipulados;

8.2.37. Não permitir a utilização de qualquer trabalho de menor de dezesseis 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;

8.2.38. A CONTRATADA fica obrigada a respeitar os termos estipulados no Decreto nº 38.365, publicado no Diário Oficial do Distrito Federal nº 143, de 27 de julho de 2017, que regulamenta a Lei nº5.448, de 12 de janeiro de 2015, os quais proíbem conteúdo discriminatório contra a mulher e na Lei n° 6.679, de 24 de setembro de 2020, que dispõe sobre a exigência de garantir a de equidade salarial entre homens e mulheres nas empresas que contratam com o Poder Público do Distrito Federal.

9. MODELO DE EXECUÇÃO DO CONTRATO

9.1. Condições de Execução

9.1.1. O início da execução do contrato dar-se-á com a realização da Reunião Inicial, convocada pelo Gestor do Contrato, cuja pauta observará:

9.1.1.1. Esclarecimento de questões de gerenciamento do contrato, operacionais e administrativas;

9.1.1.2. Presença do representante legal da empresa CONTRATADA, que indicará formalmente o Preposto Contratual;

9.1.1.3. Entrega da comprovação da formação e qualificação técnica do Preposto Contratual;

9.1.1.4. O prazo para entrega das demais comprovações da formação e qualificações técnicas serão definidas pelo Gestor do Contrato;

9.1.1.5. Entrega do Termo de Confidencialidade da Informação, contendo declaração de manutenção do sigilo das informações e respeito às normas de segurança vigentes da CONTRATANTE, assinado pelo representante legal da empresa CONTRATADA.

9.1.1.6. Entrega do Termo de Ciência das obrigações quanto à confidencialidade das informações e quanto às normas de segurança vigentes da CONTRATANTE, a ser assinado por todos os empregados da empresa CONTRATADA diretamente envolvida na contratação.

9.2. Reunião Inicial

9.2.1. Conforme definido junto aos requisitos.

9.3. Período de Ambientação Inicial

9.3.1. Conforme definido junto aos requisitos.

9.4. Cronograma de execução

9.4.1. O Cronograma está assim definido:

EVENTO	PRAZOS APLICÁVEIS
Assinatura do Contrato	Deverá ocorrer no prazo de até 5 (cinco) dias úteis contados do recebimento da convocação formal.
Reunião Inicial de Alinhamento	Deverá ocorrer no prazo de até 10 (dez) dias úteis a contar da assinatura do contrato.
Disponibilização da Solução	Deverá ocorrer no prazo previsto no cronograma contratual, contados da assinatura do contrato.
Implantação / Customização / Integrações	Conforme Plano de Implantação a ser apresentado pela contratada e aprovado pelo DETRAN-DF.
Ordens de Serviço (acompanhamentos formais)	O prazo de resposta e execução será definido na própria OS, conforme sua gravidade e criticidade.
Recebimento Provisório	Após entrega formal da solução e validação funcional inicial, conforme critérios definidos no edital.
Recebimento Definitivo	Após decurso do prazo de observação e homologação técnica da solução, nos termos do art. 140 da Lei nº 14.133/2021.
Prazo de Pagamento	Efetuado conforme cláusula contratual específica, observando o disposto no art. 143 da Lei nº 14.133/2021.
Atendimento de Chamados / Suporte	Conforme matriz de severidade e níveis de serviço definidos no contrato ou plano de suporte técnico.
Janelas de Manutenção	Devem ser previamente acordadas com o DETRAN-DF e ocorrer preferencialmente fora do horário comercial.

9.4.2. As entregas serão comprovadas por documento (ou atesto na nota fiscal) e com a verificação/confirmação que as licenças previstas estão disponíveis no portal do fabricante.

9.4.3. Todos os componentes de software requeridos para atender as funcionalidades exigidas na especificação técnica e, consequentemente, tornar a solução operante, mesmo que não tenham sido especificados e cotados na proposta apresentada pela eventual CONTRATADA, serão considerados essenciais aos serviços de instalação e deverão ser fornecidos sem custo adicional em relação à sua proposta técnico-comercial.

9.5. Local e horário de Prestação dos Serviços

9.5.1. O local encontra-se especificado junto ao anexo que trata das especificações técnicas da solução.

9.5.2. O horário de prestação dos serviços é de 08 às 18hs, em dias úteis.

9.6. Ordens de Serviço

9.6.1. A disponibilização da solução requer emissão de Ordem de Serviço ou Fornecimento, tendo seu prazo definido a partir da assinatura do contrato.

9.6.2. As Ordens de Serviços serão emitidas pela CONTRATANTE e serão partes integrantes da execução do contrato, que poderá ter tantas Ordens de serviços quanto forem necessárias. Essas Ordens de Serviço serão emitidas e deverão conter, minimamente: um número identificador; a data de emissão; a classificação do tipo de serviço; a definição e especificação dos serviços a serem realizados; o volume estimado do serviço a ser realizado, o perfil dos profissionais que atuarão na ordem de serviço, conforme a métrica definida para o serviço; o cronograma de realização dos serviços, incluídas todas as tarefas significativas e seus respectivos prazos previstos; e a autorização do Gestor do Contrato bem como dos representantes da Área Requisitante e da empresa CONTRATADA.

9.6.3. Caso haja necessidade de realização de reuniões com a CONTRATANTE para refinamento do escopo contido na demanda, com objetivo de aprimorar as estimativas do projeto, o tempo despendido com a realização dessas reuniões, poderá ser solicitado aos Fiscais do Contrato, com as devidas justificativas (evidências), a alteração das datas de entregas, tendo em vista que essas reuniões dependerão de disponibilidade por parte das áreas negociais do DETRAN/DF e poderão impactar nas entregas dependendo das suas definições.

9.6.4. Caso haja interrupção dos serviços, por interesse do CONTRATANTE, após a autorização para execução da O.S, haverá um pagamento proporcional ao esforço da empresa CONTRATADA. Neste caso a CONTRATADA terá um prazo a ser acordado com a CONTRATANTE, a partir da data do registro do cancelamento da demanda, para entrega dos produtos finalizados até então e que serão considerados para o pagamento proporcional, visando o menor impacto possível. Não serão aceitos produtos entregues após o prazo supracitado e o CONTRATANTE poderá optar por não colocar o produto incompleto em produção deixando sua decisão documentada e evidenciada.

9.6.5. Durante a execução da O.S., a empresa CONTRATADA deverá informar imediatamente à CONTRATANTE caso o escopo definido no planejamento tenha sido modificado durante a execução da O.S. Neste caso, a continuidade da O.S. dependerá de uma nova autorização formal emitida pela CONTRATANTE, que deverá conter as novas estimativas de volume e prazo dos serviços e o devido ajuste no cronograma. As exceções serão avaliadas pontualmente pelo gestor contratual.

9.6.6. Os indicadores levarão em consideração as informações de volume e prazo, após a entrega final da O.S.

9.6.7. Caberá à empresa CONTRATADA monitorar adequadamente a execução da O.S para garantir que o volume e o prazo dos serviços executados não superem os limites previamente autorizados, uma vez que não haverá pagamento de serviços executados além do escopo autorizado nem flexibilização dos níveis de serviço acordados.

9.6.8. A existência da divergência quanto ao dimensionamento dos serviços não autoriza a empresa CONTRATADA a onerar os prazos ou a qualidade dos serviços prestados, sendo necessário, neste caso, o replanejamento da demanda junto a gestão contratual.

9.6.9. A CONTRATANTE irá monitorar a execução da ordem de serviço, com base na metodologia e nos indicadores estabelecidos neste documento. Durante a execução das O.S., como resultado desse monitoramento, poderão ser necessárias correções de produtos bem como a adequação de serviços em andamento, visando o atendimento aos critérios de qualidade previamente estabelecidos.

9.6.10. Ao final da Ordem de Serviço, deverão ser observadas as condições de aceite e pagamento estabelecidas neste documento. O faturamento somente será feito para as Ordens de Serviço encerradas no período cujos produtos tenham sido entregues, aferidos e atestados e após a aplicação dos descontos e/ou sanções previstas nos Níveis Mínimos de Serviço.

9.7. Materiais a serem disponibilizados

9.7.1. Não se aplica.

9.8. Especificação da garantia do serviço (art. 40, §1º, inciso III, da Lei nº 14.133, de 2021)

9.8.1. O prazo de garantia contratual dos serviços é aquele estabelecido na Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor).

9.9. Formas de transferência de conhecimento

9.9.1. Não se aplica.

9.10. Plano de definição de requisitos e padronização

9.10.1. As contratações públicas realizadas no âmbito do Distrito Federal devem observar o disposto no Decreto Distrital nº 44.330, de 16 de março de 2023, que regulamenta a aplicação da Lei Federal nº 14.133/2021 no território distrital. Nos termos do art. 81 do referido Decreto, a Administração deve, sempre que possível, adotar o princípio da padronização, assegurando a compatibilidade das especificações técnicas, funcionais e de desempenho dos bens e serviços, bem como a coerência quanto às condições de manutenção, suporte e garantias ofertadas.

9.10.2. No que tange ao segmento de segurança da informação e defesa cibernética, verifica-se que, até o presente momento, não há norma distrital de padronização vigente que discipline requisitos técnicos uniformes para este tipo de solução. Assim, inexiste impedimento jurídico para a definição das especificações com base em critérios técnicos usuais de mercado, desde que observadas as diretrizes de interoperabilidade, conformidade normativa e alinhamento às políticas de segurança da informação da Administração Pública.

9.10.3. O objeto em estudo constitui-se de serviços tecnológicos especializados de monitoramento e resposta a incidentes cibernéticos, enquadrando-se, portanto, como bem e serviço comum de tecnologia, conforme as definições da Instrução Normativa SEGES/ME nº 94/2022, cuja descrição técnica pode ser padronizada por meio de requisitos de desempenho, capacidade e confiabilidade, sem vinculação a fabricantes, modelos ou marcas específicas.

9.10.4. Ainda que inexista padronização formal instituída pelo Governo do Distrito Federal para esta categoria tecnológica, a presente contratação observará, como diretriz técnica e estratégica, a necessidade de uniformidade operacional e coerência arquitetural entre os componentes da solução. Essa medida visa assegurar compatibilidade funcional, facilidade de integração, homogeneidade na experiência de uso e racionalização de custos de operação, capacitação e manutenção, alinhando-se ao princípio da eficiência administrativa e aos objetivos institucionais do DETRAN-DF, especialmente no tocante à proteção de dados, continuidade dos serviços e resguardo da infraestrutura tecnológica crítica da Autarquia.

9.11. Procedimentos de transição e finalização do contrato

9.11.1. Os procedimentos de transição e finalização do contrato constituem-se das seguintes etapas:

9.11.1.1. A CONTRATADA deverá manter a Base de Conhecimento atualizada para repasse de conhecimento durante a transição contratual.

9.11.1.2. Na ocasião do encerramento contratual, seja por decurso de seu prazo de vigência ou por rescisão, se demandado pelo CONTRATANTE, a CONTRATADA deverá providenciar um Plano de Transição e executar a Transição Contratual com transferência de tecnologia e técnicas empregadas, sem perda de informações, capacitando os profissionais indicados pelo CONTRATANTE, sem ônus ao Órgão, em até um mês antes do encerramento.

9.11.1.3. Durante o período necessário à elaboração e execução do Plano de Transição Contratual, a CONTRATADA se responsabilizará pela capacitação dos receptores mencionados acima quanto às atividades, tarefas, pesquisas e procedimentos relativos à transferência de conhecimento entre a CONTRATADA e o CONTRATANTE, assim como pela confecção de documentação ou qualquer outro esforço vinculado à transição, com apoio do CONTRATANTE, contudo sem ônus à este.

9.11.1.4. A ocorrência de evento no qual a CONTRATADA, ou qualquer de seus representantes, não cooperarem ou reterem quaisquer informações ou dados requeridos pelo CONTRATANTE que venha a prejudicar, de alguma maneira, a execução e consequente conclusão do procedimento de transição contratual, constituirá em Inexecução Parcial do Objeto, sujeitando a CONTRATADA ao cumprimento de obrigações relativas ao reparo de todos os danos que possam vir a ser causados ao CONTRATANTE, além das sanções previstas neste Termo de Referência.

9.11.1.5. Fica a cargo do CONTRATANTE a indicação dos recursos profissionais humanos qualificados (cujos perfis estejam identificados no Plano de Transição) como os receptores da transferência de conhecimento.

9.11.1.6. Será de total responsabilidade da CONTRATADA, com apoio do CONTRATANTE, a execução integral do Plano de Transição Contratual, bem como a garantia do repasse bem sucedido de todas as informações necessárias para a continuidade dos serviços pelo Órgão.

9.11.1.7. O CONTRATANTE poderá solicitar ajustes, alterações ou adequações no Plano de Transição Contratual caso forem detectados itens que exacerbadamente onerem o Órgão ou que comprometam a execução e/ou conclusão da transição.

9.11.1.8. O Plano de Transição será considerado um adendo contratual, no qual deverão estar registrados todos os compromissos, papéis, responsabilidades, artefatos e tarefas concernentes ao procedimento transitório, bem como a identificação de todos os envolvidos no processo e os prazos necessários para execução das atividades de transição.

9.11.1.9. Todo conhecimento adquirido ou desenvolvido, bem como toda informação produzida e/ou utilizada para a execução dos serviços contratados deverão ser disponibilizados ao CONTRATANTE, ou aos profissionais designados pelo DETRAN/DF, em até 30 (trinta) dias após o encerramento do contrato.

9.12. Mecanismos formais de comunicação

9.12.1. São definidos como mecanismos formais de comunicação, entre o CONTRATANTE e a CONTRATADO, os seguintes:

9.12.1.1. Ordem de Serviço;

9.12.1.2. Ata de Reunião;

9.12.1.3. Ofício;

9.12.1.4. Sistema de abertura de chamados;

9.12.1.5. E-mails e Cartas;

9.13. Formas de Pagamento

9.13.1. Os critérios de medição e pagamento dos serviços prestados serão tratados em tópico próprio quanto a pagamentos.

10. MODELO DE GESTÃO DO CONTRATO

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

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

10.3. 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.

10.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

10.5. Preposto

10.5.1. A CONTRATADA designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado.

10.5.2. A CONTRATADA deverá manter preposto da empresa no local da execução do objeto durante o horário comercial.

10.5.3. O CONTRATANTE poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em que a CONTRATADA designará outro para o exercício da atividade.

10.6. Fiscalização

10.6.1. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput), nos termos do art. 33 da IN SGD nº 94, de 2022, recepcionado pelo Decreto Distrital N.º 45.011, 27 de setembro de 2023 observando-se, em especial, as rotinas a seguir.

10.6.2. A fiscalização não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, emprego de material inadequado ou de qualidade inferior, e, na ocorrência desta, não implica em corresponsabilidade da Administração ou de seus agentes e prepostos, em conformidade com o art. 120 da Lei Federal n.º 14.133, de 2021.

10.7. Fiscalização Técnica

10.7.1. O fiscal técnico do contrato, além de exercer as atribuições previstas no art. 33, II, da IN SGD nº 94, de 2022, recepcionado pelo Decreto Distrital N.º 45.011, 27 de setembro de 2023, acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração, conforme o inciso VI do art. 24 do Decreto Distrital n.º 44.330, de 2023.

10.7.2. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados, de acordo com §1º, do art. 117, Lei Federal n.º 14.133, de 2021, e inciso II do art. 24 do Decreto Distrital n.º 44.330, de 2023.

10.7.3. Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção, conforme o inciso III do art. 24 do Decreto Distrital n.º 44.330, de 2023.

10.7.4. O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso, conforme o inciso IV do art. 24 do Decreto Distrital n.º 44.330, de 2023.

10.7.5. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato, conforme o inciso V do art. 24 do Decreto Distrital n.º 44.330, de 2023.

10.7.6. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual, conforme o inciso VII do art. 24 do Decreto Distrital n.º 44.330, de 2023.

10.8. Fiscalização Administrativa

10.8.1. O fiscal administrativo do contrato, além de exercer as atribuições previstas no art. 33, IV, da IN SGD nº 94, de 2022, recepcionado pelo Decreto Distrital N.º 45.011, 27 de setembro de 2023, verificará a manutenção das condições de habilitação do Contratado, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário, conforme o inciso II do art. 25 do Decreto Distrital n.º 44.330, de 2023.

10.8.2. Caso ocorram descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência, conforme o inciso IV do art. 25 do Decreto Distrital n.º 44.330, de 2023.

10.9. Gestor do Contrato

10.9.1. O gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022, recepcionado pelo Decreto Distrital N.º 45.011, 27 de setembro de 2023, coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração. (Decreto nº 11.246, de 2022, art. 21, IV).

10.9.2. O gestor do contrato acompanhará a manutenção das condições de habilitação do Contratado, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais, conforme o inciso IV do art. 23 do Decreto Distrital n.º 44.330, de 2023.

10.9.3. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência, conforme o inciso II do art. 23 e e art. 142 a 150 do Decreto Distrital n.º 44.330, de 2023.

10.9.4. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo Contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme o inciso VIII do art. 23 do Decreto Distrital n.º 44.330, de 2023.

10.9.5. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso, de acordo com o inciso X do art. 23 do Decreto Distrital n.º 44.330, de 2023.

10.9.6. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou prorrogação contratual, conforme o inciso VII do art. 23 do Decreto Distrital n.º 44.330, de 2023.

10.9.7. O gestor do contrato deverá elaborará relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração, conforme o inciso VI do art. 23 do Decreto Distrital n.º 44.330, de 2023.

11. DO REAJUSTE

11.1. Os preços são fixos e irreajustáveis no prazo de um ano contado da data limite para a apresentação das propostas.

11.2. Dentro do prazo de vigência do contrato e mediante solicitação da contratada, os preços contratados poderão sofrer reajuste após o interregno de um ano, aplicando-se o **Índice de Custo da Tecnologia da Informação - ICTI**, apurado e mantido pelo Instituto de Pesquisa Econômica Aplicada - IPEA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

11.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir da data de início dos efeitos financeiros do último reajuste.

11.4. No caso de atraso ou não divulgação do índice de reajustamento, o CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo. Fica a CONTRATADA obrigada a apresentar memó ria de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.

11.5. Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.

11.6. Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.

11.7. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficia l, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

11.8. O reajuste será realizado por apostilamento.

12. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

12.1. A avaliação da execução do objeto utilizará os requisitos e indicadores definidos neste termo.

12.2. Do recebimento

12.2.1. Os itens serão recebidos provisoriamente, no prazo de 05 (cinco) dias, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo. (Art. 140, I, a , da Lei nº 14.133 e Arts. 22, X e 23, X do Decreto nº 11.246, de 2022).

12.2.2. O prazo da disposição acima será contado do recebimento de comunicação de cobrança oriunda do contratado com a comprovação da prestação dos serviços ou do fornecimento a que se referem a parcela a ser paga.

12.2.3. O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico. (Art. 22, X, Decreto nº 11.246, de 2022).

12.2.4. O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo. (Art. 23, X, Decreto nº 11.246, de 2022).

12.2.5. O fiscal setorial do contrato, quando houver, realizará o recebimento provisório sob o ponto de vista técnico e administrativo.

12.2.6. Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal técnico do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade do fornecimento ou da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à CONTRATADA, registrando em relatório a ser encaminhado ao gestor do contrato.

12.2.7. Será considerado como ocorrido o recebimento provisório com a entrega do termo detalhado ou, em havendo mais de um a ser feito, com a entrega do último.

12.2.8. A CONTRATADA fica obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição do objeto até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

12.2.9. A fiscalização não efetuará o ateste da última e/ou única medição do objeto até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório. (Art. 119 c/c art. 140 da Lei nº 14133, de 2021).

12.2.10. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

12.2.11. O objeto poderá ser rejeitado, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

12.2.12. Quando a fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá- los ao gestor do contrato para recebimento definitivo.

12.2.13. O objeto será recebido definitivamente no prazo de 10 (dez) dias, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:

12.2.13.1. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento (art. 21, VIII, Decreto nº 11.246, de 2022).

12.2.13.2. Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à CONTRATADA, por escrito, as respectivas correções.

12.2.13.3. Emitir Termo Detalhado para efeito de recebimento definitivo dos itens fornecidos ou prestados, com base nos relatórios e documentações apresentadas.

12.2.13.4. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

12.2.14. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.

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

12.2.16. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

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

12.3. Liquidação

12.3.1. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §2º da Instrução Normativa SEGES/ME nº 77/2022.

12.3.2. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021.

12.3.3. 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:

12.3 Liquidação

12.3.3.1. o prazo de validade;

12.3.3.2. a data da emissão;

12.3.3.3. os dados do contrato e do órgão contratante;

12.3.3.4. o período respectivo de execução do contrato;

12.3.3.5. o valor a pagar; e

12.3.3.6. eventual destaque do valor de retenções tributárias cabíveis.

12.3.4. 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 o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao CONTRATANTE;

12.3.5. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021.

12.3.6. A Administração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, que implique proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas. (INSTRUÇÃO NORMATIVA Nº 3, DE 26 DE ABRIL DE 2018);

12.3.7. 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 do CONTRATANTE;

12.3.8. Não havendo regularização ou sendo a defesa considerada improcedente, o 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;

12.3.9. Persistindo a irregularidade, o CONTRATANTE deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa;

12.3.10. 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.

12.4. Prazo de Pagamento

12.4.1. O pagamento será efetuado em até 30 (trinta) dias, contados a partir da data de apresentação da Nota Fiscal, desde que o documento de cobrança esteja em condições de liquidação de pagamento.

12.4.2. Passados 30 (trinta) dias sem o devido pagamento por parte da Administração, a parcela devida será atualizada monetariamente, desde o vencimento da obrigação até a data do efetivo pagamento de acordo com a variação pro rata tempore do Índice de Custos de Tecnologia da Informação – ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada – IPEA, nos termos do art. 24 da IN 01/2019 - SGD.

12.5. Forma de pagamento

12.5.1. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

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

12.5.3. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

12.5.4. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

12.5.5. O contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

12.6. Cessão de crédito

12.6.1. É admitida a cessão fiduciária de direitos creditícios com instituição financeira, nos termos e de acordo com os procedimentos previstos na Instrução Normativa SEGES/ME nº 53, de 8 de Julho de 2020, conforme as regras deste presente tópico.

12.6.2. As cessões de crédito não fiduciárias dependerão de prévia aprovação do CONTRATANTE.

12.6.3. A eficácia da cessão de crédito, de qualquer natureza, em relação à Administração, está condicionada à celebração de termo aditivo ao contrato administrativo.

12.6.4. Sem prejuízo do regular atendimento da obrigação contratual de cumprimento de todas as condições de habilitação por parte do contratado (cedente), a celebração do aditamento de cessão de crédito e a realização dos pagamentos respectivos também se condicionam à regularidade fiscal e trabalhista do cessionário, bem como à certificação de que o cessionário não se encontra impedido de licitar e contratar com o Poder Público, conforme a legislação em vigor, ou de receber benefícios ou incentivos fiscais ou creditícios, direta ou indiretamente, conforme o art. 12 da Lei nº 8.429, de 1992, nos termos do Parecer JL-01, de 18 de maio de 2020.

12.6.5. O crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (contratado) pela execução do objeto contratual, restando absolutamente incólumes todas as defesas e exceções ao pagamento e todas as demais cláusulas exorbitantes ao direito comum aplicáveis no regime jurídico de direito público incidente sobre os contratos administrativos, incluindo a possibilidade de pagamento em conta vinculada ou de pagamento pela efetiva comprovação do fato gerador, quando for o caso, e o desconto de multas, glosas e prejuízos causados à Administração (INSTRUÇÃO NORMATIVA Nº 53, DE 8 DE JULHO DE 2020).

12.6.6. A cessão de crédito não afetará a execução do objeto contratado, que continuará sob a integral responsabilidade do CONTRATADO.

12.7. Detalhamento dos Níveis de serviços

12.7.1. Níveis de serviços são critérios objetivos e mensuráveis estabelecidos, com a finalidade de aferir e avaliar diversos fatores relacionados com os serviços contratados.

12.7.2. Para mensurar esses fatores serão utilizados indicadores de desempenho relacionados com a natureza e característica dos serviços contratados, para os quais foram estabelecidas metas quantificáveis a serem cumpridas pela CONTRATADA.

12.7.3. A frequência de aferição e avaliação dos níveis de serviços será mensal, devendo a CONTRATADA elaborar relatório gerencial, onde constem os indicadores/metas de níveis de serviços alcançados, recomendações técnicas, administrativas e gerenciais para o próximo período e demais informações relevantes para a gestão contratual.

12.7.4. O início da medição dos indicadores ocorrerá a partir da data de início da efetiva execução dos itens, ou seja, do recebimento definitivo.

12.7.5. Os primeiros 90 (noventa) dias após o início da execução dos serviços serão considerados como período de estabilização e ajustes dos serviços prestados ou itens fornecidos (Ambientação Inicial), desde que a CONTRATADA não recuse o recebimento de nenhuma Ordem de Serviço.

12.7.6. Neste período, os resultados esperados e os níveis de qualidade exigidos sofrerão a flexibilização prevista nos requisitos de Ambientação Inicial.

12.7.7. Os descontos realizados, decorrentes da aplicação dos indicadores, não poderão ultrapassar 20% dos valores devidos, em cada processo de apuração.

12.7.8. Abaixo, detalhamos os indicadores que serão considerados no âmbito deste objeto:

Indicador: Indicador de Recebimento da Demanda (IRD)	
Finalidade	Medir a eficiência da CONTRATADA no recebimento formal e tempestivo das Ordens de Serviço (OS) ou demandas emitidas pela CONTRATANTE, com o devido registro de ciência e aceite nos canais oficiais definidos contratualmente.
Meta a Cumprir	100% das demandas emitidas pela Administração devem ser formalmente recebidas e registradas pela CONTRATADA no prazo máximo de 4 (quatro) horas úteis após o envio oficial.
Forma de Acompanhamento	Verificação em sistema de gestão de OSs, registro de protocolo eletrônico, e-mails ou dashboards integrados com log de recebimento.
Mecanismo de Cálculo	IRD = (Nº de demandas recebidas e registradas dentro do prazo / Nº total de demandas emitidas no período) × 100
Início da Vigência	A partir da emissão da primeira Ordem de Serviço no âmbito do contrato.
Periodicidade	Mensal, com apuração consolidada ao final de cada ciclo de faturamento.
Sanções/ faixas de ajuste	≥ 95%: Sem ajuste; Entre 90% e 94,99%: Glosa de 2% sobre o item vinculado; Entre 85% e 89,99%: Glosa de 5%; < 85%: Glosa de 10% e abertura de notificação formal para readequação dos processos internos da CONTRATADA.

Observações	O descumprimento sistemático deste indicador poderá comprometer o fluxo de execução contratual e ensejar aplicação de medidas adicionais conforme cláusula de sanções administrativas. A ausência de registro não será passível de justificativa sem prova documental de indisponibilidade dos sistemas utilizados.

Indicador: Indicador de Prazo de Atendimento (IPA)	
Finalidade	Assegurar o cumprimento dos prazos de execução e resolução dos serviços demandados, com o objetivo de manter a regularidade operacional e a eficiência contratual.
Meta a Cumprir	Cumprimento de, no mínimo, 95% das demandas dentro dos prazos pactuados em OS ou definidos conforme categoria de severidade.
Forma de Acompanhamento	Será realizada por meio de verificação cruzada entre os registros do sistema de gestão de chamados, Ordens de Serviço e relatórios técnicos validados pela fiscalização, que evidenciem a data de abertura da demanda e sua efetiva finalização.
Mecanismo de Cálculo	Índice de Prazo Cumprido = (Número de demandas finalizadas dentro do prazo / Número total de demandas no período) × 100
Início da Vigência	A partir da emissão da primeira Ordem de Serviço ou chamado técnico formalizado após o início da execução contratual.
Periodicidade	Mensal, com apuração acumulada por período de faturamento.
Sanções/ faixas de ajuste	≥ 95%: Sem ajuste (100% do valor devido). ≥ 90% e < 95%: Redução de 5% do valor mensal proporcional ao item. ≥ 80% e < 90%: Redução de 10% do valor mensal proporcional ao item. < 80%: Redução de 20% do valor mensal proporcional ao item + justificativa formal obrigatória. Persistência por mais de 2 meses consecutivos abaixo de 80% poderá ensejar apuração para eventual aplicação de penalidades administrativas.
Observações	O indicador considera apenas as demandas cuja execução esteja sob responsabilidade direta da contratada, não sendo computadas as pendências decorrentes de fatores atribuíveis ao contratante, como indisponibilidade de ambientes ou atrasos na aprovação de entregas. Demandas prorrogadas formalmente não serão consideradas em atraso.

13. SANÇÕES APLICÁVEIS NA EXECUÇÃO DO CONTRATO

13.1. As sanções aplicáveis são:

13.1.1. Advertências;

13.1.2. Multa;

13.1.3. Suspensão temporária de participação em licitação, e impedimento de contratar com a Administração do Distrito Federal, por prazo não superior a 2 (dois) anos, e dosada segundo a natureza e a gravidade da falta cometida;

13.1.4. Para a licitante e/ou CONTRATADA que, convocada dentro do prazo de validade de sua proposta, não celebrar o contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução do seu objeto, comportar-se de modo inidôneo ou cometer fraude fiscal; a penalidade será aplicada por prazo não superior a 5 (cinco) anos, e a licitante e/ou contratada será descredenciada do Sistema de Cadastro de Fornecedores, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais, aplicadas e dosadas segundo a natureza e a gravidade da falta cometida;

13.1.5. Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a CONTRATADA ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior.

13.2. As sanções previstas nos incisos I, III e IV do subitem anterior poderão ser aplicadas juntamente com a do inciso II, facultada a defesa prévia do interessado, no respectivo processo, no prazo de 5 (cinco) dias úteis.

13.3. Da advertência

13.3.1. A advertência é o aviso por escrito, emitido quando a licitante e/ou CONTRATADA descumprir qualquer obrigação, seja quando o descumprimento da obrigação ocorrer durante o procedimento licitatório ou na fase de execução contratual, entendida desde a recusa em retirar a nota de empenho ou assinar o contrato.

13.4. Da multa

13.4.1. A multa é a sanção pecuniária que será imposta à CONTRATADA pelo ordenador de despesas do DETRAN/DF, por atraso injustificado na entrega ou execução do contrato, e será aplicada nos seguintes percentuais:

I - 0,33% (trinta e três centésimos por cento) por dia de atraso, na execução de serviços, calculado sobre o valor correspondente à parte inadimplente, até o limite de 9,9%, que corresponde a até 30 (trinta) dias de atraso;

II - 0,66 % (sessenta e seis centésimos por cento) por dia de atraso, na execução de serviços, calculado, desde o primeiro dia de atraso, sobre o valor correspondente à parte inadimplente, em caráter excepcional, e a critério do órgão contratante, quando o atraso ultrapassar 30 (trinta) dias;

III - 5% (cinco por cento) sobre o valor total do contrato/nota de empenho, por descumprimento do prazo de entrega, sem prejuízo da aplicação do disposto nos incisos I e II

deste subitem;

IV - 15% (quinze por cento) em caso de recusa injustificada do adjudicatário em assinar o contrato ou retirar o instrumento equivalente, dentro do prazo estabelecido pela Administração, recusa parcial ou total na entrega do material, recusa na conclusão do serviço, ou rescisão do contrato/ nota de empenho, calculado sobre a parte inadimplente; e

V - 20% (vinte por cento) sobre o valor do contrato/nota de empenho, pelo descumprimento de qualquer cláusula do contrato, exceto prazo de entrega.

13.5. Da suspensão

13.6. A suspensão é a sanção que impede temporariamente o fornecedor de participar de licitação e de contratar com a Administração, e, se aplicada em decorrência de licitação na modalidade pregão, ainda suspende o registro cadastral da licitante e/ou CONTRATADA no Cadastro de Fornecedores do Distrito Federal, instituído pelo Decreto nº 25.966, de 23 de junho de 2005, e no Sistema de Cadastramento Unificado de Fornecedores – SICAF, de acordo com os prazos a seguir:

I - por até 30 (trinta) dias, quando, vencido o prazo de advertência, emitida pelo DETRAN/DF, a licitante e/ou CONTRATADA permanecer inadimplente;

II - por até 90 (noventa) dias, quando a licitante deixar de entregar, no prazo estabelecido no edital, os documentos e anexos exigidos, quer por via fax ou internet, de forma provisória, ou, em original ou cópia autenticada, de forma definitiva;

III - por até 12 (doze) meses, quando a licitante, na modalidade pregão, convocada dentro do prazo de validade de sua proposta, não celebrar o contrato, ensejar o retardamento na execução do seu objeto, falhar ou fraudar na execução do contrato; e

IV - por até 24 (vinte e quatro) meses, quando a licitante:

a) apresentar documentos fraudulentos, adulterados ou falsificados nas licitações, objetivando obter, para si ou para outrem, vantagem decorrente da adjudicação do objeto da licitação;

b) tenha praticado atos ilícitos visando a frustrar os objetivos da licitação;

c) receber qualquer das multas previstas no subitem anterior e não efetuar o pagamento.

14. DO ALINHAMENTO COM AS DETERMINAÇÕES DO ÓRGÃO DE CONTROLE (DECISÃO TCDF Nº 38/2026)

14.1. A presente contratação circunscreve-se ao fornecimento de **uma única solução específica de Inteligência Artificial (IA)** . Diante do escopo delimitado do objeto, os riscos inerentes à opacidade algorítmica ("caixa-preta") e a eventuais vieses cognitivos ou estatísticos encontram-se mapeados pelo órgão.

14.2. Em estrito cumprimento ao **Item IV, alínea 'b' da Decisão TCDF nº 38/2026** , justifica-se que a contratação de serviços terceiros especializados é a modelagem adotada pela Administração para suprir a atual limitação quantitativa de pessoal técnico interno, mitigando o risco de falhas na entrega tecnológica e garantindo que a fiscalização não ocorra de forma meramente formal.

14.3. A governança do objeto dar-se-á por meio de transferência de conhecimento da Contratada para a equipe de fiscalização. Adicionalmente, **na medida do possível e observada a disponibilidade operacional e orçamentária do órgão, a equipe interna será submetida a treinamentos e capacitações** ao longo da vigência contratual para o progressivo aperfeiçoamento na supervisão da ferramenta de IA.

15. DAS OBRIGAÇÕES ESPECÍFICAS DE PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO

15.1. **Vinculação e Subordinação às Diretrizes do Encarregado pelo Tratamento de Dados Pessoais (DPO):** A CONTRATADA obriga-se a submeter-se de forma estrita, integral e irrestrita às orientações, ordens, determinações e diretrizes técnicas emanadas pelo Encarregado pelo Tratamento de Dados Pessoais (DPO) do CONTRATANTE. Tal sujeição abrange toda e qualquer operação de tratamento de dados realizada no âmbito da execução do objeto, devendo a CONTRATADA adequar seus procedimentos técnicos de imediato sempre que instada pelo referido DPO.

15.2. **Condição de Eficácia para Início dos Serviços (Plano de Resposta a Incidentes):** A CONTRATADA deverá, obrigatoriamente, elaborar e entregar o **Plano de Resposta a Incidentes de Segurança e Privacidade**, devidamente estruturado e alinhado às melhores práticas de governança.

15.2.1. A entrega e aprovação formal do referido Plano por parte deste Órgão constitui **condição de eficácia indispensável e pré-requisito obrigatório** para a emissão da Ordem de Serviço (OS) inicial.

15.2.2. A exigência contida neste item dar-se-á em estrito e fiel cumprimento às disposições do **Decreto Distrital nº 45.771/2024** e ao comando do **Item III, alínea 'f' da Decisão TCDF nº 38/2026**, restando vedado o início de qualquer atividade executiva antes do adimplemento desta obrigação, sem prejuízo das sanções administrativas cabíveis por atraso.

16. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E REGIME DE EXECUÇÃO

16.1. Forma de seleção e critério de julgamento da proposta:

16.1.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo menor preço por grupo (grupo único), no modo aberto e fechado, adotando o procedimento auxiliar – Sistema de Registro de Preços.

16.1.1.1. O intervalo mínimo de lances a ser observado é de 1,0% (um por cento), de modo a não inviabilizar a competitividade definindo-se valores e incentivar a oferta de propostas mais vantajosas, na busca pela contratação mais atrativa.

16.1.1.2. De acordo com o art. 25, parágrafo único da Instrução Normativa SGD/ME nº 94, de 2022, é obrigatória a utilização da modalidade Pregão para as contratações de que trata está Instrução Normativa sempre que a solução de TIC for enquadrada como bem ou serviço comum, podendo-se utilizar o Diálogo Competitivo nos casos específicos previstos no art. 32 da Lei nº 14.133, de 2021, desde que devidamente justificado nos autos, conforme definido pela equipe de contratação do DETRAN/DF, este contratação se enquadra como serviços comum de TI.

16.1.2. Serão desclassificadas as propostas que não atenderem às especificações e exigências contidas neste Termo de Referência e/ou Edital, bem como aquelas que apresentarem preços excessivos ou manifestamente inexequíveis, comparados aos preços de mercado.

16.1.3. Conforme art. 12, § 4º, da IN SGD/ME nº 94, de 2022, "nas licitações por preço global, cada serviço ou produto do lote deverá estar discriminado em itens separados nas propostas de preços, de modo a permitir a identificação do seu preço individual na composição do preço global, e a eventual incidência sobre cada item das margens de preferência para produtos e serviços que atendam às Normas Técnicas Brasileiras - NTB, de acordo com o art. 26 da Lei nº 14.133, de 2021.

16.2. Regime de execução

16.2.1. O regime de execução do contrato será por preço global.

16.3. Exigências de habilitação

16.4. Para fins de habilitação, deverá o licitante comprovar os requisitos estabelecidos neste tópico.

16.5. Habilitação jurídica

16.5.1. Pessoa física: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

16.5.2. Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

16.5.3. Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-e-negocios/pt-br/empreendedor;

16.5.4. Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

16.5.5. Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020;

16.5.6. Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

16.5.7. Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz;

16.5.8. Sociedade cooperativa: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

16.5.9. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

16.6. Habilitação fiscal, social e trabalhista

16.6.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

16.6.2. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

16.6.3. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

16.6.4. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

16.6.5. Prova de inscrição no cadastro de contribuintes relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

Prova de regularidade com a Fazenda do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

16.6.6. Caso o fornecedor seja considerado isento dos tributos relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

16.6.7. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar

n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

16.7. Qualificação Econômico-Financeira

16.7.1. Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de pessoa física, desde que admitida a sua participação na licitação (art. 5º, inciso II, alínea "c", da Instrução Normativa Seges/ME nº 116, de 2021), ou de sociedade simples;

16.7.2. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II);

16.7.3. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, comprovando:

16.7.3.1. índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um);

16.7.4. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura; e

16.7.5. Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos.

16.7.6. Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped.

16.7.7. Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido para fins de habilitação. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. (Lei nº 14.133, de 2021, art. 65, §1º).

16.7.8. O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

16.8. Qualificação Técnica

16.8.1. Comprovação de aptidão para execução de serviço de complexidade pedagógica, tecnológica e operacional equivalente ou superior superior às demandas descritas neste termo de Referência, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso.

16.8.2. Para fins de comprovação da capacidade técnica (qualificação técnico-operacional), a licitante deverá apresentar no mínimo, 01 (um) Atestado de Capacidade Técnica comprovando a prestação de serviços fornecidos à pessoa jurídica de direito público ou privado, declarando que a licitante forneceu ou prestou serviços de complexidade similar.

16.8.3. Os atestados deverão:

16.8.3.1. Informar a razão social, o número do CNPJ e o endereço completo, tanto da empresa emitente, quanto da empresa contratada;

16.8.3.2. Conter data de emissão, bem como o nome, o cargo, o telefone de contato e a assinatura do responsável pela sua expedição;

16.8.3.3. Comprovar experiência mínima de 12 meses na execução de serviços de natureza semelhante ao objeto desta contratação, admitindo-se para esse fim o somatório de atestados, conforme previsto na alínea "b" do item 10.6 do Anexo VII-A da IN SEGES/MP nº 5/2017;

16.8.3.4. Fabricantes e Part-Numbers.

16.8.4. São requisitos a serem comprovados junto ao (s) atestado (s):

16.8.4.1. No mínimo 1.300 dispositivos de análise de segurança com IA (50% do item 1);

16.8.4.2. No mínimo 1.000 caixas postais monitoradas em ambiente em cloud (50% do item 4);

16.8.4.3. No mínimo 12 meses de serviço 24x7 de segurança da informação (50% do item 6).

16.9. Prova de Conceito - PoC

16.9.1. A licitante classificada provisoriamente em primeiro lugar será convocada pelo Pregoeiro para participar de uma Prova de Conceito - PoC, com o objetivo exclusivo de comprovação de que os recursos tecnológicos são suficientes e capazes de atender aos requisitos mínimos.

16.9.2. A convocação se deverá diretamente no chat, quando o Pregoeiro convocará a empresa mais bem classificada, para iniciar o evento de amostra de sua solução, que deverá iniciar em até 05 dias úteis, tendo como duração máxima, 02 dias corridos.

16.9.3. A empresa que não atender os itens exigidos, será inabilitada, resultando na convocação das demais licitantes, na ordem de classificação.

16.9.4. Após convocação, a licitante que realizará a amostra deverá enviar um e-mail, indicando o nome, cargo e documentos de identificação do responsável pela condução da PoC.

As demais licitantes poderão participar do evento, apenas na condição de ouvinte.

16.9.5. A empresa deverá comprovar, minimamente, os seguintes recursos:

16.9.5.1. Itens:

a) A solução deve possuir ISO 42001;

b) A solução deve ser capaz de aprender o comportamento da rede e de seus componentes (dispositivos e usuários) de forma autônoma e continuar se adaptando a variações de comportamento destes durante o tempo;

c) A solução deve realizar todas as inspeções, processamento, análise e detecção de anormalidades e gerenciamento localmente, ou seja, é vedada qualquer forma de envio de dados para fora da rede do órgão para o funcionamento da solução;

d) A solução deve possuir mecanismos de DPI (Deep Packet Inspection);

e) Solução deve realizar o aprendizado do ambiente de rede e inspeção do tráfego de forma off-line através de tráfego espelhado de porta nos switches, ou seja, não dependendo de qualquer escaneamento ativo, alteração de roteamento e fluxo de dados da rede;

f) A solução deve ser capaz de tomar ações autônomas de resposta contra ameaças e/ou ataques cibernéticos baseadas em sua inteligência artificial, nativamente, sem a necessidade de instalação de agentes, sem a necessidade de integração com outras soluções de segurança e sem depender de modo de operação inline que implique em mudanças na topologia de rede;

g) A solução deve permitir a inspeção de dados do Microsoft Office 365. Não será necessária a análise de e-mails;

h) A solução deve identificar de forma autônoma, sem intervenção humana, todas as redes ativas no ambiente (que tiveram tráfego inspecionado) e apresentar uma relação com todas as redes, máscara de rede, primeira vez em que a rede foi observada e quantidade de dispositivos observados na rede correspondente;

i) A solução deve identificar de forma autônoma, sem intervenção humana, todos os endereços IPs que trafegaram nas redes inspecionadas apresentando uma relação com no mínimo os seguintes dados:

j) Classificação do tipo de dispositivo (desktop, servidor, Impressora, câmera, iot, etc);

k) IP do dispositivo;

l) Mac Address;

m) Nome DNS do dispositivo;

n) Primeira vez que o dispositivo/IP foi visto na rede;

o) Última vez que o dispositivo foi visto na rede;

p) A solução deve fornecer visibilidade sobre vários os subprodutos da Plataforma Microsoft 365, incluindo Sharepoint/OneDrive, Dynamics, Teams e outros serviços do Microsoft 365, incluindo atividade do usuário no Tenant, criação e compartilhamento de arquivos e eventos administrativos. Para o Microsoft 365, não será necessária a análise de e-mails;

q) A solução deve ser comprovadamente baseada em análise de comportamento permitindo a detecção de, no mínimo, as seguintes anomalias:

r) Em caso de alertas, a solução deverá prover todas as hipóteses analisadas pela Inteligência Artificial para o devido diagnóstico;

s) A solução deve possuir mecanismos para exportar os dados armazenados no padrão de extensão '.pcap';

t) A solução deve permitir descriptografar dados de forma passiva ou ativa conexões SSL/TLS de, no mínimo, tráfego HTTP e HTTP2;

u) Deve ser capaz de tomar ações baseadas em desvio de comportamento;

v) Deve possuir a capacidade de quarentenar ou semi-quarentenar temporariamente dispositivos na rede;

w) Deve ser altamente configurável permitindo vários níveis de resposta a uma anomalia na rede;

x) Deve ser capaz de registrar todas as ações de resposta para propósitos de auditoria;

y) Deve fornecer ações de resposta na Plataforma Microsoft 365 em resposta a atividades altamente anômalas e potencialmente maliciosas - forçar um usuário a sair, desabilitar um usuário e bloquear um IP (ou intervalo de IP), autonomamente e no modo de confirmação humana;

z) Sumário dos dados aprendidos como: Dados totais processados por dia, Quantidade de Redes, Dispositivos e usuários identificados na rede;

aa) Área para gerenciamento de arquivos .pcap, exportação e visualização na própria interface;

ab) A solução deve possuir mecanismo para automação de investigação de alertas permitindo a correlação entre múltiplos eventos apesentando em uma única tela as seguintes informações;

ac) Deve possuir Inteligência artificial para automatizar triagens, análises e investigações de ameaças;

ad) Deve possuir um aplicativo mobile capaz de visualizar, responder a incidentes, notificar, reportar e aprovar remediações para Android e iOS;

ae) A solução de monitoramento de Deep/Dark Web deve ter como objetivo principal o rastreamento de salas, blogs, fóruns e sites na Deep/Dark Web para identificar informações relativas à CONTRATANTE e seus colaboradores como: credenciais roubadas e outros vazamentos de informações pessoais identificáveis;

af) Deve possuir alertas automáticos para os ativos expostos do Detran para identificação de Novas portas abertas, ceritificados SSL expirados e de novas vulnerabilidades descobertas

Deverá ser possível cadastrar a política de senha utilizada, para que a solução faça a comparação automática das credenciais vazadas com a política em vigência; ag) Solução deve permitir a busca por atores de ameaça cibernético, sendo necessário o seguinte:

ah) A solução deve fornecer em dashboard, um "Feed" de notícias de segurança cibernética atuais, com comentários e sugestões. Esse Feed permitirá ao DETRAN ficar sempre atualizado quanto aos últimos acontecimentos com relação aos termos pesquisados. Deve também ser possível fazer buscas e filtros no Feed diário de cyber;

ai) Deve possuir uma Central de Alertas, para habilitar notificações em caso de novas credenciais comprometidas e ativo exposto. Deve permitir configurar o envio de email em caso de novos alertas, bem como exportar os alertas atuais;

aj) A solução deve permitir buscas e análise de resultados vindos do Shodan;

ak) A solução deverá permitir o cadastro de produtos utilizados pelo Detran, de forma a realizar uma análise de vulnerabilidade dos produtos, com o respectivo CVE; al) Deve possuir inteligência artificial para realizar análise do resultado da busca realizada. A IA deve realizar, no mínimo.

16.9.6. Os itens exigidos serão registrados em ata, devendo ter a seguinte classificação: "atendido" ou "não atendido".

16.9.7. Os itens não atendidos e atendidos com ressalva deverão ser devidamente justificados, dando transparência aos motivos que impediram seu aceite.

16.9.8. Ao final será lavrada uma ata da sessão, que servirá de base para a homologação ou não da amostra.

16.10. Declaração do Fabricante

16.10.1. Será exigida como condição de celebração do instrumento contratual, declaração de que a licitante é parceiro oficial e está devidamente autorizada à comercializar seus produtos, suporte e manutenções.

16.11. Da Proposta Técnica

16.11.1. Deverá ser apresentada proposta técnica detalhada, com identificação precisa da solução ofertada, incluindo sua nomenclatura comercial, desenvolvedor responsável, versão homologada, arquitetura funcional, módulos integrados, tecnologias suportadas, protocolos de segurança e demais especificações que viabilizem a análise de aderência aos requisitos funcionais e pedagógicos estabelecidos. Tal documentação deverá vir acompanhada de memorial descritivo, planilha analítica de custos por item e resumo executivo da solução, contemplando vinculações explícitas entre funcionalidades ofertadas e exigências constantes do edital, contendo, ainda:

16.11.1.1. Razão social, CNPJ, Inscrição estadual, municipal e distrital, endereço completo, e-mail e telefone;

16.11.1.2. Dados bancários com nome do banco, agência, conta;

16.11.1.3. Dados da solução ofertada;

16.11.1.4. Planilha de custos;

16.11.1.5. Nome do fabricante, da solução, versão, partnumber ou qualquer elemento que a identifique;

16.11.1.6. Prazo de validade não inferior a 60 dias corridos, contados da sua apresentação;

16.11.1.7. Dados do responsável pela assinatura do contrato, com nome completo, CPF, RG, cargo, telefone e e-mail.

16.11.2. Deverá apresentar junto com a sua proposta técnica, para fins de avaliação de aderência técnica, uma planilha ponto-a-ponto, mostrando onde cada requisito do edital está sendo exigido em documento oficial do fabricante.

16.11.2.1. Para comprovação do Ponto a Ponto precisa apresentar manual, link, folder, datasheet, etc.

16.12. Vistoria

16.12.1. Não se aplica.

16.13. Preços Diferentes

16.13.1. Não haverá possibilidade de oferecer preços diferentes, considerando as características do objeto, sua padronização e configuração, uma vez que localidades distintas, quantidades e prazos, não são justificativas para interferir na composição dos custos.

17. GARANTIA DA CONTRATAÇÃO

17.1. Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, no percentual de 5% (cinco por cento) do valor total do contrato, conforme regras previstas no contrato.

17.2. A garantia, nas modalidades caução e fiança bancária, deverá ser prestada em até 10 dias úteis após a assinatura do contrato.

17.3. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à garantia da contratação.

18. DA SUSTENTABILIDADE

18.1. A contratada deverá declarar que atende aos requisitos de sustentabilidade previstos no art. 2º, da Lei Distrital nº 4.770/2012, em conformidade com o Decreto nº 7.746/2012, estabelece a implementação de critérios, práticas e ações de logística sustentável no âmbito da Administração Pública do Distrito Federal direta, autárquica e fundacional e das empresas estatais dependentes, devendo ser observados os requisitos ambientais com menor impacto ambiental em relação aos seus similares.

19. DA SEGURANÇA

19.1. Manutenção de Sigilo e Normas de Segurança

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

19.1.2. 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 da CONTRATADA, encontra-se anexado a este termo.

20. DA PREFERÊNCIA PARA EMPRESAS DE TECNOLOGIA DA INFORMAÇÃO

20.1. Não se aplica, pois existem empresas que não são do segmento de TIC que podem participar também.

21. DA ESTIMATIVA DE QUANTIDADE

21.1. Considerando o cenário mais adequado à realidade institucional e os elementos detalhados nos tópicos anteriores, a estimativa das quantidades relativas a cada item da solução foi definida com base em parâmetros objetivos e critérios técnico-demonstráveis, obtidos por meio dos cálculos apresentados a seguir:

21.1.1. Item 01: 01 unidade de subscrição;

21.1.2. Item 02: 20 unidades de subscrição;

21.1.3. Item 03: 500 unidades de subscrição;

21.1.4. Item 04: 2.248 unidades de subscrição;

21.1.5. Item 05: 02 unidades SaaS;

21.1.6. Item 06: 24 unidades mensais;

21.1.7. Item 07: 01 unidade de serviço.

22. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

22.1. O custo estimado total da contratação é de R$ 18.093.444,58 (dezoito milhões, noventa e três mil quatrocentos e quarenta e quatro reais e cinquenta e oito centavos), conforme o Mapa Comparativo de Preços 215045511:

Item	Serviço	CATMAT/CATSER	Métrica	Qtd	TOTAL ESTIMADO
1	Solução de previsão, monitoramento, detecção, notificação, investigação e resposta autônoma a ataques cibernéticos para dispositivos em análise de rede.	27502	Unidade	1	R$ 4.450.000,00
2	Expansão de Solução de previsão, monitoramento, detecção, notificação, investigação e resposta autônoma a ataques cibernéticos dispositivos em análise de rede – 100 dispositivos.	27502	Unidade	20	R$ 3.080.000,00

3	Expansão de Solução de previsão, monitoramento, detecção, notificação, investigação e resposta autônoma a ataques cibernéticos dispositivos em análise local com agente.	27502	Unidade	500	R$ 2.105.000,00
4	Solução de monitoramento, detecção, notificação, investigação e resposta autônoma a ataques cibernéticos em plataforma Microsoft 365.	27502	Unidade	2248	R$ 2.255.485,84
5	Solução de previsão, monitoramento, detecção, notificação, e investigação em plataforma aberta	27502	Unidade	2	R$ 3.906.380,30
6	Serviço ininterrupto de Notificações Proativas e de Ameaças de alto grau de criticidade e impacto em caráter 24x7	21202	Mensal	24	R$ 2.144.459,04
7	Serviço de Instalação e Configuração da Plataforma de Segurança para Defesa	27260	Unidade	1	R$ 152.119,40
					R$ 18.093.444,58

23. DA LICITAÇÃO EXCLUSIVA/COTA RESERVADA

23.1. Quanto à previsão de participação exclusiva das entidades preferenciais prevista nos Arts. 25, da Lei Distrital nº 4.611/2011 e 7º, do Decreto Distrital nº 35.592/2014, esclarecemos que tal proveito não se aplica à contratação almejada.

23.2. Quanto à previsão do benefício da Cota Reservada prevista na Lei Distrital nº 4.611/2011, que regulamenta no Distrito Federal o tratamento favorecido, diferenciado e simplificado para microempresas, empresas de pequeno porte e microempreendedores individuais, esclarecemos que tal proveito não se aplica à contratação almejada.

23.3. Não há viabilidade técnica tendo em vista não ser possível separar as quotas dos serviços, pois trata-se de contratação de solução que não permite a divisão de forma econômica e que garanta o fornecimento do objeto sem prejuízo técnico, em consonância ao art. 10, inciso I, do Decreto nº 35.592/2014.

23.4. Por tratar-se de serviços que devem ser prestados por uma única empresa, tendo em vista que sua divisão pode trazer prejuízos técnicos e de logística na sua prestação, não é possível previsão dos institutos da Subcontratação Compulsória, prevista no Art. 2º, Decreto distrital nº 35.592/2014.

24. ADEQUAÇÃO ORÇAMENTÁRIA

24.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Normas de Planejamento, Orçamento, Finanças, Patrimônio e Contabilidade do Distrito Federal.

24.2. A contratação será atendida pela seguinte dotação:

24.2.1. Gestão/Unidade: XXX

24.2.2. Fonte de Recursos: XXX

24.2.3. Programa de Trabalho: XXX

24.2.4. Elemento de Despesa: XXX

24.2.5. Plano Interno: XXX

25. CRONOGRAMA FÍSICO-FINANCEIRO

25.1. O fornecimento do objeto e a vigência de cada unidade deverá obedecer ao cronograma estipulado no projeto, sendo os pagamentos:

25.1.1. Item 01: Único para 24 meses;

25.1.2. Item 02: Único para 24 meses;

25.1.3. Item 03: Único para 24 meses;

25.1.4. Item 04: Único para 24 meses;

25.1.5. Item 05: Único para 24 meses;

25.1.6. Item 06: Mensal;

25.1.7. Item 07: Único.

26. DOS ANEXOS

26.1. São partes integrantes deste Termo de Referência, os seguintes anexos:

26.1.1. ANEXO I - ESPECIFICAÇÃO TÉCNICA;

26.1.2. ANEXO II - MODELO DE PROPOSTA DE PREÇOS;

26.1.3. ANEXO III - TERMO DE CONFIDENCIALIDADE CORPORATIVO;

26.1.4. ANEXO IV - TERMO DE CIÊNCIA

27. RESPONSÁVEIS PELA ELABORAÇÃO

O presente Termo de Referência foi elaborado em harmonia com a Instrução Normativa SGD/ME N.º 94, de 2023, recepcionada pelo Decreto Distrital N.º 45.011, 27 de setembro de 2023, bem como em conformidade com os requisitos técnicos necessários ao cumprimento das necessidades apresentadas pela Área Demandante. Além disso, atende adequadamente às demandas de negócio formuladas, os benefícios pretendidos são adequados, os custos previstos são compatíveis e caracterizam a economicidade, os riscos envolvidos são administráveis.		
Equipe de Planejamento da Contratação Instrução Nº 980/2023 (155454332)		
Fabio Fontes Borges matrícula: 256.790-3 Integrante Técnico	**Celso Henrique Sanches Medeiros matrícula: 1.727.015-4** Integrante Requisitante	**Augusto Henrique Parente Farias matrícula: 1.726.729-3** Integrante Administrativo

28. DA APROVAÇÃO

28.1. Considerando os termos do Decreto Distrital N.º 45.011, 27 de setembro de 2023, que recepcionou a Instrução Normativa SGD/ME N.º 94, de 2023, APROVO o presente Termo de Referência e ratifico a veracidade de todas as informações exaradas, assim como afirmo a ausência de direcionamento do objeto em tela.

Waldir da Silva Ferreira Júnior Matrícula: 256.634-6

Diretor de Tecnologia da Informação de Comunicação

29. ANEXO I - ESPECIFICAÇÃO TÉCNICA

Requisitos

29.1. **ITENS 1 a 4 - CARACTERÍSTICAS GERAIS**

29.1.1. A solução poderá ser composta por diversos módulos/ferramentas para atender os requisitos solicitados.

29.1.2. Deverá ser entregue junto com a proposta, uma planilha que comprove o atendimento de todos os itens técnicos, com indicação do manual e página de comprovação técnica.

29.1.3. Todos os componentes devem ser oficialmente suportados pelo(s) fabricante(s) da solução em acordo com as condições especificadas.

29.1.4. Não serão aceitos produtos ou serviços OpenSource.

29.1.5. A solução deve permitir Threat Hunting, análise comportamental da rede e seus componentes, detecção de anomalia(s) o e visibilidade de rede.

29.1.6. A solução deve ser dotada de tecnologia baseada em Inteligência Artificial a fim de identificar anomalias de comportamento e ataques sutis não identificados pelas tecnologias tradicionais de segurança da informação.

29.1.6.1. Para garantir a segurança dos dados, toda análise em Inteligência Artificial, deve ser realizada no ambiente do DETRAN/DF, sem envio de dados para fora do ambiente.

29.1.6.2. A solução deve possuir ISO 42001.

29.1.7. Deve utilizar no mínimo os seguintes métodos de inteligência artificial para criação de perfis de uso e identificação de desvios comportamentais na rede:

29.1.7.1. Machine learning não supervisionado;

29.1.7.2. Machine learning supervisionado;

29.1.7.3. Deep Learning;

29.1.7.4. Redes Neurais;

29.1.8. A solução não deve depender de pré-configurações baseadas na rede do órgão para que identifique associações entre múltiplos elementos da rede para que consiga identificar anomalias de comportamento.

29.1.9. A solução deve ser capaz de aprender o comportamento da rede e de seus componentes (dispositivos e usuários) de forma autônoma e continuar se adaptando a variações de comportamento destes durante o tempo.

29.1.10. A plataforma deverá prover arquitetura escalável, horizontalmente, permitindo o crescimento de dispositivos suportados, além dos previstos nesta contratação, por meio da adição de novos sensores e licenciamento, não se limitando a ativos de TI (desktops, laptops, servidores, impressora, câmeras, etc), mas que suporte a inclusão futura de ativos de IoT industrial provenientes de redes de automação.

29.1.11. A solução deve realizar todas as inspeções, processamento, análise e detecção de anormalidades e gerenciamento localmente, ou seja, é vedada qualquer forma de envio de dados para fora da rede do órgão para o funcionamento da solução.

29.1.12. A solução deve possuir mecanismos de DPI (Deep Packet Inspection).

29.1.13. Solução deve realizar o aprendizado do ambiente de rede e inspeção do tráfego de forma off-line através de tráfego espelhado de porta nos switches, ou seja, não dependendo de qualquer escaneamento ativo, alteração de roteamento e fluxo de dados da rede.

29.1.14. A solução deve inspecionar e analisar os dados brutos da rede através de espelhamento de porta (SPAN/Port Mirror) ou através do uso de TAP – Terminal Access Point.

29.1.15. Para usuários em localidade remota (item 3), deverá possuir agente de instalação local no dispositivo, com as seguintes características mínimas:

29.1.15.1. Consumir no máximo 100MB de espaço em disco;

29.1.15.2. Consumir no máximo 50MB de memória;

29.1.15.3. Consumir o máximo 2 kB/s de banda;

29.1.15.4. Não requerer reboot da máquina;

29.1.15.5. Ser compatível com os seguintes sistemas operacionais:

a) Windows 365;

b) Windows 10;

c) Windows 11;

d) Windows Server 2022;

e) Windows Server 2019;

f) Windows Server 2016;

g) MacOS 13;

h) MacOS 14;

i) Debian 9 ou superior;

j) Ubuntu 18.04 ou superior;

k) OpenSUSE 15.0 ou superior;

l) Centos 7 ou superior;

m) RHEL 7 ou superior;

n) SUSE Linux Enterprise 12.4 ou superior.

29.1.16. A solução deve suportar a ingestão de dados através de mecanismos de tunelamento de tráfego na camada 2 (enlace) do modelo OSI como VXLAN e ERSPAN.

29.1.17. A solução deve suportar a ingestão de dados no formato Netflow.

29.1.18. A solução deve ser capaz de tomar ações autônomas de resposta contra ameaças e/ou ataques cibernéticos baseadas em sua inteligência artificial, nativamente, sem a necessidade de instalação de agentes, sem a necessidade de integração com outras soluções de segurança e sem depender de modo de operação inline que implique em mudanças na topologia de rede.

29.1.19. A solução deve ser capaz de integrar-se a soluções de segurança terceiras a fim de permitir ações adicionais de bloqueio contra ataques cibernéticos.

29.1.20. A solução deve permitir a inspeção de dados do Microsoft Office 365. Não será necessária a análise de e-mails.

29.1.21. A solução deve identificar de forma autônoma, sem intervenção humana, todas as redes ativas no ambiente (que tiveram tráfego inspecionado) e apresentar uma relação com todas as redes, máscara de rede, primeira vez em que a rede foi observada e quantidade de dispositivos observados na rede correspondente.

29.1.22. A solução deve identificar de forma autônoma, sem intervenção humana, todos os endereços IPs que trafegaram nas redes inspecionadas apresentando uma relação com no mínimo os seguintes dados:

29.1.22.1. Classificação do tipo de dispositivo (desktop, servidor, Impressora, câmera, iot, etc);

29.1.22.2. IP do dispositivo;

29.1.22.3. Mac Address;

29.1.22.4. Nome DNS do dispositivo;

29.1.22.5. Primeira vez que o dispositivo/IP foi visto na rede;

29.1.22.6. Última vez que o dispositivo foi visto na rede.

29.1.23. Deve ser possível visualizar o histórico de IPs de um determinado dispositivo baseado no IP provido pelo servidor DHCP.

29.1.24. A solução deve fornecer visibilidade sobre vários os subprodutos da Plataforma Microsoft 365, incluindo Sharepoint/OneDrive, Dynamics, Teams e outros serviços do Microsoft 365, incluindo atividade do usuário no Tenant, criação e compartilhamento de arquivos e eventos administrativos. Para o Microsoft 365, não será necessária a análise de e-mails.

29.1.24.1. Integração via API diretamente do log de auditoria unificado da Microsoft sobre os eventos auditados pela Microsoft e dados registrados como parte dessas entradas do log de auditoria. O monitoramento da Plataforma Microsoft 365 deve ser obtido por meio de solicitações HTTPS feitas com um token autenticado no log de auditoria unificado da Microsoft.

29.1.25. A solução deve criar métricas, de forma autônoma, de raridade de Ips, Domínios DNS, Dispositivos, etc baseado na frequência que estes são acessados através da rede.

29.1.26. A solução deve criar métricas, de forma autônoma, de anormalidades comparando a ação atual de um dispositivo, usuário, IP, domínio, etc contra as ações de mesmo escopo realizadas no passado.

29.1.26.1. A métrica de anormalidade deve apresentar o percentual de desvio do comportamento atual de um dispositivo comparado com o comportamento passado aprendido.

29.1.27. A solução deve ser comprovadamente baseada em análise de comportamento permitindo a detecção de, no mínimo, as seguintes anomalias:

29.1.27.1. Dispositivo realizando conexões para destinos raros na internet não frequentemente visitados com por dispositivos da rede interna.

29.1.27.2. Dispositivo se comunicando com um servidor externo usando um certificado auto assinado.

29.1.27.3. Dispositivo se comunicando com um servidor usando um certificado expirado.

29.1.27.4. Dispositivo se comunicando com um dispositivo externo usando um certificado inválido.

29.1.27.5. Dispositivo iniciando várias conexões para um IP externo raro de maneira regular. (Beaconing)

29.1.27.6. Dispositivo gerando um grande número de solicitações para servidores Web internos o qual está retornando códigos de erro HTTP.

29.1.27.7. Novo dispositivo entrou na rede e começou a utilizar o software de teste de penetração ou escaneamento de rede.

29.1.27.8. Vários dispositivos internos começaram a desviar de suas atividades normais e escanearam a rede interna.

29.1.27.9. Dispositivo fazendo requisições de DNS repetidas recebendo respostas com registro TXT. (Tunelamento via DNS)

29.1.27.10. Dispositivo se comunicando externamente via DNS de maneira consistente com o tunelamento de DNS.

29.1.27.11. Dispositivo fazendo conexões criptografadas para um domínio relacionado a DNS Dinâmico

29.1.27.12. Dispositivo gerando um volume anormalmente alto de solicitações DNS.

29.1.27.13. Dispositivo fazendo uma série de conexões utilizando Hostnames raros que parecem não ter uma resolução de DNS legítima.

29.1.27.14. Um servidor DNS interno está agindo como um resolvedor de DNS aberto (OpenDns).

29.1.27.15. Dispositivo se comunicando com o serviço de anonimização da rede TOR.

29.1.27.16. Dispositivo se comunicando com a rede Tor por meio de um Web Service intermediário.

29.1.27.17. Atividade anormal de PowerShell e o Windown Romote Mamagement, seguido por uma conexão a um destino externo raro seguido de download de arquivo suspeito.

29.1.27.18. Dispositivo executando comandos PsExec em uma máquina remota que nunca havia recebido tráfego similar anteriormente.

29.1.27.19. Dispositivo se conectando repetidamente a destinos externos que não possuem nomes legíveis para humanos.

29.1.27.20. Dispositivo detectado conectando-se a hostnames identificados como trojans financeiros.

29.1.27.21. Dispositivo fazendo conexões com hostnames raros associados a uma botnet.

29.1.27.22. Dispositivo solicitando um domínio conhecido por hospedar malwares.

29.1.27.23. Dispositivo gravando arquivos com nomes suspeitos, relacionado a ransomware, em Servidores de arquivos da rede SMB.

29.1.27.24. Dispositivo transferindo um volume de moderado a grande de dados para fora da rede durante um período de 24 horas ou mais por meio de um grande volume de conexões.

29.1.27.25. Dispositivo fazendo download dados de um sistema interno e fazendo upload de volumes de dados semelhantes para destino externo.

29.1.27.26. Dispositivo se comunicando com domínios suspeitos na internet e, ao mesmo tempo, realizando comportamentos incomuns de SMB na rede interna.

29.1.27.27. Dispositivo acessando uma grande quantidade de compartilhamentos SMB que não foram acessados anteriormente pelo mesmo dispositivo.

29.1.27.28. Dispositivo não conseguiu estabelecer uma sessão SMB2 seguida de uma configuração bem-sucedida da sessão SMB1 usando credenciais administrativas.

29.1.27.29. Dispositivo lendo e gravando volumes de dados semelhantes para compartilhamentos de arquivos remotos.

29.1.27.30. Dispositivo acessando arquivos que possuem de senhas não criptografadas.

29.1.27.31. Dispositivo enviando um grande volume de dados para um IP externo que raramente é utilizado por qualquer dispositivo na rede interna.

29.1.27.32. Dispositivo fazendo conexões web externas sem usar um proxy web.

29.1.27.33. Dispositivo sendo bloqueado repetidamente por um proxy web durante um período de várias horas.

29.1.27.34. Dispositivo solicitando informações de configuração de proxy (WPAD) para um IP externo.

29.1.27.35. Dispositivo fazendo conexões HTTP suspeitas, de forma repetitiva, diretamente para um endereço IP sem utilizar um Hostname.

29.1.27.36. Dispositivo foi redirecionado para um Hostname HTTP raro e em seguida baixou um executável ou outro arquivo binário.

29.1.27.37. Dispositivo causando repetidos picos de conexões HTTP ou SSL na rede interna ou para a internet.

29.1.27.38. Dispositivo fazendo requisições HTTP suspeitas repetidamente em portas não padrão.

29.1.27.39. Dispositivo informando no cabeçalho User-Agent que possui um sistema operacional o qual é diferente do SO que realmente está utilizando.

29.1.27.40. Dispositivo fazendo download de um arquivo que não corresponde ao seu 'File Type' de uma fonte externa que a rede normalmente não acessa.

29.1.27.41. Dispositivo fazendo download de arquivo executável vindo de uma fonte a qual não é comumente acessada por dispositivos da rede interna.

29.1.27.42. Dispositivo fazendo download de arquivo comprimido vindo de uma fonte a qual não é comumente acessada por dispositivos da rede interna.

29.1.27.43. Dispositivo fazendo download de um arquivo suspeito e em seguida fez uma conexão para um destino externo com o qual a rede normalmente não se comunica.

29.1.27.44. Dispositivo usando uma plataforma externa de armazenamento de arquivos de terceiros.

29.1.27.45. Dispositivo enviando dados para o Pastebin.

29.1.27.46. Dispositivo usando um sistema terceiro de mensageria (Whatsapp ou similares).

29.1.27.47. Dispositivo acessando rede social (Facebook ou similares).

29.1.27.48. Dispositivo se comunicando com um destino raro na internet usando portas normalmente usadas apenas na rede interna.

29.1.27.49. Dispositivo fazendo conexões peer-to-peer BitTorrent.

29.1.27.50. Dispositivo recebeu um número anormalmente grande de conexões de entrada de IP externos raros.

29.1.27.51. Dispositivo fazendo conexões SQL para IPs externos a rede.

29.1.27.52. Dispositivo enviando uma quantidade anormal alta de dados para destinos fora da rede.

29.1.27.53. Dispositivo trocando um volume de dados anormal com outro dispositivo na rede interna.

29.1.27.54. Dispositivo enviando uma quantidade anormalmente alta de dados externamente para um local para o qual a rede não enviou dados anteriormente.

29.1.27.55. Dispositivo explorado vulnerabilidade Heartbleed na rede interna.

29.1.27.56. Dispositivo se conectando a um DNS SinkHole conhecido.

29.1.27.57. Dispositivo realizando grandes volumes de pequenas conexões SSH e/ou RDP.

29.1.27.58. Dispositivo iniciando um grande número de conexões para um servidor RDP e/ou SSH.

29.1.27.59. Dispositivo recebendo um grande número de conexões RDP de entrada de IPs externos raros.

29.1.27.60. Alteração de bloco CIDR de uma subrede.

29.1.27.61. Alteração no comportamento de tráfego DHCP.

29.1.27.62. Novo servidor DNS na rede.

29.1.27.63. Novo servidor de proxy web na rede.

29.1.27.64. Adição ou remoção de domínios DNS na rede.

29.1.27.65. Perda de pacotes é superior a X% na rede.

29.1.27.66. Uma senha de credencial de alto privilégio foi alterada no domínio Windows.

29.1.27.67. Uma credencial efetuando login de uma origem incomum.

29.1.27.68. Uma credencial foi usada em múltiplos dispositivos internos.

29.1.27.69. Um dispositivo gerou um grande número de falhas de sessão SMB.

29.1.27.70. Um dispositivo desviou de suas atividades normais criando várias falhas de login Kerberos.

29.1.28. Deve ser possível criar regras utilizando um ou mais dos componentes do item acima.

29.1.29. A solução deve permitir o recebimento de telemetria de diferentes soluções para auxílio na análise de ameaças, como:

29.1.29.1. STIX/TAXII;

29.1.29.2. Fortinet;

29.1.29.3. Tenable;

29.1.29.4. Rapid7;

29.1.29.5. Qualys

29.1.30. Deve permitir interação com Firewall’s, como:

29.1.30.1. Cisco;

29.1.30.2. Palo Alto;

29.1.30.3. Check Point;

29.1.30.4. Fortinet.

29.1.31. Todos os dados processados pela solução devem ser armazenados para posterior análise independentemente de terem gerado alertas ou não.

29.1.31.1. Em caso de alertas, a solução deverá prover todas as hipóteses analisadas pela Inteligência Artificial para o devido diagnóstico.

29.1.32. A solução deve possuir mecanismos para exportar os dados armazenados no padrão de extensão '.pcap'.

29.1.33. A solução deve permitir descriptografar dados de forma passiva ou ativa conexões SSL/TLS de, no mínimo, tráfego HTTP e HTTP2.

29.1.33.1. A solução deve analisar o handshake TLS e o payload real.

29.1.33.2. Deve ser possível delimitar o tráfego que será descriptografado, como somente o tráfego de saída para hostnames raros ou todo o tráfego.

29.1.34. Deve ser capaz de agrupar de forma autônoma dispositivos em grupos baseado em sua similaridade de comportamento.

29.1.35. Deve ser capaz de tomar ações baseadas em desvio de comportamento.

29.1.36. Deve possuir a capacidade de quarentenar ou semi-quarentenar temporariamente dispositivos na rede.

29.1.37. Deve possuir a habilidade para responder, desacelerar e/ou parar ameaças autonomamente.

29.1.38. Deve ser capaz de marcar dispositivos automaticamente para decisões de resposta e ajuste fino.

29.1.39. Deve ser altamente configurável permitindo vários níveis de resposta a uma anomalia na rede.

29.1.40. Deve ser capaz de registrar todas as ações de resposta para propósitos de auditoria.

29.1.41. Deve ser configurável para supervisão e aprovação de analistas em ações de tomada de decisão / resposta.

29.1.42. Deve fornecer ações de resposta na Plataforma Microsoft 365 em resposta a atividades altamente anômalas e potencialmente maliciosas - forçar um usuário a sair, desabilitar um usuário e bloquear um IP (ou intervalo de IP), autonomamente e no modo de confirmação humana.

29.1.43. Do gerenciamento

29.1.43.1. O gerenciador deve possuir controle de interface gráfica (GUI: Graphical User Interface) e interface texto (CLI);

29.1.43.2. A interface de texto (CLI) deve possuir comandos para permitir a realização de troubleshooting;

29.1.43.3. A interface gráfica não deve ser desenvolvida ou conter componentes baseados em java por questões de compatibilidade com browsers modernos;

29.1.43.4. A interface gráfica deve possuir no mínimo:

a) Sumário dos dados aprendidos como: Dados totais processados por dia, Quantidade de Redes, Dispositivos e usuários identificados na rede.

b) Lista de alertas de anormalidade identificadas.

c) Critérios de filtro dos alertas de anormalidade por categoria de alerta, dispositivo ou usuários.

d) Critérios de filtro de período (data e horário) para os alertas de anormalidade.

e) Critérios de filtro de prioridade (risco) para os alertas de anormalidade.

f) Apresentar a posição geográfica das redes no ambiente de TI.

g) Opções de configuração do sistema

h) Área de gerenciamento de usuários

i) Área para gerenciamento de arquivos .pcap, exportação e visualização na própria interface.

j) Área de busca de dados na base de dados da solução.

29.1.43.5. Os alertas de anomalia devem conter no mínimo os seguintes dados:

a) Identificador único (Unique ID).

b) Data e horário.

c) Dispositivo que originou a ação.

d) Apresentar o IP de origem do Dispositivo.

e) Apresentar o MAC address do Dispositivo.

f) Apresentar o Hostname (DNS) do Dispositivo.

g) Apresentar o (s) usuário(s) que se eventualmente se logaram no Dispositivo nas últimas horas.

h) Apresentar o a rede a qual o dispositivo estava conectado.

i) Descrição técnica do evento.

j) Gráfico apresentando a quantidade de eventos similares e evolução do nível de risco.

k) Atalho para acesso rápido às configurações da política que gerou o alerta.

l) Dados técnicos resumidos das ações que causaram a anomalia e subsequente alerta.

m) Atalho para acessar dados detalhados das ações que causaram a anomalia e subsequente alerta.

29.1.43.6. Durante a investigação de uma anomalia/alerta o administrador pode acessar os dados abaixo utilizando apenas o mouse.

a) Dados detalhados do dispositivo que originou a anomalia.

b) IP do dispositivo

c) Mac Address

d) Nome DNS do dispositivo

e) Primeira vez que o dispositivo/IP foi visto na rede

f) Última vez que o dispositivo foi visto na rede

g) Apresentar o (s) usuário(s) que se eventualmente se logou(aram) no Dispositivo.

h) Apresentar o a rede a qual o dispositivo estava conectado.

i) Acesso a todas as comunicações realizadas pelo dispositivo na rede.

j) Acesso a todas as anomalias as quais o dispositivo gerou na rede.

k) Acesso a ferramenta para geração de gráficos que facilitem a investigação utilizando critérios como, mas não limitados a:

l) Dados relacionados a conexões.

m) Tráfego de dados.

n) Requisições DNS.

o) Erros de Login.

p) Ações utilizando SMB.

29.1.43.7. Apresentar gráfico representando os fluxos de comunicação entre os dispositivos que originaram e receberam tráfego anômalo.

29.1.43.8. A solução deve possuir mecanismo para automação de investigação de alertas permitindo a correlação entre múltiplos eventos apesentando em uma única tela as

seguintes informações:

a) Linha do tempo apontando a correlação entre alertas emitidos para um determinado dispositivo, data e horário em que cada alerta foi emitido bem como o período em que cada ação anômala, que gerou o alerta, ocorreu.

b) Apresentação individual de cada alerta contendo: Descrição do comportamento anômalo e riscos associados.

c) Dados técnicos relacionados ao alerta como:

• Período em que a anomalia foi observada.

• IP de origem

• IP(s) de destino

• Credencial de usuário observada no dispositivo

• Ação anômala identificada pela solução.

• Acesso aos logs do tráfego anômalo.

d) Deverá classificar cada alerta baseado em fases de ataque.

e) Deve permitir ao administrador exportar todas as informações acima em documento padrão .pdf.

29.1.43.9. A interface deve permitir a procura e navegação de qualquer dispositivo, usuário, Ips, etc que tenham sido inspecionados em qualquer data armazenada pela solução.

29.1.43.10. Ao navegar pelas comunicações do dispositivo o administrador pode utilizar filtros baseados em IP, Porta e Protocolo para facilitar a visualização.

29.1.43.11. Ao navegar pelas comunicações do dispositivo o administrador pode utilizar um IP de destino como filtro permitindo a investigação de 'Origem > Destino' ou 'Destino > Origem'.

29.1.43.12. Ao navegar pelas comunicações de um usuário o administrador pode analisar todo o histórico de login do mesmo contendo a data, o ip de origem do dispositivo que utilizou a credencial do usuário e estado da autenticação.

29.1.43.13. O administrador pode gerar arquivos '.pcap' para quaisquer comunicações inspecionada pela solução.

29.1.43.14. A solução deve se integrar com serviço LDAP a fim de possibilitar a autenticação e autorização de usuários na interface de administração e para consultas com objetivos de enriquecer os dados inspecionados.

29.1.43.15. A solução deve permitir a utilização de segundo fator de autenticação para logins na interface web.

29.1.43.16. A solução deve possuir mecanismo de gerenciamento de usurários da interface web permitindo:

a) Criação, modificação ou remoção de usuários;

b) Gerenciamento de permissionamento dos usuários.;

c) Opção de gerar usuário com permissão de leitura apenas.

29.1.43.17. Deve possuir interface para visualização dos aspectos do sistema como:

29.1.43.18. A versão de software, espaço utilizado em disco, consumo de CPU e consumo de memória;

29.1.43.19. Informação de todas as interfaces ativas e respectivo tráfego recebido através de cada uma delas.

29.1.43.20. Total de banda processada no momento, a média de banda processada e o pico de banda registrado nas últimas semanas.

29.1.43.21. Uma análise detalhada de todo o tráfego recebido no dispositivo bem como a última vez em que os principais protocolos foram vistos dentre eles, HTTP, HTTPS, FTP, LDAP, SMTP, SSH, SMB, SSDP, POP3, NTLM, IMAP, Kerberos, dentre outros.

29.1.43.22. Listagem de todas as sub-redes identificadas no ambiente bem como a quantidade de dispositivos em cada sub rede.

29.1.43.23. Deve permitir o envio de e-mails de alertas emitidos pela solução.

29.1.43.24. Deve permitir o envio de logs para sistemas externos utilizando os seguintes padrões:

a) CEF;

b) LEEF;

c) JSON;

d) Syslog;

29.1.43.25. Deve permitir a integração com plataformas de Threat Inteligence utilizando os protocolos STIX/TAXII.

29.1.43.26. A plataforma deve possuir OPEN API para suportar integração com sistemas terceiros.

29.1.43.27. Deve possuir Inteligência artificial para automatizar triagens, análises e investigações de ameaças.

29.1.43.28. Deve possuir um aplicativo mobile capaz de visualizar, responder a incidentes, notificar, reportar e aprovar remediações para Android e iOS.

29.1.43.29. Deve possuir painel incorporado para executar consultas em metadados no tráfego inspecionado.

29.1.44. CARACTERÍSTICAS DE GERENCIAMENTO DE RELATÓRIOS

29.1.44.1. Deve permitir a criação automática de relatórios executivos cobrindo no mínimo:

a) Indicação da quantidade total de dispositivos, quantidade total de sub-redes e banda média processada.

b) Sumário das violações por fase do ataque.

c) Sumário dos dispositivos com maior nível de brechas não usuais.

d) Sumario dos top dispositivos que mais violaram comportamentos anômalos.

Violações mais frequentes a principais itens de compliance como: uso de USB no dispositivo, google drive, tráfego RDP saindo da rede, acesso a servidor SQL através da internet, dentre outros.

e) Sumário dos dispositivos que mais violaram os itens de compliance gerando risco a organização.

29.1.44.2. Deve permitir que o relatório seja exportado para documento padrão .PDF e/ou .csv

29.1.44.3. Deve possuir mecanismo para busca de dados diretamente na base de dados da solução.

29.1.44.4. O administrador pode gerar pesquisas e relatório dos seguintes critérios, mas não limitados a:

a) Data e Horário;

b) Endereços IPs de origem e destino;

c) Versão do protocolo IP;

d) Protocolo de comunicação;

e) Estado da conexão;

f) Dados trafegados de entrada e saída;

g) Método HTTP;

h) Cabeçalhos HTTP

i) Versão do SSL;

j) Cifragem da Conexão SSL;

k) Logins Kerberos;

l) Comunicações DNS;

m) Comunicações FTP;

n) Comunicações LDAP;

o) Comunicações Kerberos;

p) Comunicações de mineração de criptomoedas;

q) Comunicações SMB;

r) Comunicações Radius;

s) Comunicações RDP;

t) Comunicações SIP;

29.1.44.5. A procura na base da solução deve apresentar resultados em menos de 5 minutos de execução independentemente do escopo da pesquisa.

29.1.45. Do monitoramento DEEP/DARK WEB

29.1.45.1. Será aceita solução no formato de módulo integrado ou solução separada de monitoramento da Deep/Dark web. Em ambos os cenários, deverá ser ofertado como parte do item 1 e deve possuir as características a seguir:

29.1.45.2. A solução de monitoramento de Deep/Dark Web deve ter como objetivo principal o rastreamento de salas, blogs, fóruns e sites na Deep/Dark Web para identificar informações relativas à CONTRATANTE e seus colaboradores como: credenciais roubadas e outros vazamentos de informações pessoais identificáveis;

29.1.45.3. A solução de monitoramento de Deep/Dark Web deve estar licenciada para monitorar no mínimo 90 (noventa) termos, considerando: IP's externos, Pessoas, E-mail, Domínio, Modelos de Hardware e Software, dentre outros;

29.1.45.4. O serviço de monitoramento de Deep/Dark Web deve ser prestado no regime 24x7 (vinte e quatro horas por dia, sete dias por semana);

29.1.45.5. O DETRAN-DF deverá possuir acesso ao módulo de monitoramento de Dark/Depp web, com no mínimo função de visualização. A administração desse módulo será de responsabilidade da CONTRATADA;

29.1.45.6. A solução de monitoramento de Deep/Dark Web deve ter a capacidade de buscar dados pelo período mínimo de 2 anos;

29.1.45.7. Possuir uso de algoritmos de pontuação de ameaças baseados nos fluxos de trabalho e processo de análise de pesquisadores experientes em inteligência de ameaças cibernéticas;

29.1.45.8. Permitir que os usuários criem alertas dedicados com base em parâmetros definidos;

29.1.45.9. Deve possuir alertas automáticos para os ativos expostos do Detran para identificação de Novas portas abertas, ceritificados SSL expirados e de novas vulnerabilidades descobertas;

29.1.45.10. Deverá permitir classificar o risco de cada informação encontrada;

29.1.45.11. Deverá ser possível cadastrar a política de senha utilizada, para que a solução faça a comparação automática das credenciais vazadas com a política em vigência;

29.1.45.12. Oferecer análise constante de fluxo de inteligência acionável, baseada em contexto e que possa alertar os usuários sobre atividades cibernéticas suspeitas;

29.1.45.13. A solução de inteligência cibernética, deverá possuir recursos necessários para compreensão de ameaças em mais de 20 idiomas, incluindo:

a) Chinês, Russo, Árabe, Inglês e Farsi.

29.1.45.14. Permitir acesso a possíveis dados do DETRAN-DF vazados e postados em mais de 20 plataformas de compartilhamento de dados.

29.1.45.15. Possuir acesso as seguintes redes anônimas; Darknet e Zeronet

29.1.45.16. A coleta de dados para análise de ameaças deverá ser realizada diariamente.

29.1.45.17. Obter informações de repositórios de códigos GitHub

29.1.45.18. Obter informações da Zeronet

29.1.45.19. Solução deve permitir a busca por atores de ameaça cibernético, sendo necessário o seguinte:

a) Identificar blogs, fóruns, serviços de mensageria, mercados negros onde o ator de ameaça está presente;

b) Apresentar posts realizados pelo ator de ameaça em cada fonte;

c) Extrair de forma automática palavras do ator de ameaça em cada fonte de informação identificada;

d) Extrair entidades como IPs, e-mails dos posts realizados pelo ator de ameaça em cada fonte de informação identificada.

29.1.45.20. A solução deve fornecer em dashboard, um "Feed" de notícias de segurança cibernética atuais, com comentários e sugestões. Esse Feed permitirá ao DETRAN ficar sempre atualizado quanto aos últimos acontecimentos com relação aos termos pesquisados. Deve também ser possível fazer buscas e filtros no Feed diário de cyber.

29.1.45.21. Deve possuir uma Central de Alertas, para habilitar notificações em caso de novas credenciais comprometidas e ativo exposto. Deve permitir configurar o envio de email em caso de novos alertas, bem como exportar os alertas atuais.

29.1.45.22. A solução deve permitir:

a) Descobrir IPs e servidores a partir de nomes associados com a organização;

b) Filtros por severidade, de forma a encontrar IPs e servidores com vulnerabilidades mais graves;

c) Mostrar a origem das informações e a data de atualização da informação apresentada.

d) A solução deve permitir buscas e análise de resultados vindos do Shodan.

• Deverá possuir visualização da superfície de ataque encontrada, com classificação de risco.

• Deve mostrar quais são as vulnerabilidades encontradas.

e) Solução deve buscar no Shodan, fóruns russos e DarkWeb, informações sobre IPs e servidores relacionados com o DETRAN e criar um dashboard com vulnerabilidades e severidades associadas com cada ativo encontrado.

f) A partir da definição do que se deseja monitorar nas camadas da Web (Web aberta, Web privada, Deep Web e DarkWeb), o sistema deve ser capaz de coletar, analisar e organizar volumes de dados que ultrapassam milhões de dados.

g) A solução deve permitir que se faça consultas ad-hoc e individuais a fontes específicas da DarkWeb. Por exemplo, além de ser possível configurar "traga tudo da DarkWeb sobre essa 'expressão'", o DETRAN pode executar uma consulta a uma fonte específica como fórum particular de hackers russos.

h) A solução deve permitir aos analistas criar incidentes, vincularem informações aos incidentes e compartilhar informações entre analistas cibernéticos.

i) A solução deve fornecer workflows de mitigação para as atividades e riscos encontrados.

29.1.45.23. A solução deve prover acesso a dados compartilhados em sistemas de compartilhamentos de textos (como Pastebin), tanto na Web aberta como DarkWeb.

29.1.45.24. A solução deve permitir monitoramento de repositórios de códigos, incluindo o GitHub.

29.1.45.25. A solução deve permitir a coleta de dados por Feeds RSS.

29.1.45.26. A solução deve permitir a coleta e análise de dados de plataformas de mensagens instantâneas, como o Telegram.

29.1.45.27. A solução deve permitir pesquisas por IOCs – Indicadores de Comprometimento, relacionados a determinada ameaça ou incidente cibernético.

29.1.45.28. A solução deve exportar dados (como IOCs) por API no formato STIX. Deve suportar, no mínimo o protocolo TAXII.

29.1.45.29. A solução deverá permitir o cadastro de produtos utilizados pelo Detran, de forma a realizar uma análise de vulnerabilidade dos produtos, com o respectivo CVE.

a) Deverá citar, no mínimo, as 10 vulnerabilidades mais críticas dos produtos cadastrados;

b) Deverá possuir uma classificação para priorização de aplicação de patch;

c) Para cada vulnerabilidade, deve mostrar as seguintes informações:

• Vetor de Ataque;

• Impacto em Confidencialidade;

• Impacto em Integridade;

• Impacto em Disponibilidade;

• Complexidade do Ataque;

• Histórico de menção da vulnerabilidade em DarkWeb, Clear Web, Rede Sociais e RSS;

29.1.45.30. Deve permitir monitorar todos as publicações de um atacante, de forma a verificar as informações e veracidade das informações de cada um. Como exemplo: Grupo Lockbit.

a) Deve possuir uma classificação de reputação para cada atacante monitorado.

29.1.46. Da Pesquisa em Fontes Abertas

29.1.46.1. Será aceita solução no formato de módulo integrado ou solução separada de pesquisa em fontes abertas. Em ambos os cenários, deverá ser ofertado como parte do item 6 e deve possuir as características a seguir:

a) Deve permitir criar filtros para monitorar, por exemplo: Desastres naturais, eventos de violência e situações de crise;

b) Cada unidade de licenciamento deve ser para, pelo menos, 5 usuários da solução;

c) Deve possuir, no mínimo, 45 redes abertas como base de pesquisa, sendo, no mínimo:

• Tencent QQ;

• Reddit;

• Youtube;

• Raddle;

• Flickr;

• Defence Hub;

• Pastebin;

• TikTok;

• Pinterest;

• Discord;

• Tumblr;

• Vimeo;

• Telegram;

• Zeronet;

• Internet Relay Chat;

• Nairaland;

• MeWE;

• Instagram; X (Twitter);

• Mastodon;

• QQ;

• Element;

• 4chan.

d) Deve possuir um Dashboard intuitivo, com gráficos representando os resultados das pesquisas em cada fonte de dados, tipos de mídia e localização geográfica. Deve possuir:

• Top Autores;

• Hashtags mais utilizadas.

e) Deve ser capaz de interpretar mais de 20 línguas, entre elas: Russo, Chinês, Francês, Farsi e Coreano; Deve permitir a criação de filtros de pesquisa. Deve permitir filtrar, no mínimo, por:

• Palavras chaves;

• Booleano;

• Postagem de imagem e vídeo;

• Fonte de dados;

• Data;

• Localização;

• Autor do post.

f) Deve possuir inteligência artificial para realizar análise do resultado da busca realizada. A IA deve realizar, no mínimo:

• Resumo dos resultados;

• Visão positiva dos resultados;

• Visão negativa dos resultados.

g) Deve permitir salvar uma pesquisa, com possibilidade de criação de alertas para cada pesquisa salva;

• Deve permitir enviar alerta por email;

• Deve permitir criar intervalos de alerta, com opção de 1 minuto, 30 minutos e 60 minutos;

• Qualquer pesquisa salva, deve permanecer ativa por, no mínimo, 60 dias;

h) Deve possuir Inteligência Artificial / Aprendizado de máquina para classificar de forma automática as postagens encontradas. Dentre as categorias, deve existir, pelo menos:

• Vazamento de Dados;

• Ameaça;

• Ódio;

i) Para criação de contexto, resposta emergencial e monitoramento de eventos, deve possuir funcionalidade geoespacial;

• Deve permitir desenhar “muros virtuais” em tempo real;

• Deve permitir a pesquisa por localização.

j) Deve possuir tradutor embarcado na solução.

29.2. Do Appliance

29.2.1. Deverá ser ofertado com equipamento dedicado para a análise, detecção e atuação em ataques cibernéticos. Deverá ser do tipo appliance físico, não sendo aceitos equipamentos genéricos, como servidores de rede, os quais são vulneráveis a ataques.

29.2.2. O appliance fornecido deverá suportar, no mínimo, 5Gbps de throughput.

29.2.3. O appliance fornecido deverá suportar a análise de, no mínimo, 400.000 conexões por minuto.

29.2.4. O appliance fornecido não deverá ultrapassar o formato de tamanho de 3U montável em rack 19´ padrão.

29.2.5. O appliance fornecido deve possuir no mínimo as interfaces físicas:

29.2.5.1. 02 (duas) interfaces padrão 10 GBASE-T para atuarem como Interfaces de cobre para análise do tráfego;

29.2.5.2. 08 (oito) interfaces padrão 1/10 Gbe SFP+ para atuarem como portas de análise SFP+;

29.2.5.3. 01 (uma) interface padrão 10/100/1000 BASE-T para atuar como interface de administração;

29.2.5.4. 01 (uma) interface padrão 10/100/1000 BASE-T para atuar como interface de gerenciamento remoto.

29.2.6. O hardware fornecido deverá possuir fonte de alimentação redundante.

29.2.7. Para a solução de análise do Microsoft 365, poderá ser:

29.2.7.1. Integrada ao appliance ofertado;

29.2.7.2. Entrega de outro appliance, físico ou virtual. Em caso de appliance virtual, deverá ser acompanhado do hardware necessário;

29.2.7.3. No formato SaaS – Software como serviço.

29.2.8. Para a solução de monitoramento Dark/Deep Web, poderá ser:

29.2.8.1. Integrada ao appliance ofertado;

29.2.8.2. Entrega de outro appliance, físico ou virtual. Em caso de appliance virtual, deverá ser acompanhado do hardware necessário;

29.2.8.3. No formato SaaS – Software como serviço.

29.3. ITEM 6 - Serviço em caráter 24x7

29.3.1. Os serviços deverão ser prestados pela CONTRATADA, em regime 24x7x365, que deverá atender os seguintes requisitos mínimos:

29.3.2. A CONTRATADA deverá informar, em tempo real, incidente críticos através da solução de comunicação atual, Microsoft TEAMS.

29.3.3. A CONTRATANTE poderá solicitar mais informações sobre os incidentes detectados através de Microsoft TEAMS, Portal de Atendimento, e-mail e/ou por telefone, conforme previamente acordado com a CONTRATADA na fase de Planejamento e Projeto.

29.3.4. As solicitações de serviços e as notificações de incidentes de segurança cibernética reportadas pela solução proposta ou pela CONTRATANTE deverão ser registradas.

29.3.5. Em caso de incidentes, a CONTRATADA deverá prover relatórios com trilhas de auditoria.

29.3.6. Receber e fazer a triagem de chamados de segurança cibernética;

29.3.7. Fazer primeiro atendimento de reportes de incidentes de segurança cibernética;

29.3.8. Elaborar consultas(queries)/scripts de rastreamento quando necessário e/ou solicitados pela CONTRATANTE;

29.3.9. Elaborar manual de usuário das atividades que se fizerem necessários e/ou solicitados pela CONTRATANTE;

29.3.10. Fazer passagem de turno, acompanhar os incidentes e realizar “follow-ups”, de modo que haja acompanhamento integral dos tickets abertos

29.3.11. Prestar suporte/apoio ao processo de automação das atividades relacionadas à resposta e tratamento de incidentes cibernéticos

29.3.12. Liberação de acesso à solução para usuários autorizados pela CONTRATANTE

29.3.13. Geração de indicadores de performance (KPI) definidos neste documento e acordados na fase de Planejamento e Projeto;

29.3.14. Atualização da solução, quando necessário/aplicável e/ou solicitados pela CONTRATANTE

29.3.15. Resolução de chamados de suporte junto ao(s) fabricante(s) da solução

29.3.16. A equipe da CONTRATADA deve atuar no monitoramento dos incidentes detectados pela solução e serviços propostos, sendo responsável por:

29.3.16.1. Analisar os incidentes recebidos da CONTRATANTE.

29.3.16.2. Comunicar, à equipe de segurança cibernética da CONTRATANTE, em caso de verificação de incidente de forma pró-ativa.

29.3.16.3. Emitir relatórios mensais, provendo, no mínimo, as seguintes informações à CONTRATANTE:

a) Alertas e notificações;

b) Quantidade de incidentes tratados/fechados;

c) Quantidade de incidentes registrados.

29.3.16.4. Relativo ao monitoramento de Deep/Dark Web, a CONTRATADA deverá prover, no mínimo, os seguintes serviços:

a) Monitoramento e envio de notificações para a equipe técnica da CONTRATANTE contendo os alertas críticos identificados no regime 24x7 (vinte e quatro horas por dia, sete dias por semana);

b) Envio de um relatório ao fim do mês à CONTRATANTE contendo, no mínimo, as informações a seguir:

• Vazamento de dados da CONTRATANTE que foram encontrados na Deep/Dark Web, através do monitoramento de domínios, IPs e e-mails.

• Descrição detalhada dos alertas.

29.4. ITEM 7 – SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO

29.4.1. A fase de ativação dos serviços deverá ser conduzida e concluída nos primeiros 60 (sessenta) dias corridos contados a partir da assinatura do contrato, quando serão executados o planejamento para implantação das ferramentas.

29.4.2. A CONTRATADA deve realizar o planejamento, a implantação, configuração e ativação dos serviços e soluções propostas no prazo de até 60 (sessenta) dias

corridos, contados a partir da entrega do appliance, conforme objetivos, escopo, requisitos, premissas e demais condições elencadas nesta especificação.

29.4.3. Os papéis e responsabilidades das partes nos processos de gestão de segurança cibernética, bem como indicadores necessários para medir e melhorá-los continuamente, serão definidos também com base nos referidos parâmetros (baseline).

29.4.4. As atividades de implantação e ativação do contrato poderão ocorrer de forma remota e deverão contemplar, no mínimo, as seguintes fases:

29.4.4.1. Planejamento e Projeto;

29.4.4.2. Reunião de kick-off;

29.4.4.3. Coleta de dados e requisitos complementares;

29.4.4.4. Detalhamento de cronograma;

29.4.4.5. Implantação, Configuração e Ativação da solução:

a) Instalação e ativação da solução on-line e console de gerência;

b) Instalação e ativação dos agentes, coletores, console de gerência e demais componentes da solução (pertinentes aos ativos monitorados) no ambiente computacional da CONTRATANTE: servidores, estações de trabalho, firewalls, servidores de diretório e cloud;

29.4.4.6. Instalação e ativação dos coletores de logs e dos coletores de tráfego de rede;

29.4.4.7. Configuração e o correto funcionamento da coleta, processamento e correlação de logs de eventos.

29.4.4.8. Testes e homologação.

29.4.4.9. Definição de Processos e Outras Configurações.

29.4.5. Transferência de conhecimento do formato Hands-On, com pelo menos 12 horas, para Operação, Sustentação e Melhoria Contínua.

29.5. DAS CONDIÇÕES GERAIS DE CESSÃO DE APPLIANCE

29.5.1. Por se tratar de um contrato de serviço, todos os appliances locais deverão ser alocados no formato COMODATO.

29.5.2. A CONTRATADA deverá garantir ao CONTRATANTE, a disponibilização dos componentes de hardwares da Plataforma de Segurança e Defesa Cibernética (leia-se equipamentos), em regime de “COMODATO” durante toda a vigência contratual do Objeto desta Licitação, bem como, cessão das licenças de uso de softwares e demais funcionalidades descritas com base nas demais condições do Termo de Referência e instrumento contratual celebrado entre as partes, e ainda:

29.5.3. Os equipamentos deverão entregues, em regime de comodato pela CONTRATADA ao CONTRATANTE, em local a ser indicado e disponibilizado pela equipe técnica designada, local o qual, onde estes também deverão ser devolvidos, ao fim do prazo de vigência contratual, ou quando, instrumento contratual celebrado entre as partes assim for encerrado;

29.5.4. No ato da entrega e devolução desses e equipamentos, as partes se obrigam a vistoriar os mesmos, e apontar eventuais desconformidades, ressalvadas aquelas que só possam ser detectadas com os equipamentos em funcionamento, de forma que irão gerar um “Laudo de Vistoria de Entrega e de Devolução” dos mesmos, e que compreenderá o presente instrumento contratual celebrado entre as partes, e para todos os fins (entrega e devolução);

29.5.5. Caso na devolução dos equipamentos seja constatada a ausência de quaisquer acessórios, ou observado dano físico junto aos mesmos, o CONTRATANTE se compromete a ressarcir os componentes ou danos, mediante apresentação orçamento e laudo técnico formal, ambos fornecidos pela CONTRATADA;

29.5.6. Os custos decorrentes da entrega e devolução dos equipamentos ficarão às expensas da CONTRATADA;

29.5.7. A CONTRATADA e CONTRATANTE se obrigam a emitir toda a documentação fiscal hábil relativa ao regime de “COMODATO”, para comprovação e execução instrumento contratual celebrado entre as partes.

29.5.8. Requisitos de Suporte Técnico e Garantia

29.5.8.1. A CONTRATADA deverá prover canais de acesso (telefone, aplicativo de mensagens, endereço eletrônico, site), para fins de acionamento de suporte técnico e garantia, objetivando a resolução de problemas técnicos e dúvidas quanto ao funcionamento ou disponibilizaçaõ dos recursos da solução.

29.5.8.2. Todos os chamados, independentemente de sua criticidade, deverão ser abertos em um único número telefônico e cada chamado técnico deverá receber um número único de identificação por parte da fabricante, e deverá registrar ao menos as seguintes informações:

a) Data e hora da abertura do chamado;

b) Responsável pelo chamado no canal de atendimento;

c) Descrição do problema;

d) Histórico de atendimento;

e) Data e hora do encerramento.

29.5.8.3. O chamado técnico para as subscrições de software objeto deste Termo de Referência será classificado de acordo com a severidade do problema, da seguinte forma:

29.5.8.4. SEVERIDADE 01: Incidente de erro ou falha que torne indisponível o acesso aos serviços, internet ou da plataforma.

a) Início do atendimento: até 02 (duas) horas após abertura do chamado.

b) Medidas Preliminares: até 08 (oito) horas após início do atendimento.

c) Prazo máximo de solução: até 24 (vinte e quatro) horas após sua abertura.

29.5.8.5. SEVERIDADE 02: Incidente detectado que cause falhas de funcionamento, operação, acesso, mas que não cause indisponbilidade total dos recursos.

a) Início do atendimento: até 04 (quatro) horas após abertura do chamado.

b) Medidas Preliminares: até 08 (oito) horas após início do atendimento.

c) Prazo máximo de solução: até 48 (quarenta e oito) horas após sua abertura.

29.5.8.6. SEVERIDADE 03: Dúvidas relativas à operação ou configuração da solução.

a) Início do atendimento: até 08 (oito) horas após abertura do chamado.

b) Medidas Preliminares: até 12 (doze) horas após início do atendimento.

c) Prazo máximo de solução: até 72 (setenta e duas) horas após sua abertura.

29.5.8.7. O chamado será considerado resolvido quando o problema for solucionado ou quando forem aplicados os melhores esforços da CONTRATADA para solucionar o problema ou apresentar solução de contorno que restaure o funcionamento dos serviços afetados dentro do prazo definido.

29.5.8.8. O início da contagem dos prazos de atendimento de suporte (para efeito de ANS) se dará a partir da data e hora de abertura do chamado pelos canais de atendimento disponibilizados pela CONTRATADA.

29.5.8.9. O nível de severidade dos chamados será informado no momento de abertura. Desde que previamente autorizado pelo DETRAN/DF, o nível de um chamado poderá ser alterado para nível inferior ao informado na abertura. Nesse caso, será iniciada nova contagem de prazo, conforme o novo nível estabelecido, e os prazos serão iniciados a contar do evento da reclassificação.

29.5.8.10. Os profissionais de atendimento deverão estar capacitados para responder às solicitações dos usuários esclarecendo dúvidas sobre características e funcionalidades da solução.

29.5.8.11. Após o diagnóstico, o analista responsável pelo atendimento deverá entrar em contato com o usuário informando a(s) solução(ões) encontrada(s) ou auxiliando-o a resolver o problema por telefone ou e-mail, desde que a solicitação esteja no escopo de atendimento.

29.5.8.12. O prazo citado acima poderá ser prorrogado a critério da CONTRATANTE desde que solicitado pela CONTRATADA com os devidos motivos justificados e aceitos pela CONTRATANTE.

29.5.8.13. Informar ao CONTRATANTE, sempre que a solução de contorno ou definitiva de um Incidente esteja dependendo do fornecimento de algum insumo que não seja responsabilidade exclusiva da CONTRATADA, como por exemplo: Serviços de fornecedores externos, fornecimento de equipamentos de hardware, fornecimento de software, fornecimento de energia elétrica a fim de se resguardar contra eventuais quebras do Acordo de Nível de Serviço.

29.5.8.14. A CONTRATADA manterá cadastro das pessoas indicadas pela contratante para abertura e autorização de fechamento de chamado. Cada pessoa cadastrada deverá receber identificação e senha que permitam acesso seguro ao sistema, de maneira a evitar uso indevido por pessoa não autorizada.

30. ANEXO II - MODELO DE PROPOSTA DE PREÇOS

Ao DETRAN/DF

Pregão Eletrônico nº /2025.

Apresentamos nossa proposta para XX, durante o período de XX (xxx) meses:

DADOS DA EMPRESA

Razão Social:

CNPJ (MF) nº:

Endereço:

Cidade: UF:

CEP:

Telefone:

Endereço Eletrônico:

DADOS BANCÁRIOS BANCO:

AGÊNCIA:

CONTA:

Dados do Representante para fim de apresentação da proposta e assinatura do contrato: Nome:

CPF: Cargo/Função:

Carteira de Identidade: Expedido por: Endereço Eletrônico:

ITEM	ESPECIFICAÇÃO	CATSER	QUANTIDADE ESTIMADA	UNIDADE	VALOR UNITÁRIO ESTIMADO	VALOR TOTAL ESTIMADO
1						
2						
3						
4						

Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na prestação do serviço, apurados mediante o preenchimento do modelo de acima.

Nos propomos a fornecer os serviços de acordo com as especificações concordando com o prazo de pagamento e demais condições estabelecidas no Edital e seus anexos. Informamos que o prazo de validade de nossa PROPOSTA DE PREÇOS é de ( ) dias, a contar da data de abertura da licitação (o prazo não poderá ser inferior a 60 dias).

31. ANEXO III - TERMO DE CONFIDENCIALIDADE CORPORATIVO

TERMO DE CONFIDENCIALIDADE CORPORATIVO

CLÁUSULA PRIMEIRA – DO OBJETO

O objeto deste termo é a proteção das INFORMAÇÕES CONFIDENCIAIS disponibilizadas pela Departamento de Trânsito do Distrito Federal, em razão do contrato celebrado entre as partes.

CLÁUSULA SEGUNDA – DAS DEFINIÇÕES

Todas as informações técnicas obtidas através da execução do contrato celebrado entre a Departamento de Trânsito do Distrito Federal do Distrito Federal e a empresa contratada serão tidas como confidenciais.

PARÁGRAFO ÚNICO: Serão consideradas confidenciais, para efeito deste Termo, toda e qualquer informação disponibilizada pela Departamento de Trânsito do Distrito Federal do Distrito Federal que, ainda que não estejam acobertadas pelo sigilo legal.

CLÁUSULA TERCEIRA - DA RESPONSABILIDADE

Os empregados da Empresa Contratada se comprometem a manter sigilo, não utilizando tais informações confidenciais em proveito próprio ou alheio. Os empregados que detiverem os dados confidenciais incorrem nos mesmos deveres dos servidores públicos conforme estabelece o art. 327 do Código Penal.

PARÁGRAFO PRIMEIRO: A Empresa Contratada deverá fornecer Termo de Confidencialidade dos funcionários que prestarão serviço à Departamento de Trânsito do Distrito Federal do Distrito Federal, bem como atualizá-lo em caso de dispensa e nova contratação.

PARÁGRAFO SEGUNDO: A Departamento de Trânsito do Distrito Federal do Distrito Federal poderá exigir Termos de Confidencialidade individuais quando entender necessário.

CLÁUSULA QUARTA – DA GUARDA DAS INFORMAÇÕES

O dever de confidencialidade e sigilo previsto neste termo terá validade durante toda a vigência da execução contratual. A custódia das informações deverá obedecer aos padrões de segurança contratualmente estipulados.

CLÁUSULA QUINTA – DAS OBRIGAÇÕES

A contratada se obriga a:

Cumprir as disposições da Política de Segurança da Informação desta instituição; Usar tais informações apenas com o propósito de bem e fiel cumprir o objeto contratado; Manter o sigilo relativo às informações confidenciais e revelá-las apenas aos empregados cadastrados que tiverem necessidade de ter conhecimento sobre elas; Manter procedimentos administrativos adequados à prevenção de extravio ou perda de quaisquer documentos ou informações confidenciais, devendo comunicar à Contratante, imediatamente, a ocorrência de incidentes desta natureza, o que não excluirá sua responsabilidade.

PARÁGRAFO PRIMEIRO: A quebra do dever de sigilo e a violação das obrigações deste Termo sujeitarão o responsável à pena prevista no artigo 325 do Código Penal.

PARÁGRAFO SEGUNDO: Os funcionários da contratada deverão destruir todos e quaisquer documentos por eles produzidos que contenham informações confidenciais

quando não mais for necessária a manutenção desses, comprometendo-se a não reter quaisquer reproduções, sob pena de incorrer nas responsabilidades previstas neste instrumento.

CLÁUSULA SEXTA - DAS DISPOSIÇÕES ESPECIAIS

Ao assinar o presente instrumento, a Empresa Contratada manifesta sua concordância no seguinte sentido:

Todas as condições, termos e obrigações, ora constituídas, serão regidas pelo presente Termo, bem como pela legislação e regulamentação brasileiras pertinentes; O presente Termo só poderá ser alterado mediante a celebração de novo termo, posterior e aditivo; As alterações do número, natureza e quantidade das informações confidenciais disponibilizadas pela Contratada não descaracterizarão ou reduzirão o compromisso ou as obrigações pactuadas neste Termo de Confidencialidade, que permanecerá válido e com todos os seus efeitos legais em qualquer das situações tipificadas neste instrumento; O acréscimo, complementação, substituição ou esclarecimento de qualquer das informações confidenciais conhecidas pelo funcionário, serão incorporadas a este Termo, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, não sendo necessária, nessas hipóteses, a assinatura ou formalização de Termo de Confidencialidade aditivo.

CLÁUSULA SÉTIMA – DA VALIDADE

Este Termo tornar-se-á válido a partir da data de sua efetiva assinatura pelas partes, mantendo-se esse compromisso, inclusive, após o término da contratação. CLÁUSULA OITAVA – DA RESPONSABILIDADE CIVIL

A não-observância de quaisquer das disposições estabelecidas neste instrumento, sujeitará a Empresa Contratada, por ação ou omissão de qualquer de seus agentes, ao pagamento ou recomposição de todas as perdas e danos comprovados pela Departamento de Trânsito do Distrito Federal do Distrito Federal.

Nome e Assinatura do Responsável pela CONTRATADA CNPJ CONTRATADA

32. ANEXO IV - MODELO DE TERMO DE CIÊNCIA

Contrato N°:			
Objeto:			
Contratante:			
Gestor do Contrato:		Matr.:	
Contratado:		CNPJ:	
Preposto da Contratada:		CPF:	

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

_____,_____ de _____ de 20_____.

Ciência

CONTRATADO	
Funcionários	
_____ <Nome> Matrícula: <Matr.>	_____ <Nome> Matrícula: <Matr.>
_____ <Nome> Matrícula: <Matr.>	_____ <Nome> Matrícula: <Matr.>
_____ <Nome> Matrícula: <Matr.>	_____ <Nome> Matrícula: <Matr.>

Documento assinado eletronicamente por **AUGUSTO HENRIQUE PARENTE FARIAS - Matr.1726729-3**, **Assessor(a) Especial**, em 22/09/2026, às 16:47, conforme art. 6º do Decreto n° 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 **CELSO HENRIQUE SANCHES MEDEIROS - Matr.1727015-4**, **Coordenador(a) de Gestão de Suporte e Segurança de Infraestrutura**, em 24/09/2026, às 15:03, conforme art. 6º do Decreto n° 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 **FABIO FONTES BORGES - Matr.0256790-3**, **Gerente de Segurança de Infraestrutura**, em 24/09/2026, às 16:54, conforme art. 6º do Decreto n° 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 **WALDIR DA SILVA FERREIRA JÚNIOR - Matr.0256634-6**, **Diretor(a) de Tecnologia da Informação e Comunicação**, em 24/09/2026, às 16:55, conforme art. 6º do Decreto n° 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: https://sei.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 Código Verificador: **215045611** Código CRC: **C2371DEA**.