



TERMO DE REFERÊNCIA

Contratação do licenciamento da solução corporativa Bitdefender GravityZone Business Security Enterprise com console centralizada em nuvem (Cloud Console)

A Prefeitura Municipal de Cabo Frio, RJ torna público, por meio deste Termo de Referência, a abertura de processo administrativo para **contratação do licenciamento da solução corporativa de segurança digital já implantada no ambiente institucional**, incluindo licenciamento, atualização de versões, suporte técnico e garantia de funcionamento durante toda a vigência contratual, destinada à proteção dos ativos de tecnologia da informação da Administração Municipal.

A solução deverá contemplar recursos de prevenção, detecção e resposta a ameaças cibernéticas, com gerenciamento centralizado, proteção de estações de trabalho, servidores e demais dispositivos integrantes da infraestrutura tecnológica municipal, conforme especificações técnicas, requisitos operacionais e níveis de serviço estabelecidos neste Termo de Referência (TR), observadas as diretrizes de segurança da informação e continuidade dos serviços públicos digitais.

1. INTRODUÇÃO

A Administração Pública Municipal vem ampliando de forma progressiva a utilização de sistemas informatizados estruturantes voltados à gestão tributária, contábil, administrativa e de atendimento ao cidadão, o que exige a adoção de mecanismos eficazes de proteção dos ativos tecnológicos e das informações institucionais sob sua responsabilidade.

Nesse contexto, a segurança da informação constitui requisito essencial para garantir a continuidade dos serviços públicos digitais, a integridade das bases de dados corporativas (ainda que hospedadas em datacenters externos), a proteção das informações sensíveis tratadas pela Administração Municipal e a mitigação de riscos operacionais relacionados a incidentes cibernéticos, tais como infecções por malware, ataques de ransomware, acessos indevidos e indisponibilidade de sistemas críticos.

A inexistência ou insuficiência de solução corporativa de proteção de endpoints com gerenciamento centralizado pode comprometer diretamente a disponibilidade dos serviços públicos, gerar riscos à integridade das informações institucionais e ocasionar prejuízos operacionais e administrativos relevantes, inclusive com potencial impacto na arrecadação municipal e na prestação de serviços essenciais ao cidadão.

Dessa forma, a contratação de solução corporativa de antivírus com gerenciamento centralizado mostra-se necessária para assegurar níveis adequados de proteção do ambiente computacional da Prefeitura Municipal de Cabo Frio, permitindo a prevenção, detecção e resposta a ameaças digitais, bem como o monitoramento contínuo dos dispositivos conectados à rede institucional, em conformidade com as boas práticas de governança de tecnologia da informação e segurança cibernética.

A presente contratação encontra fundamento no art. 75, inciso II, da Lei nº 14.133/2021, considerando tratar-se de solução padronizada de mercado, amplamente utilizada na Administração Pública, cujo valor estimado se enquadra nos limites legais para contratação direta por dispensa de licitação, observados os princípios da economicidade,



eficiência, planejamento, motivação administrativa e seleção da proposta mais vantajosa para a Administração Pública.

Adicionalmente, a adoção da solução pretendida contribui para o atendimento às diretrizes da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD), especialmente no que se refere à proteção de dados pessoais tratados pela Administração Municipal, bem como ao fortalecimento da governança de TIC (tecnologia da informação e comunicação) e da continuidade dos serviços públicos digitais ofertados ao cidadão.

Registra-se ainda que a contratação está alinhada às necessidades institucionais previamente identificadas pela área técnica responsável pela infraestrutura tecnológica da secretaria de fazenda do Município, integrando as ações de mitigação de riscos operacionais e de fortalecimento da segurança do ambiente computacional municipal, atendendo às recomendações dos órgãos de controle quanto à formalização do planejamento das contratações públicas de tecnologia da informação.

Diante desse cenário, justifica-se a realização da presente contratação por dispensa de licitação, com fundamento no art. 75 da Lei nº 14.133/2021, visando garantir a proteção dos ativos tecnológicos municipais e assegurar a continuidade e confiabilidade dos serviços públicos digitais prestados pela Prefeitura Municipal de Cabo Frio e mais especificamente pela secretaria de fazenda.

2. ÓRGÃO SOLICITANTE

A presente contratação foi demandada pela **Secretaria Municipal de Fazenda**, unidade administrativa responsável pela gestão e operação do ambiente computacional institucional no qual se encontra implantada a solução corporativa de segurança digital objeto deste Termo de Referência.

3. OBJETO DA CONTRATAÇÃO

Constitui objeto da presente contratação, por dispensa de licitação, a contratação da solução corporativa de proteção de endpoints já implantada no ambiente institucional, visando a necessidade operacional, atualmente baseada na solução Bitdefender GravityZone, com console de gerenciamento centralizado em nuvem (Cloud Console), disponibilizada no modelo Software como Serviço (SaaS), incluindo atualização automática de assinaturas, gerenciamento remoto dos endpoints protegidos, suporte técnico especializado e direito às atualizações oficiais do fabricante pelo período de 36 (trinta e seis) meses, ou solução equivalente ou superior, desde que atendidos os requisitos técnicos estabelecidos neste Termo de Referência.

A solução destina-se à proteção das estações de trabalho e servidores que compõem o ambiente computacional da Secretaria Municipal de Fazenda de Cabo Frio/RJ, abrangendo funcionalidades de prevenção, detecção e resposta a ameaças cibernéticas, com administração centralizada e aplicação uniforme das políticas institucionais de segurança da informação.

A contratação contempla o fornecimento das seguintes licenças:



Item	Unid.	Quant.	Descrição
1	Unidade	136	Contratação do licenciamento de uso da solução corporativa de proteção de endpoints Bitdefender GravityZone Business Security Enterprise, com console de gerenciamento centralizado em nuvem (Cloud Console), disponibilizada no modelo Software como Serviço (SaaS), incluindo atualização automática de assinaturas, gerenciamento remoto dos endpoints protegidos, suporte técnico especializado e direito às atualizações oficiais do fabricante pelo período de 36 (trinta e seis) meses para estações de trabalho.
2	Unidade	20	Contratação do licenciamento de uso da solução corporativa de proteção de endpoints Bitdefender GravityZone Business Security Enterprise, com console de gerenciamento centralizado em nuvem (Cloud Console), disponibilizada no modelo Software como Serviço (SaaS), incluindo atualização automática de assinaturas, gerenciamento remoto dos endpoints protegidos, suporte técnico especializado e direito às atualizações oficiais do fabricante pelo período de 36 (trinta e seis) meses para servidores.

A Solução Bitdefender GravityZone encontra-se previamente implantada no ambiente tecnológico da Secretaria Municipal de Fazenda, integrando o modelo operacional de proteção de endpoints atualmente utilizado pela equipe técnica do setor de Tecnologia da Informação e Comunicação (TIC).

Nesse contexto, a contratação fundamenta-se na necessidade de manutenção da padronização tecnológica existente, conforme admitido pela legislação vigente, considerando que eventual substituição da solução implicaria:

- necessidade de reestruturação do ambiente institucional de segurança digital;
- migração das políticas de proteção, monitoramento e resposta a incidentes já consolidadas;
- reconfiguração integral da console de gerenciamento centralizado da solução;
- geração de custos indiretos associados ao processo de transição tecnológica;
- exposição do ambiente computacional a riscos operacionais durante o período de substituição da solução;
- potencial impacto sobre a integridade, disponibilidade e confidencialidade de dados fiscais, contábeis e demais informações sensíveis sob responsabilidade da Secretaria Municipal de Fazenda;
- possibilidade de ocorrência de vulnerabilidades temporárias decorrentes do período de adaptação operacional à nova solução eventualmente adotada;
- necessidade de capacitação adicional e retreinamento da equipe técnica de tecnologia da informação, com reflexos na eficiência operacional e na continuidade das rotinas institucionais de segurança da informação.

A adoção da solução contratada mantém compatibilidade integral com a infraestrutura tecnológica existente, preservando os procedimentos operacionais já



consolidados pela equipe técnica e garantindo a continuidade da proteção ativa contra malwares, ransomwares, exploits, scripts maliciosos e demais ameaças cibernéticas.

A presente contratação encontra respaldo no princípio da padronização administrativa e da continuidade do serviço público, previstos na Lei nº 14.133/2021, especialmente quando demonstrada a vantagem técnica e operacional da manutenção da solução já implantada, conforme evidenciado no respectivo Estudo Técnico Preliminar (ETP).

A solução destina-se à proteção dos ativos digitais que suportam sistemas estruturantes da Secretaria Municipal de Fazenda, especialmente aqueles relacionados à arrecadação tributária, execução orçamentária, gestão contábil e tratamento de informações sensíveis da Administração Pública Municipal, caracterizando-se como serviço essencial à segurança da informação institucional e à continuidade administrativa.

4. DEFINIÇÃO DA TERMINOLOGIA DO OBJETO

Para fins deste Termo de Referência, a solução **Bitdefender GravityZone Business Security Enterprise**, com console de gerenciamento centralizado em nuvem (Cloud Console), disponibilizada no modelo Software como Serviço (SaaS), incluindo atualização automática de assinaturas, gerenciamento remoto, suporte técnico especializado e direito às atualizações oficiais do fabricante, será doravante denominada simplesmente “**Solução Bitdefender GravityZone**”.

Sempre que mencionada ao longo deste documento, a expressão **Solução Bitdefender GravityZone** refere-se integralmente ao conjunto de funcionalidades e serviços descritos no objeto da contratação.

5. DA JUSTIFICATIVA DA CONTRATAÇÃO

A presente contratação caracteriza-se como continuidade de solução tecnológica já implantada, sendo necessária para evitar descontinuidade operacional, riscos à segurança da informação e custos associados à eventual substituição da plataforma atualmente utilizada.

Importante destacar que a contratação tem por finalidade assegurar a continuidade da proteção dos ativos de tecnologia da informação da Secretaria Municipal de Fazenda do Município de Cabo Frio, por meio da Contratação do licenciamento da solução atualmente implantada no ambiente computacional institucional há aproximadamente 48 (quarenta e oito) meses, com histórico comprovado de estabilidade operacional, efetividade técnica e ausência de incidentes relevantes de segurança com impacto institucional.

A solução encontra-se implantada em aproximadamente 110 estações de trabalho e 20 servidores institucionais, abrangendo integralmente o ambiente fazendário municipal, o



que evidencia sua criticidade operacional e o grau de dependência tecnológica da infraestrutura institucional em relação à ferramenta.

A presente contratação caracteriza-se como Contratação de licenciamento previamente implantado, cuja manutenção demonstra-se tecnicamente adequada, economicamente vantajosa e administrativamente recomendável, considerando:

- inexistência de descontinuidade operacional;
- inexistência de custos de migração tecnológica;
- domínio técnico da equipe interna sobre a solução;
- compatibilidade integral com a infraestrutura existente;
- preservação do padrão tecnológico institucional de segurança digital.

Tal medida encontra respaldo nos princípios do planejamento das contratações públicas, eficiência administrativa, continuidade do serviço público e padronização tecnológica, previstos nos arts. 11, 18 e 5º da Lei nº 14.133/2021.

5.1 Continuidade operacional e mitigação de riscos tecnológicos

A solução encontra-se plenamente integrada ao modelo institucional de segurança da informação, constituindo ferramenta essencial à proteção:

- das estações de trabalho;
- dos servidores físicos e virtuais;
- dos dispositivos conectados à rede institucional;
- dos sistemas fazendários estruturantes;
- das bases de dados fiscais, contábeis e financeiras.

A eventual substituição da solução atualmente implantada implicaria riscos técnicos e operacionais relevantes, tais como:

- desinstalação e reinstalação da solução em todos os endpoints institucionais;
- reconstrução integral das políticas de segurança digital;
- reconfiguração de regras de proteção e exceções operacionais;
- revalidação de compatibilidade com sistemas fazendários críticos;
- reconfiguração das integrações com diretório corporativo e infraestrutura virtualizada;
- necessidade de capacitação técnica adicional da equipe interna;
- aumento temporário da superfície de risco cibernético durante a transição tecnológica.

Durante esse período de migração poderia ocorrer redução temporária da capacidade de detecção e resposta a ameaças, com potencial impacto na continuidade dos serviços públicos digitais essenciais.

Dessa forma, a manutenção da solução atualmente implantada representa medida tecnicamente prudente e alinhada ao princípio da continuidade administrativa previsto na Lei nº 14.133/2021.

5.2 Compatibilidade técnica com o ambiente institucional



A Solução Bitdefender GravityZone encontra-se plenamente compatível com a arquitetura tecnológica institucional, permitindo gerenciamento centralizado do ambiente por meio de console única integrada, contemplando:

- proteção antivírus e antimalware corporativo;
- EDR (Endpoint Detection and Response);
- firewall corporativo gerenciado;
- controle de dispositivos e aplicações;
- detecção comportamental baseada em machine learning;
- análise de arquivos suspeitos em sandbox segura;
- monitoramento contínuo de eventos de segurança;
- integração com ambientes virtualizados e sistemas operacionais corporativos Windows e Linux.

A adoção de solução distinta implicaria reconstrução integral da arquitetura de proteção digital institucional, com aumento de riscos operacionais e necessidade de esforço técnico adicional da equipe de TIC.

5.3 Vantajosidade econômica e racionalidade administrativa

Sob o aspecto econômico, a Contratação do licenciamento apresenta relação custo-benefício favorável à Administração Pública, considerando que:

- a solução encontra-se previamente implantada e operacional;
- não haverá custos de migração tecnológica;
- não haverá necessidade de reimplantação de agentes de segurança;
- não haverá necessidade de capacitação adicional da equipe técnica;
- não será necessário investimento complementar em infraestrutura;
- preserva-se o modelo institucional de segurança digital já consolidado.

A substituição da solução implicaria custos indiretos relevantes associados à transição tecnológica, incluindo retrabalho técnico, curva de aprendizagem da equipe, interrupções operacionais temporárias e aumento do risco institucional durante o período de estabilização da nova plataforma.

5.4 Adequação à Lei Geral de Proteção de Dados – LGPD

A manutenção da solução contribui diretamente para o atendimento das obrigações previstas na Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), especialmente no que se refere à adoção de medidas técnicas e administrativas aptas a proteger dados pessoais contra:

- acessos não autorizados;
- perda ou destruição acidental;
- alteração indevida;
- divulgação não autorizada;
- incidentes de segurança da informação.

Nesse contexto, a solução constitui camada essencial de proteção preventiva das bases de dados sob responsabilidade da Administração Fazendária Municipal.



5.5 Aderência às boas práticas de governança digital na Administração Pública

A Contratação do licenciamento encontra respaldo nas diretrizes nacionais de segurança da informação aplicáveis ao setor público, especialmente:

- Estratégia de Governo Digital;
- boas práticas de gestão de riscos cibernéticos;
- recomendações dos Tribunais de Contas quanto à continuidade tecnológica de soluções críticas;
- normas técnicas baseadas na ISO/IEC 27001 e ISO/IEC 27002.

A manutenção de solução corporativa consolidada contribui para o aumento da maturidade institucional em segurança da informação e para o fortalecimento da resiliência digital da Administração Pública.

5.6 Reconhecimento técnico e posicionamento da solução no mercado

A Solução Bitdefender GravityZone apresenta elevado grau de reconhecimento técnico em avaliações independentes internacionais conduzidas por instituições especializadas em segurança cibernética, destacando-se pela alta taxa de detecção de ameaças avançadas, baixa incidência de falsos positivos e desempenho consistente em ambientes corporativos heterogêneos.

Adicionalmente, apresenta compatibilidade com múltiplas plataformas operacionais, independência de ecossistemas proprietários específicos e arquitetura integrada de prevenção, detecção e resposta a incidentes, características especialmente relevantes para ambientes públicos com infraestrutura tecnológica diversificada.

5.7 Capacidade operacional da equipe interna

Registra-se ainda que a Secretaria Municipal de Fazenda dispõe de equipe reduzida de Tecnologia da Informação, composta por três profissionais responsáveis pela sustentação integral do ambiente computacional institucional, circunstância que reforça a vantagem administrativa da manutenção da solução atualmente implantada, evitando processos complexos de migração tecnológica que poderiam comprometer a continuidade dos serviços públicos digitais.

5.8 Conclusão

Diante da análise técnica, administrativa, econômica e jurídica apresentada, verifica-se que a Contratação do licenciamento da Solução Bitdefender GravityZone constitui medida plenamente alinhada ao interesse público, assegurando:

- continuidade da proteção cibernética institucional;
- estabilidade operacional dos serviços fazendários;
- preservação da integridade das informações públicas;
- mitigação de riscos operacionais;
- atendimento às exigências da Lei nº 14.133/2021;
- conformidade com a Lei Geral de Proteção de Dados.



Dessa forma, resta plenamente caracterizada a adequação técnica, jurídica e administrativa da contratação pretendida, demonstrando-se tratar da alternativa mais segura, eficiente e vantajosa para a Administração Pública Municipal.

6. MODALIDADE DE CONTRATAÇÃO

(Dispensa de Licitação – art. 75, inciso II, da Lei nº 14.133/2021)

A presente contratação tem por objeto a continuidade de solução de segurança da informação já implantada no ambiente institucional da Secretaria de Fazenda, caracterizando-se como contratação necessária à manutenção da operação regular de proteção dos ativos computacionais e dos serviços públicos digitais.

A contratação será realizada mediante **dispensa de licitação**, com fundamento no **art. 75, inciso II, da Lei nº 14.133/2021**, considerando que o valor estimado da despesa encontra-se dentro do limite legal estabelecido para contratações diretas por baixo valor.

Nos termos do art. 72 da Lei nº 14.133/2021, a instrução processual deve contemplar a adequada caracterização da necessidade administrativa, a estimativa da despesa e a realização de pesquisa de preços, a qual será oportunamente elaborada e juntada aos autos, bem como a demonstração da compatibilidade do valor da contratação com aqueles praticados no mercado, de modo a assegurar a regularidade da contratação direta pretendida.

A pesquisa de preços deverá, sempre que possível, basear-se em múltiplas fontes, tais como contratações similares realizadas por outros órgãos públicos, propostas de fornecedores, sítios eletrônicos especializados e bases de dados oficiais, buscando-se, preferencialmente, a obtenção de, no mínimo, três referências válidas e contemporâneas.

O valor estimado da contratação será apurado mediante metodologia adequada — média, mediana ou menor valor — precedida de análise crítica dos dados coletados, com a devida exclusão de preços inexequíveis, discrepantes ou inconsistentes, mediante justificativa fundamentada.

Por fim, a pesquisa de preços será formalizada nos autos com a devida memória de cálculo e a identificação das fontes consultadas, servindo como parâmetro para a aferição da compatibilidade da proposta com os preços de mercado, em conformidade com o disposto no art. 72 da Lei nº 14.133/2021.

Registra-se que a solução objeto da contratação é regularmente disponibilizada no mercado por meio de rede de revendedores autorizados, circunstância que permite a realização de pesquisa de preços e a seleção da proposta mais vantajosa para a Administração Pública, observados os princípios da economicidade e da eficiência administrativa.

Destaca-se, ainda, que a presente contratação não se fundamenta em hipótese de inexigibilidade, tampouco em inviabilidade de competição, mas exclusivamente no critério objetivo do valor estimado da contratação, conforme previsto no art. 75, inciso II, da Lei nº 14.133/2021.



Dessa forma, restam atendidos os pressupostos legais para a realização da contratação direta por dispensa de licitação, observadas as exigências previstas nos arts. 72 e 75 da Lei nº 14.133/2021, mostrando-se juridicamente adequada a adoção da modalidade pretendida.

7. MEMORIAL DESCRITIVO DA SOLUÇÃO

a. ESPECIFICAÇÕES PARA AS ESTAÇÕES DE TRABALHO E SERVIDORES FÍSICOS E VIRTUAIS

- i. A solução deverá operar com agente único integrado e console centralizada compatível com a arquitetura atualmente implantada no ambiente institucional, garantindo continuidade operacional sem necessidade de substituição de infraestrutura existente.
- ii. Possuir console central única de gerenciamento. As configurações do Antimalware (incluindo antivírus e antispyware), Firewall, Detecção de intrusão, controle de Dispositivos e Controle de Aplicações deverão ser realizadas através da mesma console;
- iii. O Produto deverá ter a capacidade de remoção do software de antivírus já instalado e ser instalado de forma remota pela console de gerenciamento;
- iv. O produto deverá possuir no mínimo os seguintes módulos:
 1. Console de Gerenciamento fornecendo funcionalidades de gestão;
 2. Módulos para estações físicas, laptops e servidores;
 3. Módulo para ambientes virtualizados, sendo criado especialmente para ambientes virtuais;
 4. Utilizar mecanismos de detecção heurística e comportamental baseados em análise estática e dinâmica;
- v. Oferecer tecnologia onde a solução explore vulnerabilidades de softwares instalados no intuito de reduzir o risco de infecções (anti-exploit);
- vi. Oferecer tecnologia nativa no intuito de eliminar ameaças do tipo Ransomware;
- vii. A solução deverá possuir recursos nativos de EDR (Endpoint Detection and Response), permitindo detecção, investigação e resposta a incidentes de segurança com visibilidade contextual de eventos, correlação automática de eventos de múltiplos endpoints e ações remotas de contenção diretamente pela console central.
- viii. Oferecer inventário de softwares;
- ix. Oferecer tecnologia de análise de arquivos potencialmente maliciosos em ambiente isolado (sandbox), hospedado em infraestrutura segura do fabricante ou ambiente equivalente oficialmente suportado;
- x. Oferecer proteção por base de assinaturas.
- xi. A solução deverá possuir arquitetura compatível com ambientes híbridos (físicos,



virtuais e em nuvem), garantindo escalabilidade, interoperabilidade com a infraestrutura existente e continuidade operacional durante toda a vigência contratual

B. INSTALAÇÃO E CONFIGURAÇÃO

- I. Deverá ser fornecido como appliance virtual local, executável para instalação em servidores Windows ou console em nuvem (SaaS) hospedada em infraestrutura segura do fabricante.
- II. Deverá suportar prioritariamente a plataforma Microsoft Hyper-V, considerando sua adoção predominante no ambiente institucional, bem como compatibilidade com as demais plataformas de virtualização corporativa descritas na seção "Requisitos mínimos suportados pelo sistema".
- III. Deverá ser fornecido com base de dados embutido na Console em Nuvem, sem a necessidade de baixar para máquina do administrador da Console;
- IV. Permitir instalação remota via console WEB de gerenciamento para ambientes virtualizados;
- V. O mecanismo de varredura deverá permitir distribuição otimizada via repositório local ou nuvem;
- VI. solução deverá permitir mecanismos de alta disponibilidade e continuidade operacional para ambientes com múltiplos servidores com funções equivalentes, quando suportado pela arquitetura da solução.
- VII. A console de gerenciamento deverá possuir interface administrativa disponível em idioma português.

C. CARACTERÍSTICA GERAIS

- I. Interface centralizada e simplificada para atualização dos componentes e serviços da solução
- II. Permitir que o administrador escolha qual o pacote será atualizado;
- III. As notificações devem ser destacadas como item não lida, enviar e-mail para o administrador;
- IV. No mínimo enviar notificações: Problemas com licenças, Alertas de Surto de vírus, Máquinas desatualizadas, Eventos de antimalware,
- V. Painel para Monitoramento baseado em "portlets" configuráveis com no mínimo as seguintes especificações: Nome; Tipo de relatório; Alvo do relatório;
- VI. Deverá disponibilizar "portlets" para qualquer serviço de segurança, máquinas físicas, virtuais, dispositivos móveis;
- VII. Disponibilizar painel centralizado de gerenciamento de incidentes de segurança com correlação automática de eventos e priorização de alertas.
- VIII. Permitir integração com soluções SIEM por meio de syslog, API ou mecanismos



equivalentes oficialmente suportados pelo fabricante.

- IX.** Disponibilizar API oficial documentada para integração com ferramentas corporativas de automação e orquestração de segurança.

D. INVENTÁRIO DA REDE

- I.** Possuir no mínimo as integrações abaixo:
- múltiplos domínios Active Directory
 - múltiplos servidores Microsoft Hyper-V
 - múltiplos VMware vCenters (quando existentes);
 - Múltiplos Citrix Xen Servers (quando existentes);
- II.** Possuir a possibilidade de definição de sincronização com o Active Directory em horas;
- III.** Deverá ser compatível com plataformas de virtualização corporativa descritas na seção “Requisitos mínimos suportados pelo sistema”;
- IV.** Descoberta de rede para máquinas em grupo de trabalho;
- V.** Possuir busca em tempo real pelo menos com os seguintes filtros: Nome, Sistema Operacional, Endereço IP;
- VI.** Possibilitar a instalação remota e desinstalação remota do antivírus;
- VII.** Possibilitar a configuração de pacotes de instalação do produto de antivírus;
- VIII.** Possuir tarefas remotas e configuráveis de Scan;
- IX.** Possuir tarefa de reinicialização remota de estação ou servidor;
- X.** Atribuir políticas para no mínimo os níveis: Computador, Máquina Virtual ou Possuir a propriedade detalhada de objetos gerenciados para: Nome, IP, Sistema Operacional, Grupo, Política aplicada, ultimo status de malware;
- XI.** Permitir consulta remota avançada em tempo real aos endpoints gerenciados para coleta de eventos, indicadores de segurança e informações do sistema operacional.
- XII.** Disponibilizar recursos de análise contínua de risco e redução da superfície de ataque (Attack Surface Reduction), incluindo identificação automática de vulnerabilidades, aplicações desatualizadas, configurações inseguras e recomendações de mitigação priorizadas;
- XIII.** Permitir execução de ações remotas investigativas nos endpoints, incluindo coleta de artefatos, execução de comandos administrativos autorizados e análise forense remota para resposta a incidentes de segurança.

E. POLÍTICAS

- I.** Modelo único para todos os equipamentos, seja físico ou virtual;



- II. Cada serviço de segurança deve ter seu modelo configurável de política com opções específicas de ativar/desativar;
- III. Deverá configurar as funcionalidades como escaneamento do Antivírus, firewall de duas vias de detecção de intrusão, controle de acesso a rede, controle de aplicação, controle de acesso web, autenticação e ações para serem aplicadas em caso de vírus e dispositivos em não conformidade;
- IV. Permitir categorização dinâmica de endpoints por meio de etiquetas (tags) para aplicação automatizada de políticas de segurança.

F. RELATÓRIOS

- I. Relatório para cada serviço de segurança;
- II. Facilidade de usar e visualização simplificada;
- III. Agendamento, com opção de envio por e-mail para qualquer destinatário conforme escolhido administrador;
- IV. Filtros de agendamento de relatórios;
- V. Arquivo com todas as instâncias de relatório agendados;
- VI. Exportar o relatório nos formatos .pdf e/ou .csv;
- VII. Oferecer possibilidade de criar relatórios de maneira dinâmica no painel administrativo da solução.
- VIII. Permitir visualização gráfica da cadeia de ataque (attack chain), incluindo origem, propagação e impacto do incidente de segurança.

G. QUARENTENA

- I. Restauração remota, com configuração de localidade e deleção;
- II. Criação e exclusão para arquivos restaurados;

H. USUÁRIOS

- I. Administração baseada em regras;
- II. Disponibilizar tipos de usuários pré-definidos como no mínimo: Administrador - Gerente dos componentes da solução, Administrador de rede - Gerente dos serviços de segurança;
- III. Relatório - Monitora e cria relatórios;
- IV. Deverá ser possível customizar um tipo de usuário;
- V. Deverá permitir a integração do usuário com o Active Directory para autenticação da console de gerenciamento;



- VI. Logs de utilização;
- VII. Registrar as ações do usuário na console de gerenciamento;
- VIII. Detalhar cada ação do usuário;
- IX. Permitir busca complexa baseada em ações do usuário, intervalos de tempo;

I. CERTIFICADO DE SEGURANÇA

- I. Deverá prover o acesso via HTTPS;
- II. Deverá permitir a importação de certificados digitais;
- III. O gerenciamento e a comunicação com dispositivos móveis deve ser feito de forma segura utilizando certificados digitais;

J. PROTEÇÃO PARA ESTAÇÕES DE TRABALHO E SERVIDORES FÍSICOS

- I. Deverá permitir a configuração do scan do antivírus do cliente como: Scan local, Scan Híbrido, Scan Central;
- II. Deverá permitir a instalação customizada do antivírus com no mínimo: instalar o antivírus sem o controle de acesso a internet, instalar o antivírus sem o módulo de firewall (caso desejável);
- III. Deverá suportar no mínimo os seguintes sistemas operacionais para estação de trabalho: Windows 10 32 e 64Bits ou superior;
- IV. Deverá suportar no mínimo os seguintes sistemas operacionais para servidores: Windows Server 2016 ou superior;
- V. A solução deverá possuir compatibilidade com sistemas operacionais da plataforma Linux em versões oficialmente suportadas pelos respectivos fabricantes durante toda a vigência contratual, incluindo, no mínimo:
 - Red Hat Enterprise Linux
 - Ubuntu LTS
 - SUSE Linux Enterprise Server
 - openSUSE
 - Fedora Linux
 - Debian
 - Admitindo-se ainda compatibilidade com outras distribuições Linux corporativas equivalentes ou derivadas tecnicamente suportadas pelo fabricante da solução durante a vigência contratual.



K. GERENCIAMENTO E INSTALAÇÃO REMOTA

- I. Deverá permitir ao administrador customizar a instalação;
- II. A instalação deverá ser possível executar com no mínimo das seguintes maneiras: Executar o pacote de antivírus diretamente na estação de trabalho, instalar remotamente, distribuído via console de gerencia web;
- III. Deverá ser possível ter um relatório com as estações instaladas e as faltantes da instalação;
- IV. A console de gerenciamento deve incluir informações detalhadas sobre as estações e servidores com no mínimo as seguintes informações: Nome, IP, Sistema Operacional, Política Aplicada;
- V. Através da console, o administrador poderá enviar uma política única para configurar o antivírus;
- VI. A console de gerenciamento deverá incluir sessão de log com as seguintes informações: Login, Edição, Criação, Log-out, ter a capacidade de criar um único pacote independente ser for para 32 bits ou 64 bits;
- VII. Deverá permitir ao administrador criar grupos e subgrupos para mover as estações de trabalho;
- VIII. O agente utilizado na sincronização deve ser incluído no cliente do antivírus e não ser necessário à distribuição em um agente separado;

L. PROTEÇÃO PARA ESTAÇÕES E SERVIDORES VIRTUAIS

- I. Proteção de antivírus dedicado para ambientes virtuais;
- II. Oferecer recursos de otimização de varredura para ambientes virtualizados, incluindo mecanismos com ou sem agente, quando suportados pela plataforma de virtualização;
- III. A console de gerenciamento central da solução deverá ter a possibilidade de integrar múltiplos vCenters da VMWare;
- IV. Deverá proteger em tempo real e agendado as máquinas virtuais Linux;
- V. Permitir integração com Microsoft Hyper-V, incluindo otimização de varredura para ambientes virtualizados;
- VI. Permitir integração com múltiplos servidores Hyper-V via console central;
- VII. Proteger máquinas virtuais Windows e Linux com varredura em tempo real e agendada;
- VIII. Possuir agentes compatíveis com plataformas de virtualização corporativa descritas na seção "Requisitos mínimos suportados pelo sistema";
- IX. A solução deverá disponibilizar agente compatível com ambientes virtualizados corporativos, contemplando prioritariamente Microsoft Hyper-V, bem como compatibilidade com as demais plataformas de virtualização descritas na seção "Requisitos mínimos suportados pelo sistema", em versões oficialmente



suportadas durante toda a vigência contratual.

M. FUNÇÕES GERAIS

- I. Deverá ter métodos de detecção de vírus, Spyware, rootkits e outros mecanismos de segurança;
- II. Deverá reportar o estado atual das VMs no mínimo, protegida/desprotegida;

N. REQUISITOS MÍNIMOS SUPORTADOS PELO SISTEMA

- I. A solução deverá possuir compatibilidade com ambientes de virtualização corporativa, com suporte preferencial à plataforma Microsoft Hyper-V, incluindo versões baseadas em Windows Server 2016, windows server 2019, Windows Server 2022 ou superiores, considerando sua adoção predominante no ambiente institucional.
- II. Adicionalmente, deverá manter compatibilidade com outras plataformas amplamente utilizadas no mercado, em versões oficialmente suportadas durante toda a vigência contratual, incluindo:
 - Microsoft Hyper-V
 - VMware vSphere
 - VMware vCenter Server
 - VMware Tools
 - Citrix Hypervisor
 - Citrix Virtual Apps and Desktops
 - Oracle Linux KVM
 - Red Hat Virtualization
 - A compatibilidade deverá abranger versões oficialmente suportadas pelos fabricantes durante toda a vigência contratual.
- III. Sistemas Operacionais Desktop
 - A solução deverá possuir compatibilidade com sistemas operacionais para estações de trabalho (32 e 64 bits) baseados em Microsoft Windows 10, Microsoft Windows 11 ou superiores, contemplando versões oficialmente suportadas pelo fabricante durante toda a vigência contratual.
- IV. Sistemas Operacionais Servidores
 - A solução deverá possuir compatibilidade com sistemas operacionais de servidores em versões oficialmente suportadas pelos respectivos fabricantes durante toda a vigência contratual, incluindo, no mínimo:
 - Ambiente Microsoft (preferencial):



- ❖ Windows Server 2019
- ❖ Windows Server 2022
- ❖ versões superiores suportadas
- Ambiente Linux corporativo:
 - ❖ Red Hat Enterprise Linux
 - ❖ Ubuntu LTS
 - ❖ SUSE Linux Enterprise Server
 - ❖ openSUSE
 - ❖ Fedora Linux
 - ❖ Debian

V. Admitindo-se compatibilidade com distribuições equivalentes tecnicamente suportadas pelo fabricante da solução durante a vigência contratual.

O. COMPONENTES E FUNCIONALIDADE DO ANTIVÍRUS GERAL

- I. Deverá fazer scan em tempo real automático;
- II. Deverá ser configurável para não escanear arquivos conforme necessidade do administrador, ou seja, por tamanho ou por tipo de extensão;
- III. Escaneamento de comportamento heurístico;
- IV. Deverá escanear em tempo real qualquer informação localizadas em mídias de armazenamento como: CD/DVD, Discos Externos, Pen-Drivers, Deverá permitir a escolha e configuração de pastas a serem escaneadas;
- V. Para melhor proteção, o antivírus deverá ter no mínimo 3 tipos de detecção: Baseada em Assinaturas, Baseada em Heurística, Baseada em monitoramento contínuo de processos;
- VI. Possuir capacidade de escaneamento e inspeção de tráfego HTTP e HTTPS, incluindo análise de tráfego criptografado SSL/TLS, configurável pelo administrador por meio de políticas centralizadas de segurança da informação, com possibilidade de definição de exceções, uso de certificados confiáveis e controle granular por endpoint, grupo ou usuário, observando os princípios da necessidade, proporcionalidade e finalidade no tratamento de dados, em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), respeitando os princípios de segurança, necessidade, adequação e minimização previstos na LGPD, com mecanismos de auditoria administrativa e rastreabilidade das políticas aplicadas.
- VII. O cliente do antivírus deverá ter o módulo de Antiphishing que deverá ter a opção de verificar links pesquisados com os sites de pesquisas acessados por meio de mecanismos de reputação web e proteção antiphishing baseada em inteligência de ameaças na Estações de trabalho;
- VIII. Deverá possuir módulo de firewall que de acordo com o administrador poderá ou



não ser

- IX. instalado/desinstalado nas estações de trabalho;
- X. O módulo de firewall deverá ser possível configurar o modo invisível tanto a nível de rede local ou Internet nas estações de trabalho;
- XI. Deverá permitir o envio automático de arquivos da quarentena para o laboratório de vírus;
- XII. Deverá fazer a remoção automática de arquivos antigos, pré-definidos pelo administrador;
- XIII. Deverá permitir a movimentação do arquivo da quarentena para seu local original ou outro destino que o administrador definir;
- XIV. Deverá de forma automática criar exclusão para arquivos restaurados da quarentena;
- XV. Deverá permitir escanear a quarentena após a atualização das atualizações de assinaturas;

P. CONTROLE DE USUÁRIO

- I. Deverá ter módulo de controle de acesso de usuário integrando com as seguintes características: Bloqueio de acesso a internet, Bloqueio de acesso a aplicações definidas pelo administrador;

Q. CONTROLE DO DISPOSITIVO

- I. Deverá ser possível a instalação do módulo de controle de dispositivos através da console de gerenciamento;
- II. Através do módulo de controle de dispositivo deverá ser possível controlar: Bluetooth, CDROM/DVDROM, IEEE 1284.4, IEEE 1394, Windows Portable, Adaptadores de Rede, Adaptadores de rede Wireless, Discos Externos;
- III. Deverá permitir regras de definição de bloqueio/desbloqueio;
- IV. Deverá permitir regras de exclusão;

R. ATUALIZAÇÃO

- I. Após a atualização o administrador deverá ter a capacidade de adiar uma reinicialização;
- II. Possibilidade de utilizar um servidor local para efetuar as atualizações das estações de trabalho;
- III. Permitir atualizações de assinatura de hora em hora;
- IV. Permitir motor de varredura local, no servidor de rede ou em nuvem afim de



aumentar o desempenho da estação de trabalho quando a mesma estiver sendo escaneada.

S. PROTEÇÃO PARA CAIXA DE E-MAIL:

- I. Quando suportado pela solução ofertada e licenciamento contratado, fornecer proteção para ambiente Microsoft Exchange;
- II. Oferecer tecnologia para proteção contra spam;
- III. Oferecer análise comportamental e proteção para zero-day;
- IV. Oferecer proteção contra vírus e tentativas de phishing;

T. CRIPTOGRAFIA

- I. Possibilitar o gerenciamento centralizado de criptografia de disco por meio da console de administração da solução, em ambiente local ou em nuvem.
- II. Permitir o gerenciamento centralizado dos mecanismos nativos de criptografia dos sistemas operacionais Windows (BitLocker) e macOS (FileVault), quando disponíveis e suportados pelo fabricante da solução sem substituição dos mecanismos nativos do sistema operacional
- III. Deverá solicitar autenticação quando iniciado o sistema operacional do equipamento;
- IV. Deverá ser compatível com sistemas operacionais macOS em versões suportadas oficialmente pelo fabricante, permitindo integração com os mecanismos nativos de criptografia FileVault e gerenciamento centralizado pela console da solução.

U. PROTEÇÃO AVANÇADA NGAV

- I. Detectar e bloquear todos os tipos de ameaças sofisticadas e malwares desconhecidos bem como eliminar malwares desconhecidos e ameaças avançadas que ignoram as soluções tradicionais de proteção de endpoints, incluindo o ransomware.
- II. Detectar e bloquear ataques avançados, como os ataques do PowerShell, baseados em scripts, ataques sem arquivos e malware sofisticado, devendo ser detectados e bloqueados antes de serem executados.
- III. Detectar e parar, bloquear e interromper malwares sem arquivos.
- IV. Parar os ataques com base em macros e scripts. Analisar scripts, como Powershell, WMI, intérpretes de Javascript, etc, bem como adicionar técnicas de analisador de linha de comando para interceptar e proteger scripts, enquanto alerta os administradores e bloqueia a execução de scripts no caso de executar comandos maliciosos.
- V. Fazer reparo e resposta automatizada a ameaças.



-
- VI.** Quando uma ameaça é detectada, a ferramenta deve neutralizá-la imediatamente por meio de ações que incluem a conclusão do processo, a quarentena, a exclusão e a reversão de alterações mal intencionadas.
 - VII.** Permitir reversão automática de alterações maliciosas realizadas por ransomware, incluindo restauração de arquivos afetados quando suportado pela solução.
 - VIII.** Permitir isolamento automático ou manual de endpoints comprometidos diretamente pela console de gerenciamento, mantendo comunicação apenas com a infraestrutura de segurança para contenção de incidentes.
 - IX.** Utilizar inteligência global de ameaças baseada em nuvem com coleta e correlação de telemetria anonimizada para detecção antecipada de ataques emergentes.
 - X.** Compartilhar as informações sobre ameaças em tempo real com o serviço de inteligência contra ameaças baseadas na nuvem do fabricante, para impedir ataques semelhantes.
 - XI.** Obter visibilidade e contexto sobre ameaças devendo identificar e reportar atividades suspeitas alertando antecipadamente para comportamentos maliciosos, como ações suspeitas do sistema operacional.
 - XII.** Operar com um único agente e console integrados bem como personalizar automaticamente o pacote de instalação e minimizar o carregamento do agente.
 - XIII.** Deverá ter um nível de proteção na fase de pré-execução com modelos locais de aprendizado de máquina e heurística avançada e treinada para detectar ferramentas de hackers, explorações e técnicas de ocultação de malware, a fim de bloquear ameaças sofisticadas antes que elas sejam executadas.
 - XIV.** Também deverá detectar técnicas de propagação e sites que hospedam kits de exploração, além de bloquear tráfego suspeito na web.
 - XV.** Deverá permitir que os administradores de segurança ajustem a proteção para combater os riscos.
 - XVI.** Detectar e bloquear técnicas de movimentação lateral entre endpoints da rede corporativa.
 - XVII.** Possuir capacidade de correlação automática e contextualização de eventos de segurança entre múltiplos endpoints, permitindo a identificação de ataques complexos, movimentações laterais e técnicas avançadas de exploração na rede corporativa.
 - XVIII.** Disponibilizar contextualização dos eventos de segurança com base em técnicas e táticas reconhecidas de ataques avançados, permitindo melhor investigação e resposta a incidentes.
 - XIX.** Detectar e bloquear ataques sem arquivos (fileless) em fase de pré-execução por meio de integração com mecanismos nativos do sistema operacional.
 - XX.** A solução deverá permitir contextualização dos eventos de segurança com base no framework MITRE ATT&CK ou equivalente reconhecido internacionalmente



V. MACHINE LEARNING

- I. As técnicas de Machine Learning devem utilizar modelos e algoritmos extensamente treinados para prever e bloquear os ataques avançados.
- II. A ferramenta de Machine Learning deve se basear em características estáticas e dinâmicas, e se treinar continuamente com bilhões de amostras de arquivos legítimos e maliciosos devendo melhorar significativamente a efetividade da detecção de malware e minimizar os falsos positivos, incluindo a detecção de ações evasivas e conexões com centros de comando e controle (C2).

W. SANDBOX

- I. Sandbox integrado à solução com análise automatizada de arquivos suspeitos em profundidade, acionar ações destrutivas em ambiente isolado hospedado em infraestrutura segura do fabricante ou ambiente oficialmente suportado, analisando seu comportamento e informando sobre intenções maliciosas.
- II. O Sandbox deve ser integrado com o agente e encaminhar automaticamente os arquivos suspeitos para análise.
- III. Ao retornar uma análise com resultado "malicioso", o Sandbox deverá bloquear automaticamente o arquivo malicioso em sistemas em toda rede imediatamente.
- IV. O recurso de envio automático deve permitir que os administradores de segurança da empresa escolham o modo de monitoramento ou bloqueio, o que impede o acesso a um arquivo até que um resultado seja emitido.
- V. Os administradores também podem enviar arquivos manualmente para análise.
- VI. As informações forenses devem fornecer um contexto claro das ameaças e ajudar a entender o comportamento delas.

X. ANTIEXPLOIT AVANÇADO

- I. Deverá conter antiexploit avançado para prevenção de exploração e proteção a memória e aplicativos vulneráveis, como navegadores, leitores de documentos, arquivos multimídia e ambientes de execução suportados oficialmente pelos fabricantes.
- II. Os mecanismos avançados devem observar a rotina de acesso na memória para detectar e bloquear técnicas de exploração, como verificação de chamadas de API, pivotamento de pilha, ROP (return oriented programming), etc.
- III. Detectar e bloquear técnicas de exploração baseadas exclusivamente em memória (memory-based attacks), inclusive sem utilização de arquivos persistentes.

Y. INSPETOR DE PROCESSO

- I. Inspetor de Processos deverá operar em um modo de confiança zero, monitorando



continuamente todos os processos em execução no sistema operacional.

- II. Deverá procurar atividades suspeitas ou comportamentos anormais de processos, como tentativas de ocultar o tipo de processo, executar código no espaço de outro processo (sequestro de memória do processo para escalonamento de privilégios), replicar, descartar arquivos, ocultar para processar aplicativos de listagem etc.
- III. Tomar as medidas de reparação adequadas, incluindo o encerramento do processo e a reversão das alterações efetuadas. Deverá detectar de malwares desconhecidos, avançando ataques sem arquivos, incluindo ransomware.

8. DESCRIÇÃO DA SOLUÇÃO CONSIDERANDO O CICLO DE VIDA

A presente contratação contempla o fornecimento e a continuidade operacional da solução durante todo o seu ciclo de vida, compreendendo as etapas de disponibilização, ativação, suporte técnico especializado, manutenção evolutiva e corretiva, atualizações tecnológicas e sustentação da plataforma ao longo da vigência contratual.

Considera-se que a solução já se encontra implantada e integrada ao ambiente tecnológico institucional, de modo que a Contratação das licenças representa medida mais econômica, eficiente e segura do que a substituição da plataforma, evitando custos adicionais relacionados à migração tecnológica, reconfiguração de ambiente, capacitação de usuários e riscos de descontinuidade operacional.

Dessa forma, a contratação observa o ciclo de vida da solução como elemento de planejamento, garantindo continuidade do serviço, estabilidade operacional, segurança da informação e otimização dos recursos públicos.

9. DO VALOR E PROPOSTA

9.1. O custo estimado total da contratação será estimado pela Secretaria-Adjunta de Compras e Licitação (ADCL), conforme custos resultantes da Pesquisa de Preços acostadas ao referido processo, o que não exime a necessidade do levantamento de valor apresentado no ETP.

9.2. A proposta deverá ser digitada, redigida em linguagem clara, sem emendas, rasuras ou entrelinhas, e deverá conter os seguintes elementos:

9.2.1. Indicar CNPJ, e-mail, endereço e telefone de contato;

9.2.2. especificação do item com preço unitário e total expressos em moeda corrente nacional em algarismos e por extenso, relativo ao item cotado, já inclusa todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de



administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

9.3. Declarar expressamente a concordância com as condições constantes no Termo de Referência, e do Edital.

10. TRATAMENTO DIFERENCIADO ÀS ME/EPP

Nos termos da Lei Complementar nº 123/2006 e da Lei nº 14.133/2021, será assegurado tratamento favorecido às microempresas e empresas de pequeno porte quanto às condições de participação, regularidade fiscal e trabalhista e critérios legais de desempate, quando aplicáveis.

Contudo, considerando as características específicas do objeto contratado, sua natureza tecnológica especializada, a dependência operacional da solução e a forma de execução contratual prevista neste Termo de Referência, o tratamento diferenciado não poderá resultar em restrições à adequada execução do objeto, à continuidade dos serviços, à segurança institucional da solução contratada ou à vantajosidade da contratação para a Administração Pública.

Adicionalmente, registra-se que a aplicação dos benefícios previstos na Lei Complementar nº 123/2006 observará, quando cabível, a compatibilidade com a natureza da contratação, especialmente nos casos em que a execução do objeto dependa de solução tecnológica proprietária, infraestrutura operacional específica ou fornecedor tecnicamente habilitado à prestação integral do serviço.

A presente disposição observa os princípios da isonomia, da eficiência, da continuidade do serviço público e da seleção da proposta mais vantajosa para a Administração, conforme previsto na legislação aplicável e nas boas práticas de planejamento das contratações públicas.

11. QUALIFICAÇÃO TÉCNICA

A licitante deverá comprovar sua regularidade jurídica, fiscal, trabalhista, econômico-financeira e técnica, mediante a apresentação da documentação mínima exigida pela legislação vigente e por este Termo de Referência, observadas as disposições da Lei Federal nº 14.133/2021. **Os critérios de avaliação da proposta e seleção do fornecedor encontram-se descritos no item 28 deste Termo de Referência.**

No que se refere à qualificação técnica, a licitante deverá comprovar aptidão para o fornecimento de solução compatível com o objeto da contratação, mediante apresentação de atestado(s) ou certidão(ões) emitido(s) por pessoa jurídica de direito público ou privado, que demonstre(m) a execução satisfatória de serviços ou fornecimentos similares, de complexidade tecnológica e operacional equivalente ou superior, incluindo, dentre outros, fornecimento ou Contratação de licenciamento



de antivírus corporativo, console centralizado de gerenciamento, suporte técnico especializado e atualização contínua da solução.

Os atestados deverão evidenciar o cumprimento adequado de prazos, especificações e níveis de qualidade, sendo admitida a apresentação e o somatório de diferentes atestados executados de forma concomitante para fins de comprovação da capacidade técnica. A Administração poderá solicitar informações complementares para verificação da legitimidade dos documentos apresentados, incluindo cópia de contratos, dados da contratante e demais elementos pertinentes.

Não será admitida a apresentação de atestado emitido por empresa integrante do mesmo grupo econômico da licitante, quando ambas pertencerem ao mesmo conglomerado empresarial. Os documentos apresentados estarão sujeitos à verificação quanto à autenticidade e veracidade de seus conteúdos, inclusive para os fins previstos na legislação aplicável.

Certificados emitidos por fabricantes, comprovação de parceria autorizada ou relação de projetos atendidos poderão ser apresentados como documentação complementar de reforço técnico, sem caráter obrigatório. A Administração poderá promover diligências para esclarecer ou complementar informações, nos termos da legislação vigente.

12. EXECUÇÃO DO CONTRATO

A execução do objeto consiste na Contratação do licenciamento da solução Bitdefender GravityZone, atualmente implantada e em pleno funcionamento no ambiente tecnológico institucional do CONTRATANTE, devendo a CONTRATADA assegurar a continuidade operacional da solução durante toda a vigência contratual.

A solução encontra-se implantada em arquitetura baseada em console centralizado em nuvem do fabricante (GravityZone Cloud), com agentes instalados nos ativos computacionais institucionais, devendo a Contratação do licenciamento preservar o ambiente lógico existente, suas parametrizações administrativas e políticas de segurança aplicadas, sempre que compatível com o modelo de licenciamento disponibilizado pelo fabricante.

A Contratação deverá ocorrer sem necessidade de reinstalação da console centralizada ou reimplantação dos agentes já instalados, evitando procedimentos desnecessários de migração ou reconfiguração.

A CONTRATADA deverá disponibilizar integralmente as licenças renovadas no prazo máximo de 05 (cinco) dias úteis, contados da emissão da Ordem de Fornecimento, por meio eletrônico.

Durante a execução contratual, a CONTRATADA deverá assegurar:

- disponibilização das licenças compatíveis com a infraestrutura tecnológica institucional existente;
- manutenção da comunicação funcional entre a console centralizada em nuvem e os agentes instalados;



- atualização automática e contínua das assinaturas e mecanismos de proteção contra ameaças cibernéticas;
- suporte técnico durante a vigência contratual, observado o SLA;
- rastreabilidade e auditabilidade das ações administrativas realizadas na plataforma;
- disponibilização dos acessos administrativos necessários à gestão institucional da solução;
- correção de falhas críticas de segurança eventualmente identificadas;
- comunicação tempestiva ao CONTRATANTE acerca de incidentes relevantes.

A solução deverá estar ativa e operacional na assinatura do contrato, assegurando a continuidade da proteção do ambiente computacional institucional.

Considerando tratar-se de Contratação de licenciamento de solução já implantada, não haverá necessidade de nova implantação da infraestrutura de gerenciamento, devendo ser preservada a estrutura tecnológica existente, sem prejuízo da possibilidade de futura adoção de arquitetura alternativa pela Administração, conforme avaliação de conveniência e oportunidade.

Compete ao CONTRATANTE:

- disponibilizar acesso ao ambiente tecnológico necessário à validação da solução;
- indicar os administradores responsáveis pela gestão da plataforma;
- validar tecnicamente o funcionamento da solução após a ativação das licenças.

Fica vedada qualquer interrupção da cobertura de proteção antivírus decorrente de falha de ativação, licenciamento ou manutenção contratual imputável à CONTRATADA.

13. RECEBIMENTO, MEDIÇÃO E PAGAMENTO DO OBJETO

O recebimento do objeto ocorrerá em duas etapas, observadas as disposições da Lei nº 14.133/2021, considerando tratar-se de Contratação de licenciamento de solução de segurança da informação já implantada e em operação no ambiente tecnológico institucional do CONTRATANTE.

13.1 Recebimento Provisório

O recebimento provisório deverá ocorrer em até 05 (cinco) dias, contados da disponibilização e ativação das licenças no ambiente institucional, para efeito de posterior verificação da conformidade dos produtos ofertados com as especificações, condições, local e prazo previstos neste Termo de Referência.



Nesta etapa, serão verificados:

- ativação das licenças contratadas no ambiente institucional;
- continuidade operacional da solução;
- apresentação de evidências técnicas extraídas da console administrativa da solução.

Os bens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta apresentada, devendo ser substituídos ou regularizados no prazo de até 10 (dez) dias, contados da notificação da CONTRATADA, às suas expensas, sem prejuízo da aplicação das penalidades cabíveis.

13.2 Recebimento Definitivo

O recebimento definitivo deverá ocorrer em até 08 (oito) dias após a conclusão das verificações técnicas e da comprovação da conformidade do objeto, mediante aceitação pelo setor competente.

Para fins de recebimento definitivo, será realizada validação técnica pela equipe responsável, mediante verificação de:

- pleno funcionamento da solução no ambiente produtivo institucional;
- inexistência de descontinuidade da proteção antivírus;
- conformidade da execução com as especificações estabelecidas neste Termo de Referência;
- regularidade da ativação e vigência das licenças contratadas.

Considerar-se-á cumprida a obrigação contratual quando comprovados:

- ativação válida das licenças contratadas no ambiente institucional;
- continuidade operacional da solução;
- apresentação de evidências técnicas extraídas da console administrativa da solução;
- conformidade da solução com os requisitos técnicos e operacionais previstos neste Termo de Referência.

A CONTRATADA deverá apresentar faturamento em parcela única após o recebimento definitivo do objeto, contendo:

- identificação da solução licenciada (fabricante, edição e modalidade);
- quantitativo total de licenças fornecidas;
- período de vigência do licenciamento;



- relatórios técnicos extraídos da console de gerenciamento da solução;
- declaração de conformidade com as condições contratuais.

O pagamento será efetuado após:

- emissão do Termo de Recebimento Definitivo pela equipe técnica responsável;
- verificação da regularidade fiscal da CONTRATADA;
- apresentação da documentação comprobatória da ativação das licenças.

Considerando tratar-se de Contratação de licenciamento de solução já implantada e disponibilizada por meio eletrônico, a medição por entrega integral mostra-se adequada à natureza do objeto, devendo ser o pagamento realizado de forma única e integral, permanecendo obrigatória a manutenção da disponibilidade operacional da solução durante toda a vigência contratual.

13.3 Do Pagamento

13.3.1 Forma de Pagamento:

13.3.1.1 O pagamento será realizado através de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo CONTRATADO.

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

13.3.1.3 O pagamento deverá ser realizado de forma única e integral.

13.3.2 Prazo de Pagamento:

13.3.2.1 O pagamento será efetuado no prazo máximo de até 30 (trinta) dias, contados do recebimento da Nota Fiscal.

13.3.2.2 Considera-se ocorrido o recebimento da nota fiscal quando o órgão CONTRATANTE atestar a execução do objeto do contrato.

13.3.2.3 No caso de atraso pela CONTRATANTE, os valores devidos ao CONTRATADO serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice IPCA de correção monetária.

13.3.2.4 Obedecerá a ordem cronológica conforme art. 141, II da Lei nº 14.133/2021.



13.3.3 Condições de Pagamento:

13.3.3.1 A emissão da Nota Fiscal será precedida do recebimento definitivo do objeto da contratação, conforme disposto neste instrumento e/ou no Termo de Referência.

13.3.3.2 As Notas Fiscais devem ser discriminativas, em 02 (duas) vias, devidamente atestada por 02 (dois) servidores designados pelo setor competente, demonstrando que os bens foram entregues conforme pactuado, em nome da Unidade demandante.

13.3.3.3 Quando houver glosa parcial do objeto, à CONTRATANTE deverá comunicar a empresa para que emita nota fiscal com o valor exato dimensionado.

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

- a) o prazo de validade;
- b) a data da emissão;
- c) os dados do contrato e do órgão CONTRATANTE;
- d) o período respectivo de execução do contrato;
- e) o valor a pagar; e
- f) eventual destaque do valor de retenções tributárias cabíveis.

13.3.3.5 Havendo erro na apresentação da Nota Fiscal, ou circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que o CONTRATADO providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação não acarretando qualquer ônus para a CONTRATANTE.

13.3.3.6 A Nota Fiscal deverá ser obrigatoriamente acompanhada 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 14.133/2021.

13.3.3.7 Previamente à emissão de nota de empenho e a cada pagamento, 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, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas.

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

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

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

13.3.3.11 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.

14. CRITÉRIOS DE REAJUSTE

- 14.1. Os preços são fixos e irrealizáveis no prazo de 1 (um) ano.
- 14.2. Após o decurso desse prazo, admite-se o reajuste, com data-base vinculada à data do orçamento estimado, conforme o disposto no art. 92, §3º, da Lei 14.133/21.
- 14.3. Dentro do prazo de vigência do contrato e mediante solicitação da contratada, os preços contratados poderão sofrer reajuste após o interregno de 1 (um) ano, aplicando-se o índice IPCA-E exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade. Na ausência deste, deve-se considerar o IGP-M.

15. DA VIGÊNCIA

O contrato decorrente deste Termo de Referência terá vigência de 36 (trinta e seis) meses, contados da data de assinatura contratual ou da ativação das licenças,



conforme definido no instrumento contratual, assegurando a continuidade da proteção do ambiente tecnológico institucional durante todo o período.

A vigência abrangerá, no mínimo:

- disponibilização das licenças da solução corporativa de proteção de endpoints;
- acesso ao console central de gerenciamento da plataforma;
- atualizações automáticas dos mecanismos de detecção e das assinaturas antivírus;
- suporte técnico durante todo o período de subscrição;
- manutenção integral das funcionalidades de segurança contratadas;
- garantia de funcionamento contínuo da solução.

A CONTRATADA deverá assegurar a manutenção contínua da subscrição da solução junto ao fabricante, garantindo a validade das licenças, suporte técnico e atualizações de segurança durante os 36 meses de execução contratual.

A definição do prazo contratual fundamenta-se na natureza continuada e essencial dos serviços de proteção contra ameaças cibernéticas, na necessidade de manutenção permanente da segurança dos ativos de informação, na compatibilidade com práticas de mercado, na economicidade decorrente da contratação por período ampliado e na observância dos princípios de planejamento, eficiência e continuidade administrativa previstos na Lei nº 14.133/2021.

A eventual prorrogação poderá ocorrer nos termos da legislação vigente, mediante demonstração de: vantajosidade administrativa, regular execução contratual, manutenção da necessidade institucional, disponibilidade orçamentária e autorização da autoridade competente.

16. CENTRAL DE SUPORTE TÉCNICO

A CONTRATADA deverá disponibilizar canal formal de suporte técnico especializado para registro, acompanhamento e tratamento de incidentes e solicitações relacionadas à solução de segurança da informação contratada.

O suporte técnico deverá ser prestado por meio de plataforma eletrônica, portal de atendimento, sistema de chamados, correio eletrônico institucional ou outro mecanismo equivalente que permita:

- registro formal das solicitações;
- acompanhamento do status dos atendimentos;
- manutenção do histórico das ocorrências;



- rastreabilidade das demandas para fins de auditoria e fiscalização contratual.

O acesso ao canal de suporte deverá ser disponibilizado a até 10 (dez) usuários indicados pelo CONTRATANTE, sem prejuízo de eventual ampliação justificada por necessidade operacional.

Considerando tratar-se de solução corporativa estratégica de proteção de endpoints já implantada no ambiente institucional, o suporte técnico deverá assegurar atendimento compatível com a criticidade operacional da ferramenta, garantindo resposta adequada às ocorrências que possam comprometer a segurança do ambiente computacional da Administração.

17. NÍVEIS DE SERVIÇO (SLA – SERVICE LEVEL AGREEMENT)

Considerando tratar-se de solução corporativa de segurança digital já implantada e integrada ao ambiente tecnológico institucional, responsável pela proteção ativa dos endpoints da Administração Municipal contra ameaças cibernéticas, os níveis mínimos de serviço estabelecidos neste instrumento possuem natureza estratégica, essencial e vinculante à execução contratual.

17.1 Regime de Operação

Os serviços contratados deverão operar em regime contínuo **24 (vinte e quatro) horas por dia, 7 (sete) dias por semana (24x7)**, assegurando proteção permanente do ambiente computacional institucional.

Admite-se interrupção apenas nas seguintes hipóteses:

- manutenção programada previamente comunicada;
- manutenção emergencial tecnicamente justificada;
- eventos excepcionais fora da governabilidade da CONTRATADA.

17.2 Caracterização de Indisponibilidade do Serviço

Será caracterizada indisponibilidade do serviço qualquer ocorrência que comprometa a capacidade de proteção ativa dos endpoints institucionais, incluindo:

- interrupção do funcionamento da console de gerenciamento centralizado;
- falha na comunicação entre agentes instalados e servidores de atualização;
- indisponibilidade dos mecanismos automáticos de atualização de assinaturas;
- falha na aplicação das políticas de segurança definidas pelo CONTRATANTE;



- indisponibilidade dos serviços de detecção, prevenção ou resposta a ameaças;
- interrupção da comunicação com os serviços de inteligência contra ameaças mantidos pela CONTRATADA.

Considerando tratar-se de solução corporativa já implantada e integrada ao ambiente institucional, eventual indisponibilidade poderá comprometer diretamente a segurança dos ativos digitais da Administração Municipal, caracterizando risco operacional relevante.

17.3 Escopo do Acordo de Nível de Serviço

O SLA compreende:

- disponibilidade da console administrativa de gerenciamento centralizado;
- funcionamento regular dos agentes de proteção instalados nos endpoints;
- atualização automática das bases de detecção de ameaças;
- comunicação contínua com a infraestrutura de inteligência contra ameaças;
- aplicação e sincronização das políticas de segurança definidas pelo CONTRATANTE;
- funcionamento dos mecanismos de detecção, prevenção e resposta a incidentes;
- estabilidade da infraestrutura tecnológica sob responsabilidade da CONTRATADA;
- suporte técnico especializado.

17.4 Índice Mínimo de Disponibilidade

- O índice mínimo mensal de disponibilidade dos serviços será de:
Disponibilidade da solução (uptime): $\geq 99,95\%$ ao mês e **Proteção em Tempo Real (Real-time Scanning):** = **100% do tempo** nos endpoints (computadores, servidores).

Esse percentual encontra-se compatível com padrões corporativos adotados para soluções enterprise de proteção de endpoints e atende às boas práticas de governança de tecnologia da informação na Administração Pública.

17.5 Compensações por Descumprimento do SLA (Pagamento Único)



Considerando que a contratação será realizada mediante pagamento único do licenciamento, eventual descumprimento do índice mínimo de disponibilidade ensejará aplicação de compensação proporcional ao CONTRATANTE, conforme o nível de indisponibilidade verificado no período.

Disponibilidade Verificada	Compensação Aplicável
≥ 99,99%	0%
98,9% a 95%	0,5%
94,9% a 92%	1%
91,9% a 82%	1,5%
81,9% a 72%	2%
71,9% a 62%	2,5%
≤ 61,9%	3%

A compensação poderá ser efetivada mediante:

- restituição proporcional de valores;
- concessão de crédito contratual compensável em eventual Contratação;
- extensão proporcional do período de vigência do licenciamento;
- ou outra forma equivalente de recomposição do equilíbrio contratual.

A aplicação das compensações não afasta eventual incidência das demais penalidades previstas na Lei nº 14.133/2021.

Considerando tratar-se de contratação remunerada em parcela única, a apuração das glosas poderá ensejar restituição proporcional ao erário, execução parcial da garantia contratual, compensação administrativa em eventual prorrogação contratual ou aplicação das sanções previstas nos arts. 155 a 163 da Lei nº 14.133/2021.

17.6 Comprovação da Prestação do Serviço

A comprovação do cumprimento dos níveis de serviço será realizada por meio de evidências técnicas extraídas da console administrativa da solução, registros do sistema de suporte técnico e demais mecanismos de monitoramento disponibilizados pela CONTRATADA.

Considerando tratar-se de solução corporativa de proteção de endpoints operando em regime contínuo, a fiscalização contratual poderá solicitar, sempre que necessário, informações técnicas relativas à disponibilidade da solução e ao funcionamento dos mecanismos de proteção ativos.

Quando solicitado pelo CONTRATANTE, a CONTRATADA deverá disponibilizar, no mínimo:

- relação dos incidentes registrados;



- data e hora de início e término das indisponibilidades relevantes;
- causa técnica identificada;
- impactos operacionais decorrentes;
- medidas corretivas adotadas;
- evidências extraídas da console de gerenciamento da solução.

A disponibilização das informações técnicas deverá ocorrer em prazo compatível com a criticidade da demanda e com os níveis de serviço contratados.

17.7 Exclusões do Cálculo do SLA

Não serão consideradas indisponibilidades:

- manutenções programadas previamente comunicadas com antecedência mínima de 48 horas;
- manutenções emergenciais tecnicamente justificadas;
- falhas decorrentes de infraestrutura externa não gerida pela CONTRATADA;
- indisponibilidades decorrentes de falhas de conectividade de terceiros;
- ataques cibernéticos massivos de escala global;
- eventos de força maior ou caso fortuito;
- indisponibilidades provocadas por ação ou omissão do CONTRATANTE em desacordo com orientações técnicas formais.

17.8 Prazo de Resposta do Suporte Técnico

- **Tempo de resposta do suporte técnico:**
 - Suporte remoto de alta prioridade: até 1 hora;
 - Suporte remoto de prioridade média: até 4 horas;
 - Suporte remoto de baixa prioridade: até 24 horas;
- **Tempo de resolução de incidentes:**
 - Incidentes críticos (ameaça ativa ou interrupção de serviço): até 8 horas*;
 - Incidentes de média criticidade: até 24 horas;
 - Incidentes de baixa criticidade: até 72 horas;



**Considera-se incidentes críticos (incluindo, mas não se limitando a: suspeita ou confirmação de vazamento de dados, acesso não autorizado, execução de código malicioso, ransomware ou indisponibilidade de serviços essenciais):*

Resposta inicial: até 1 (uma) hora;

Contenção ou mitigação: até 2 (duas) horas;

Resolução: até 8 (oito) horas;

- **Atualizações de segurança e software:**
 - Atualizações de definições de vírus: diariamente;
 - Atualizações de software (patches e correções críticas): semanalmente ou conforme liberação do fabricante;
- **Monitoramento e relatórios:**
 - Alertas de segurança: em tempo real;
 - Relatórios gerenciais: semanalmente;
- **Disponibilidade da solução (uptime):** ≥ 99,95% ao mês e **Proteção em Tempo Real (Real-time Scanning):** = 100% do tempo nos endpoints (computadores, servidores).
- Os prazos são compatíveis com padrões corporativos aplicáveis a soluções de segurança de endpoints.

18. CÁLCULO DOS INDICADORES DE DISPONIBILIDADE

18.1 Fórmula de Cálculo da Disponibilidade

O índice mensal de disponibilidade será apurado conforme a seguinte metodologia:

$$DA (\%) = \frac{[TMC (m) - TIA (m)]}{TMC (m)} \times 100$$

- $DA (\%)$ = Índice de disponibilidade apurada (percentual);
- $TMC (m)$ = Total de minutos contratados no mês;
- $TIA (m)$ = Tempo total das interrupções do serviço durante o regime de operação em minutos;

Serão consideradas exclusivamente indisponibilidades sob responsabilidade direta da CONTRATADA.



18.2 Apuração das Indisponibilidades

Para fins de cálculo do SLA, será considerado o somatório dos minutos de indisponibilidade ocorridos durante o período de apuração, com base em registros:

- do sistema de monitoramento da solução;
- da console administrativa;
- do sistema de service desk;
- dos relatórios técnicos mensais.

Não serão computadas como indisponibilidades:

- ocorrências em ambientes não gerenciados pela CONTRATADA;
- eventos fora do regime operacional contratado;
- paradas programadas previamente comunicadas;
- eventos decorrentes de fatores externos;
- hipóteses de força maior ou caso fortuito.

18.3 Relevância Institucional da Continuidade do Serviço

Considerando tratar-se de Contratação de licenciamento de solução corporativa de proteção de endpoints já implantada e integrada ao ambiente institucional, a manutenção dos níveis mínimos de disponibilidade constitui requisito essencial para:

- proteção contra malware, ransomware e ameaças avançadas;
- preservação da integridade dos ativos digitais municipais;
- continuidade dos serviços públicos digitais;
- mitigação de riscos operacionais e jurídicos;
- conformidade com diretrizes de segurança da informação;
- atendimento às boas práticas de governança de tecnologia da informação recomendadas pelos órgãos de controle externo.

Os níveis de serviço estabelecidos neste instrumento encontram-se alinhados às diretrizes da Lei nº 14.133/2021 e às práticas de fiscalização contratual aplicáveis às contratações diretas de soluções tecnológicas estratégicas já integradas ao ambiente institucional, nos termos do art. 75, inciso IX.

19. VALIDAÇÃO E CONTROLE DE MUDANÇAS



Caso ocorram alterações no escopo, contexto operacional ou requisitos técnicos durante o ciclo de execução dos serviços, será realizada a avaliação dos impactos decorrentes sobre as atividades, prazos, níveis de serviço e recursos envolvidos.

Quando tais alterações implicarem modificação do objeto originalmente contratado, poderão ensejar entendimentos comerciais entre as partes, inclusive com a possibilidade de revisão contratual, nos termos da legislação vigente.

Nessas hipóteses, a CONTRATADA deverá elaborar e apresentar nova proposta técnica e comercial, devidamente fundamentada, para análise e eventual aprovação pelo CONTRATANTE, mediante formalização de instrumento próprio.

20. UNIDADE GESTORA E FISCALIZADORA DO CONTRATO

A Secretaria Municipal de Fazenda do Município de Cabo Frio será a unidade gestora do contrato, responsável pelo acompanhamento, coordenação e fiscalização da execução do objeto contratado, de modo a assegurar o fiel cumprimento das condições estabelecidas neste Termo de Referência e no respectivo instrumento contratual.

Será formalmente designado, por ato da autoridade competente:

20.1 Gestor do Contrato

O Gestor do Contrato será responsável pelo acompanhamento geral da execução contratual, pela interlocução com a CONTRATADA, pela orientação quanto ao cumprimento das obrigações pactuadas e, se necessário, pela adoção de medidas administrativas cabíveis para assegurar a adequada execução dos serviços, nos termos da legislação vigente.

20.2 Fiscal Administrativo do Contrato

O Fiscal Administrativo do Contrato, indicado pela autoridade competente, será responsável pela fiscalização dos aspectos administrativos da execução contratual, especialmente quanto à verificação da regularidade fiscal, trabalhista e previdenciária da CONTRATADA, bem como pela análise da documentação necessária para fins de ateste e pagamento.

Quando necessário, poderá ainda ser designado Fiscal Técnico, responsável pela verificação da conformidade técnica dos serviços prestados, especialmente quanto à disponibilidade, segurança da informação, atualização das bases de dados e cumprimento dos níveis de serviço estabelecidos.

21. DA EXECUÇÃO E GESTÃO DO CONTRATO



21.1. O prazo de vigência da contratação é de 36 (trinta e seis) meses, contados da assinatura do contrato, correspondente ao período de validade das licenças e suporte técnico, podendo ser prorrogado nos termos da Lei nº 14.133/2021, desde que comprovada a vantagem para a Administração.

21.2. Os contratos poderão ser alterados, com as devidas justificativas, nos casos previstos no art. 124 da Lei nº 14.133/2021, no que couber à presente contratação.

21.3. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133/2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial (art. 115, caput).

21.4. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o prazo de vigência será ajustado pelo tempo correspondente, mediante apostilamento (art. 115, §5º), quando aplicável à natureza do objeto.

21.5. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (art. 117, caput).

21.5.1. O fiscal do contrato anotará em registro próprio todas as ocorrências relacionadas à execução contratual, especialmente quanto à disponibilização das licenças, funcionamento da solução, atualizações e suporte técnico.

21.5.2. O fiscal do contrato informará a seus superiores, em tempo hábil, situações que demandem decisão ou providência que ultrapasse sua competência (art. 117, §2º).

21.6. O CONTRATADO será obrigado a corrigir falhas, inconsistências ou indisponibilidades da solução, bem como providenciar a adequada prestação do suporte técnico, sem ônus adicional, quando decorrentes de sua responsabilidade.

21.7. O CONTRATADO será responsável pelos danos causados diretamente à Administração ou a terceiros em razão da execução do contrato (art. 120).

21.8. Somente o CONTRATADO será responsável pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do contrato (art. 121).

21.8.1. A inadimplência do CONTRATADO não transferirá à Administração a responsabilidade pelo seu pagamento.

21.9. As comunicações entre o órgão e a CONTRATADA deverão ocorrer, preferencialmente, por meio eletrônico oficial, admitindo-se formalização por escrito quando necessário.

21.10. O órgão poderá convocar representante da empresa para adoção de providências imediatas.

21.11. A Administração poderá adotar providências acauteladoras, inclusive retenção de pagamento, em caso de risco iminente (Lei nº 9.784/1999, art. 45).

21.12. Antes do pagamento, deverá ser consultada a regularidade da empresa junto ao SICAF.



21.13. Serão exigidas as certidões de regularidade fiscal, trabalhista e fundiária, caso não estejam atualizadas no SICAF.

21.14. Além do disposto acima, a fiscalização observará:

- verificação da disponibilidade e validade das licenças;
- acompanhamento de atualizações da solução;
- monitoramento da eficácia da proteção;
- avaliação do suporte técnico prestado;
- registro de incidentes e tratativas.
- verificação da vigência e não expiração das licenças ao longo do período contratado;

21.15. A CONTRATADA designará formalmente preposto para atuação junto à Administração.

21.16 O gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022, 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);

21.17 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. (Decreto nº 11.246, de 2022, art. 21, II);

21.18 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. (Decreto nº 11.246, de 2022, art. 21, III);

21.19 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. (Decreto nº 11.246, de 2022, art. 21, VIII);

21.20 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. (Decreto nº 11.246, de 2022, art. 21, X).



21.21 O gestor do contrato deverá elaborar 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. (Decreto nº 11.246, de 2022, art. 21, VI).

21.22 O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

21.23. Será indicada a aplicação de sanções administrativas e/ou apuração de ressarcimento ao erário, proporcional à irregularidade verificada, caso se constate que a CONTRATADA:

- não disponibilizou as licenças contratadas;
- não garantiu o funcionamento adequado da solução;
- não prestou suporte técnico conforme exigido; ou
- descumpriu níveis mínimos de serviço, quando estabelecidos.

22. DO ACOMPANHAMENTO E DA FISCALIZAÇÃO

22.1. A fiscalização da contratação decorrente do termo de referência caberá a servidor indicado em tempo hábil pela CONTRATANTE, que determinará o que for necessário para regularização de falhas ou inconsistências na prestação do serviço, nos termos do art. 117 da Lei nº 14.133/2021 e do Decreto Municipal nº 6.941/2022.

22.2. A indicação do(s) membro(s) responsável(eis) pela fiscalização será realizada pelo Ordenador de Despesas, em instrumento próprio de designação, no momento oportuno.

22.3. São atividades inerentes à fiscalização do contrato:

22.3.1. Responder a eventuais esclarecimentos técnicos da CONTRATADA.

22.3.2. Após a formalização da contratação, manter registro e organização de todas as informações relevantes sobre o contrato, incluindo documentação técnica da solução, termos de licenciamento e registros de ocorrências.

22.3.3. Certificar-se de obter e manter atualizadas as informações de contato do preposto da empresa e de seus canais de suporte técnico, inclusive quanto aos níveis de atendimento e prazos de resposta.

22.3.4. Manter registro próprio onde anotar todas as ocorrências relevantes referentes ao contrato, incluindo falhas, indisponibilidades da solução, eventos de segurança e providências adotadas.



22.3.5. Apresentar, quando solicitado, relatório circunstanciado de acompanhamento da execução contratual, especialmente quanto à disponibilização das licenças, funcionamento da solução e suporte técnico.

22.3.6. Notificar por escrito ao Gestor sobre quaisquer falhas, indisponibilidades ou descumprimento das obrigações contratuais, quando não solucionadas diretamente com o preposto da CONTRATADA.

22.3.7. Atestar a Nota Fiscal emitida pela CONTRATADA, após a verificação da efetiva disponibilização das licenças, ativação da solução, início da vigência contratual e disponibilização dos canais de suporte técnico.

22.4. Ficam reservados ao Gestor do contrato o direito e a autoridade para resolver todo e qualquer caso singular, omissos ou duvidosos não previstos no processo administrativo e que se relacione com o objeto da contratação, desde que não acarrete ônus adicional ou modificação indevida.

22.5. As decisões que ultrapassarem a competência do Gestor deverão ser encaminhadas à autoridade administrativa superior, em tempo hábil para adoção das medidas cabíveis.

22.6. A existência e a atuação da gestão e da fiscalização não restringem a responsabilidade única, integral e exclusiva da CONTRATADA quanto à adequada prestação dos serviços, incluindo a disponibilidade, atualização e eficácia da solução, bem como eventuais danos causados à Administração ou a terceiros.

22.7. O fiscal administrativo do contrato, além das atribuições previstas na IN SGD nº 94/2022, verificará a manutenção das condições de habilitação, acompanhará os aspectos administrativos e financeiros da execução, inclusive empenho, pagamento, glosas e eventuais alterações contratuais, nos termos do Decreto nº 11.246/2022.

22.8. Em caso de descumprimento contratual, o fiscal administrativo atuará tempestivamente na solução, reportando ao gestor do contrato quando a situação ultrapassar sua competência.

23. DA INEXECUÇÃO E RESCISÃO CONTRATUAL

23.1. A inexecução do objeto deste Termo de Referência, total ou parcialmente, inclusive quanto à não disponibilização das licenças, falhas na prestação do suporte técnico ou indisponibilidade da solução, poderá ensejar a rescisão contratual, na forma dos arts. 137 a 139 da Lei nº 14.133/2021, com as consequências previstas em lei e neste instrumento.

23.2. A rescisão unilateral do contrato poderá ser determinada pela CONTRATANTE, nos termos do art. 138, inciso I da Lei nº 14.133/2021, com as consequências previstas no art. 139, sem prejuízo das demais sanções cabíveis.

23.3. Constituem motivo para rescisão do contrato as hipóteses previstas no art. 137 da Lei nº 14.133/2021.



23.4. Os casos de rescisão contratual serão formalmente motivados nos autos do processo, assegurados o contraditório e a ampla defesa.

23.5. A rescisão consensual será precedida de autorização escrita e fundamentada da autoridade competente.

23.6. A rescisão determinada por ato unilateral da Administração, nos casos previstos na legislação, acarretará as consequências estabelecidas na Lei nº 14.133/2021, inclusive quanto à aplicação de sanções administrativas, sem prejuízo de outras medidas cabíveis.

23.7. A ocorrência de quaisquer das hipóteses previstas no art. 137 da Lei nº 14.133/2021 poderá ensejar a rescisão do contrato.

23.8. Nos casos de rescisão, deverão ser observadas as disposições relativas à continuidade do serviço, quando aplicável, de modo a evitar descontinuidade na proteção dos ativos de tecnologia da informação da Administração, inclusive mediante adoção de soluções temporárias de contingência, se necessário.

24. DAS INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

24.1. Comete infração administrativa, nos termos do art. 155 da Lei nº 14.133/2021, a CONTRATADA que:

- a) Der causa à inexecução parcial do contrato;
- b) Der causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;
- c) Der causa à inexecução total do contrato;
- d) Deixar de entregar a documentação exigida para a contratação;
- e) Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;
- f) Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;
- g) Ensejar o retardamento da execução do objeto, inclusive quanto à disponibilização das licenças ou à prestação do suporte técnico, sem motivo justificado;
- h) Apresentar declaração ou documentação falsa ou prestar declaração falsa durante a execução do contrato;
- i) Praticar ato fraudulento na execução do contrato;
- j) Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- k) Praticar atos ilícitos com vistas a frustrar os objetivos da contratação;
- l) Praticar ato lesivo previsto no art. 5º da Lei nº 12.846/2013.



24.2. Conforme disposto no Decreto Municipal nº 7.074/2023, serão aplicadas ao responsável pelas infrações administrativas as sanções previstas no art. 156 da Lei nº 14.133/2021, conforme segue:

24.2.1. Advertência, quando a CONTRATADA der causa à inexecução parcial, quando não se justificar penalidade mais grave.

24.2.2. Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas b a g, quando não se justificar penalidade mais grave.

24.2.3. Declaração de inidoneidade, quando praticadas as condutas descritas nas alíneas h a l, bem como nas hipóteses mais graves das alíneas b a g.

24.2.4. Multa:

1. Moratória de até 1% (um por cento) por dia de atraso injustificado na disponibilização inicial das licenças ou no restabelecimento da solução em caso de falha crítica, até o limite de 30 (trinta) dias;
2. Compensatória de até 20% (vinte por cento) sobre o valor total do contrato, no caso de inexecução total, ou sobre a parcela inadimplida, no caso de inexecução parcial.

24.3. A aplicação das sanções não exclui a obrigação de reparação integral do dano causado à CONTRATANTE (art. 156, §9º).

24.4. As sanções poderão ser aplicadas cumulativamente com a multa (art. 156, §7º).

24.4.1. Será assegurado o direito à defesa prévia no prazo de 15 (quinze) dias úteis (art. 157).

24.4.2. Caso não haja valores a serem pagos, a multa poderá ser descontada de eventual garantia contratual ou cobrada administrativamente ou judicialmente.

24.4.3. A multa poderá ser recolhida administrativamente no prazo de até 30 (trinta) dias.

24.5. A aplicação das sanções observará processo administrativo com contraditório e ampla defesa, conforme art. 158 da Lei nº 14.133/2021.

24.6. Na aplicação das sanções serão considerados:

- a) natureza e gravidade da infração;
- b) peculiaridades do caso concreto;
- c) circunstâncias agravantes ou atenuantes;
- d) danos causados à Administração;
- e) eventual programa de integridade.



24.7. Os atos que também configurem infrações à Lei nº 12.846/2013 serão apurados conjuntamente (art. 159).

24.8. Poderá haver desconsideração da personalidade jurídica, nos termos do art. 160 da Lei nº 14.133/2021.

24.9. A CONTRATANTE deverá registrar as sanções no CEIS e no CNEP, no prazo legal (art. 161).

24.10. As sanções de impedimento e inidoneidade são passíveis de reabilitação (art. 163).

24.11. As penalidades serão obrigatoriamente registradas no SICAF.

25. OBRIGAÇÕES DA CONTRATADA

Constituem obrigações da CONTRATADA, além daquelas previstas na legislação aplicável, neste Termo de Referência e no contrato, as seguintes:

25.1 Execução do Objeto Contratual

A CONTRATADA obriga-se a executar o fornecimento por subscrição do licenciamento da solução antivírus corporativa em estrita conformidade com as especificações técnicas estabelecidas neste Termo de Referência, observando as boas práticas de gestão de serviços de tecnologia da informação e segurança da informação, assegurando:

I. disponibilização de licenças válidas, originais e autênticas, conforme normas do fabricante, para todas as estações de trabalho e servidores abrangidos pelo contrato;

II. ativação e plena operacionalização da console centralizada de gerenciamento da solução;

III. atualização automática e contínua das assinaturas antivírus e dos mecanismos de detecção e resposta a ameaças;

IV. manutenção da integridade funcional da solução durante toda a vigência contratual, assegurando compatibilidade com os sistemas operacionais suportados pelo fabricante;

V. observância dos níveis mínimos de serviço estabelecidos na Seção 14 – Acordo de Nível de Serviço (SLA);

VI. prestação de suporte técnico especializado durante toda a vigência contratual, incluindo reinstalação de agentes, resolução de conflitos de software e mitigação de incidentes de malware;

VII. correção tempestiva de falhas críticas de segurança identificadas na solução;

VIII. disponibilização de central de atendimento técnico com registro formal de chamados, classificação por severidade e rastreabilidade das ocorrências;



IX. garantia de que a solução fornecida não contenha componentes que possam comprometer a segurança da informação, a privacidade de dados ou a integridade dos sistemas institucionais.

25.2 Faturamento e Documentação

A CONTRATADA deverá apresentar fatura única ao CONTRATANTE, contendo:

- I. identificação clara do período de vigência das licenças;
- II. quantidade total de licenças contratadas;
- III. identificação completa da solução fornecida (fabricante, edição e modalidade de licenciamento);
- IV. evidências de ativação/licenciamento, incluindo relatórios extraídos da console de gerenciamento;
- V. declaração de conformidade com os termos contratuais e com a legislação aplicável.

25.3 Segurança da Informação e Proteção de Dados

A CONTRATADA deverá adotar controles compatíveis com a Política de Segurança da Informação do CONTRATANTE e com a Lei nº 13.709/2018 (LGPD), garantindo:

- I. confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade dos eventos relacionados à solução;
- II. comunicação imediata ao CONTRATANTE sobre incidentes relevantes, incluindo falhas de atualização, indisponibilidade da console de gerenciamento ou vulnerabilidades críticas identificadas;
- III. implementação de medidas corretivas adequadas em caso de incidentes de segurança;
- IV. proteção de dados pessoais eventualmente tratados no contexto da execução contratual;
- V. não utilização ou compartilhamento de informações do CONTRATANTE sem autorização expressa.

25.4 Recebimento do Objeto e Fiscalização

O CONTRATANTE realizará a verificação da conformidade do objeto entregue, comunicando formalmente eventuais imperfeições, falhas ou irregularidades para correção.

§1º O acompanhamento e a fiscalização contratual poderão ser realizados por servidor ou comissão formalmente designada.

§2º A fiscalização deverá garantir a rastreabilidade das etapas de execução contratual, registros técnicos e evidências necessárias à comprovação do atendimento das obrigações pactuadas, conforme arts. 116 e 117 da Lei nº 14.133/2021.



§3º A CONTRATADA deverá disponibilizar acesso às evidências necessárias à fiscalização contratual sempre que solicitado pelo CONTRATANTE ou por órgãos de controle.

25.5 Comunicação e Atendimento

A CONTRATADA deverá:

- I. responder às solicitações do CONTRATANTE no prazo máximo de 48 horas;
- II. comunicar formalmente alterações de endereço, contatos ou responsáveis técnicos;
- III. reportar imediatamente qualquer irregularidade que possa comprometer a execução contratual ou a segurança da informação institucional;
- IV. manter registro formal dos incidentes relevantes e das interações técnicas realizadas durante a execução contratual.

25.6 Continuidade da Proteção Tecnológica

A CONTRATADA deverá assegurar, durante toda a vigência contratual:

- I. funcionamento regular da console de gerenciamento;
- II. validade contínua das licenças fornecidas;
- III. atualização permanente da base de proteção e dos mecanismos antivírus;
- IV. manutenção da cobertura de proteção contra ameaças digitais compatível com as funcionalidades contratadas.

25.7 Gestão de Incidentes de Segurança

A CONTRATADA deverá tratar incidentes de segurança conforme níveis de severidade definidos na Seção 14 – SLA, comunicando imediatamente ao CONTRATANTE a ocorrência de incidentes graves que possam impactar sistemas institucionais ou dados protegidos, acompanhados das medidas adotadas para mitigação.

25.8 Manutenção das Condições de Habilitação

Durante toda a execução contratual, a CONTRATADA deverá manter:

- I. regularidade fiscal, trabalhista e previdenciária;
- II. qualificação técnica compatível com o objeto contratado;
- III. capacidade operacional adequada à execução do objeto;
- IV. autorização válida do fabricante para comercialização ou licenciamento da solução, quando aplicável.



Parágrafo único. A CONTRATADA é integralmente responsável pelos encargos decorrentes do fornecimento das licenças e do suporte técnico associado, bem como por danos causados à Administração ou a terceiros por culpa ou dolo, nos termos do art. 122 da Lei nº 14.133/2021.

25.9 Sigilo e Proteção de Informações

A CONTRATADA deverá guardar sigilo sobre informações obtidas em razão da execução contratual, garantindo:

- I. confidencialidade e integridade das informações institucionais;
- II. proteção contra acesso não autorizado ou uso indevido;
- III. devolução ou eliminação segura de informações eventualmente acessadas ao término da vigência contratual, quando aplicável.

25.10 Compliance, Integridade e Auditoria

A CONTRATADA deverá observar normas de integridade e prevenção a fraudes aplicáveis à Administração Pública, comunicando formalmente ao CONTRATANTE qualquer irregularidade identificada na execução contratual.

§1º O CONTRATANTE poderá realizar auditorias técnicas sobre a execução do objeto contratado.

§2º A CONTRATADA deverá disponibilizar registros e evidências necessárias à auditoria, inclusive junto ao fabricante da solução, quando aplicável.

25.11 Sanções Administrativas

O descumprimento das obrigações previstas neste Termo de Referência poderá ensejar aplicação das sanções administrativas previstas na Lei nº 14.133/2021, observados o contraditório e a ampla defesa.

25.12 Das Vedações à contratada

25.12.1. São expressamente vedadas à CONTRATADA:

- 25.12.1.1 A contratação de servidor pertencente ao quadro de pessoal da CONTRATANTE, durante a vigência do contrato;
- 25.12.1.2 A veiculação de publicidade acerca do, salvo se houver prévia autorização da CONTRATANTE;
- 25.12.1.3 A subcontratação de outra empresa para a execução total ou parcial do objeto do contrato.
- 25.12.1.4 Caucionar ou utilizar o contrato para qualquer operação financeira.



25.12.1.5 Interromper a execução dos serviços sob alegação de impedimento por parte da CONTRATANTE, salvo nos casos previstos em lei.

25.12.1.6 O objeto da licitação não demanda alta especialização técnica ou complexidade. Assim sendo, não é permitida a participação de consórcios, com base na análise de que a participação isolada de empresas é suficiente para atender a singularidade do objeto licitado.

25.13 Condições de Pagamento

O pagamento será realizado conforme as condições estabelecidas neste Termo de Referência e no contrato, após a verificação do atendimento das condições de recebimento do objeto.

26. OBRIGAÇÕES DO CONTRATANTE

Constituem obrigações do CONTRATANTE, além daquelas previstas na legislação aplicável e no instrumento contratual, as seguintes:

26.1 Comunicação institucional

Informar à CONTRATADA quaisquer alterações relevantes na infraestrutura tecnológica que possam interferir direta ou indiretamente na execução do objeto contratual, especialmente aquelas relacionadas a:

- domínio institucional;
- rede corporativa;
- servidores;
- políticas institucionais de segurança da informação;
- outras alterações que possam impactar o funcionamento da solução contratada.

26.2 Providências administrativas e técnicas

Adotar as providências administrativas e técnicas necessárias à adequada execução do objeto contratual, incluindo:

- disponibilização de conectividade compatível com a solução contratada;
- concessão das permissões administrativas necessárias à validação e operação da solução;
- manutenção de ambiente tecnológico compatível com os requisitos técnicos do licenciamento contratado.



26.3 Gestão das solicitações contratuais

Formalizar, por intermédio do gestor do contrato, eventuais solicitações de ajustes operacionais necessários à execução do objeto, assegurando rastreabilidade administrativa e observância ao escopo contratado, sem alteração das características essenciais da solução.

26.4 Gestão e fiscalização contratual

Designar formalmente gestor e fiscais do contrato, nos termos do art. 117 da Lei nº 14.133/2021, responsáveis pelo acompanhamento e verificação da execução contratual.

Compete à equipe de fiscalização:

- acompanhar a disponibilidade operacional da solução;
- verificar a atualização contínua dos mecanismos de proteção;
- analisar relatórios técnicos extraídos da console de gerenciamento;
- verificar o cumprimento dos níveis de serviço estabelecidos no Acordo de Nível de Serviço (SLA).

26.5 Aceite técnico do objeto

Realizar o aceite técnico do objeto após a verificação:

- da ativação das licenças no ambiente institucional;
- da continuidade operacional da solução no ambiente tecnológico existente;
- da conformidade com os requisitos técnicos estabelecidos neste Termo de Referência.

O prazo para realização do aceite técnico será de até **10 (dez) dias úteis**, contados da disponibilização da solução pela CONTRATADA.

26.6 Autorização de pagamento

Autorizar o pagamento à CONTRATADA somente após:

- emissão do termo de recebimento definitivo;
- comprovação da ativação regular das licenças;
- verificação da conformidade da execução com as condições contratuais.

26.7 Gestão de acessos administrativos

Informar à CONTRATADA os usuários institucionais autorizados a exercer funções administrativas no console de gerenciamento da solução, utilizando preferencialmente identificação funcional e e-mail institucional.



26.8 Segurança da informação

Cumprir e fazer cumprir as políticas institucionais de segurança da informação aplicáveis ao ambiente tecnológico, incluindo:

- controle de acesso;
- atualização de sistemas;
- uso seguro da rede corporativa;
- observância às diretrizes da Estratégia de Governo Digital e demais normativos institucionais vigentes aplicáveis à contratação.

27. CRONOGRAMA DE CONTRATAÇÃO E CONTINUIDADE DA OPERAÇÃO

27.1 Premissas

Constituem premissas para início da execução contratual:

- assinatura do contrato administrativo;
- emissão da Ordem de Serviço;
- disponibilização das licenças renovadas;
- manutenção da disponibilidade do ambiente tecnológico do CONTRATANTE.

27.2 Etapas da Contratação do Licenciamento

Fase	Descrição	Responsável	Prazo
1	Emissão da Ordem de Serviço	Município	Dia 0
2	Disponibilização das licenças renovadas	CONTRATADA	Até D+5
3	Validação técnica da console existente	Município	Até D+10
4	Confirmação da continuidade operacional	Município/CONTRATADA	Até D+08

27.3 Início da Operação Contratual

A operação contratual terá início:

- na data do Termo de Aceite Definitivo; ou
- automaticamente com a disponibilização das licenças renovadas em ambiente produtivo validado pela fiscalização contratual.



Para fins de caracterização do início da execução contratual, considerar-se-á como marco inicial da prestação efetiva dos serviços a continuidade operacional comprovada da solução já implantada, sem interrupção da proteção dos ativos digitais institucionais.

28. CRITÉRIO DE SELEÇÃO DA PROPOSTA

O critério de seleção do fornecedor será o de menor preço global, desde que atendidas integralmente as especificações técnicas, requisitos de desempenho e condições estabelecidas neste Termo de Referência, observando-se o julgamento objetivo da proposta, bem como os princípios da legalidade, impessoalidade, moralidade, publicidade, eficiência, economicidade e vantajosidade da contratação para a Administração Pública, em conformidade com a Lei nº 14.133/2021.

DOS CRITÉRIOS DE AVALIAÇÃO DE PROPOSTA E SELEÇÃO DO FORNECEDOR:

28.1. A proposta da CONTRATADA deverá atender integralmente as especificações contidas neste Termo de Referência.

28.2. O fornecedor será selecionado por meio da realização de procedimento de CONTRATAÇÃO DIRETA, na forma de DISPENSA DE LICITAÇÃO, com adoção do critério de julgamento pelo MENOR PREÇO GLOBAL.

28.3. Será adotado tratamento diferenciado a microempresas (ME) e empresas de pequeno porte (EPP), de acordo com o disposto no art. 48, I, da Lei Complementar nº 123, de 2006 (atualizada pela LC n. 147/2014), de maneira que seja destinado exclusivamente à participação de microempresa e empresas de pequeno porte os itens de contratação cujo valor seja de até R\$ 80.000,00 (oitenta mil reais).

28.4. Entretanto, tendo em vista o que estabelece os arts 47 a 49 da referida Lei, os itens cotados acima de R\$ 80.000,00 (oitenta mil reais) terão percentual destinado de até 25% (vinte e cinco por cento), para a participação de ME e/ou EPP's.

28.5. A exclusividade da participação de microempresa e empresas de pequeno porte poderá ser justificadamente excepcionada de acordo com o Art. 49, incisos II e III, da Lei Complementar 123/2006, quando:

28.5.1. Não houver o mínimo de 3 (três) fornecedores competitivos enquadrados como microempresas ou empresas de pequeno porte sediados local ou regionalmente e capazes de cumprir as exigências estabelecidas no instrumento convocatório.

28.5.2. O tratamento diferenciado e simplificado para as microempresas e as empresas de pequeno porte não for vantajoso para a administração pública ou representar prejuízo ao conjunto ou complexo do objeto a ser contratado, justificadamente.

28.6. Não poderão participar do processo de Licitação os interessados:



28.6.1. Proibidos de participar de licitações e celebrar contratos administrativos, na forma da legislação vigente;

28.6.2. Que não atendam às condições estabelecidas neste Termo de Referência;

28.6.3. Estrangeiros que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente;

28.6.4. Que se enquadrem nas vedações previstas no artigo 14º da Lei Federal nº 14.133/21.

28.7. Previamente à celebração do contrato, a Administração verificará o eventual descumprimento das condições para contratação, especialmente quanto à existência de sanção que a impeça, mediante a consulta a cadastros informativos oficiais, tais como:

- a) SICAF;
- b) Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União;
- c) Cadastro Nacional de Empresas Punidas - CNEP, mantido pela Controladoria-Geral da União.

28.8. A consulta aos cadastros será realizada em nome da empresa fornecedora e também de seu sócio majoritário, por força do artigo 12 da Lei nº 8.429, de 1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.

28.9. Caso conste na Consulta de Situação do Fornecedor a existência de Ocorrências Impeditivas Indiretas, o gestor diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

28.10. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.

28.11. O fornecedor será convocado para manifestação previamente a uma eventual negativa de contratação.

28.12. Caso atendidas as condições para contratação, a habilitação do fornecedor será verificada por meio do SICAF, nos documentos por ele abrangidos.

28.13. O agente de contratação poderá, quando julgar necessário, exigir do licitante que seja encaminhado pelo sistema, dentro do prazo especificado, os documentos de habilitação digitalizados, mesmo que o licitante tenha apresentado o registro no Sistema de Cadastramento Unificado de Fornecedores (SICAF), para comprovação das condições de habilitação exigidas neste instrumento e no Edital.



28.13.1. A não apresentação dos documentos solicitados no prazo estabelecido implicará na inabilitação do licitante.

28.14. É dever do fornecedor manter atualizada a respectiva documentação constante do SICAF, ou encaminhar, quando solicitado pela Administração, a respectiva documentação atualizada.

28.15. Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.

28.16. Se o fornecedor for a matriz, todos os documentos deverão estar em nome da matriz, e se o fornecedor for a filial, todos os documentos deverão estar em nome da filial, exceto para atestados de capacidade técnica, caso exigidos, e no caso daqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

28.17. Serão aceitos registros de CNPJ de fornecedor matriz e filial com diferenças de números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

28.18. Da Habilitação Jurídica:

28.18.1. Cédula de Identidade do responsável Legal.

28.18.2. Conforme o tipo societário serão exigidos os itens na seguinte forma:

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

28.18.2.2. 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>; ou

28.18.2.3. 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; ou

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

28.18.2.5. Decreto de autorização, em se tratando de empresa ou sociedades estrangeiras em funcionamento no País, e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir.



28.18.3. Prova de registro, arquivamento ou inscrição na Junta Comercial, no Registro Civil de Pessoas Jurídicas ou em repartições competentes, do ato constitutivo, estatuto ou contrato social em vigor, bem como da ata de eleição do termo de investidura dos representantes legais da pessoa jurídica.

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

28.19. Habilitações Fiscal, Social e Trabalhista:

28.19.1. Prova de inscrição no Cadastro Nacional da Pessoa Jurídica (CNPJ);

28.19.2. 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 02/10/2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional;

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

28.19.4. 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;

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

28.19.5.1. 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;

28.19.6. Certidão de Regularidade da Fazenda Municipal, da sede do proponente;

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

28.19.7.1. Caso o fornecedor seja considerado isento dos tributos estaduais ou distritais relacionados ao objeto, deverá comprovar tal condição mediante a apresentação de certidão ou



declaração da Fazenda respectiva do seu domicílio ou sede, ou por meio de outro documento equivalente, na forma da respectiva legislação de regência.

28.20. Da Qualificação Técnica:

28.20.1. Comprovação de aptidão para o fornecimento de bens similares de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso.

28.20.1.1. A comprovação de capacidade técnica, deverá ser realizada por meio da apresentação de atestado fornecido por pessoa jurídica de direito público ou privado, que comprove ter a licitante cumprido, de forma satisfatória, a execução de objeto compatível ou com complexidade superior ao especificado neste Termo de Referência, com clara menção da execução bem-sucedida, relativamente ao cumprimento de prazos, especificações e qualidade.

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

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

28.20.3. Não será admitida a apresentação de atestado de capacidade técnica emitido por empresa ou empresas do mesmo grupo econômico em favor da licitante participante, no caso desta também pertencer ao grupo econômico.

28.20.4. Os atestados ou certidões recebidas estão sujeitos à verificação do Agente de Contratação e da sua Equipe de Apoio quanto à veracidade dos respectivos conteúdos, inclusive para os efeitos previstos nos artigos 169, § 3º, inciso II, da Lei Federal nº 14.133/2021, e 337-F do Código Penal.

28.21. Das Declarações:

28.21.1. Declaração de que não emprega cônjuges, companheiros ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, de servidores do Município de Cabo Frio-RJ, em cumprimento aos requisitos do artigo 9º, §1º, da Lei nº 14.133/21.

28.21.2. Declaração de que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos,



salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7º, XXXIII, da Constituição Federal.

28.22. Não serão aceitos como documentação hábil a suprir exigências deste Termo de Referência pedidos de inscrição, protocolos, cartas ou qualquer outro documento que visem a substituir os exigidos, exceto nos casos admitidos pela legislação.

28.23. Sem prejuízo dos requisitos minuciosamente especificados nos itens anteriores, o fornecedor deverá atentar para as disposições contidas nos artigos 62 a 70 da Lei Federal nº 14.133/21, sendo vedado alegar desconhecimento dos critérios estabelecidos para o fiel cumprimento das obrigações previstas.

29. FORMA DE ENTREGA DO OBJETO

A entrega do objeto ocorrerá em **parcela única**, mediante disponibilização das licenças contratadas, ativação da console de gerenciamento, parametrização inicial da solução e validação técnica do funcionamento do ambiente de proteção corporativa.

30. SUBCONTRATAÇÃO

Não será admitida a subcontratação do objeto principal da presente contratação, considerando a natureza especializada da solução, a existência de dependência tecnológica em relação ao fabricante e a necessidade de preservação da integridade técnica, da segurança da informação e da continuidade operacional do serviço contratado.

Admite-se, exclusivamente, a participação eventual e acessória do fabricante da solução ou de seus canais oficialmente autorizados, quando indispensável à prestação de suporte técnico especializado de níveis avançados, atualização tecnológica, correções evolutivas, manutenção da compatibilidade com a infraestrutura do fornecedor originário ou atendimento a requisitos técnicos que dependam de intervenção direta do detentor da tecnologia.

Nessas hipóteses, a eventual participação do fabricante não caracteriza subcontratação do objeto principal, permanecendo integralmente sob responsabilidade da CONTRATADA:

- a execução do objeto contratual;
- o cumprimento dos níveis mínimos de serviço estabelecidos;
- a observância dos requisitos de segurança da informação;
- a garantia de continuidade da prestação do serviço;
- o atendimento às obrigações contratuais perante a Administração.

Fica vedada, em qualquer hipótese, a transferência da execução do núcleo essencial do objeto contratado a terceiros estranhos à relação contratual, especialmente quando tal transferência possa comprometer a governança contratual, a rastreabilidade das atividades executadas, a responsabilização técnica ou a segurança institucional dos dados tratados.



A presente vedação fundamenta-se:

- no princípio da responsabilidade integral da contratada pela execução do objeto;
- na natureza contínua e crítica do serviço contratado;
- na dependência tecnológica inerente à solução;
- na necessidade de manutenção do controle administrativo sobre a execução contratual;
- e nas boas práticas de governança recomendadas pelos órgãos de controle externo em contratações de soluções tecnológicas especializadas.

Eventual participação do fabricante deverá ocorrer apenas quando tecnicamente justificada, devidamente registrada pela fiscalização contratual e restrita às atividades acessórias indispensáveis à adequada execução do objeto.

31. PARTICIPAÇÃO DE CONSÓRCIO

Não será admitida a participação de empresas reunidas em consórcio na presente contratação.

A vedação fundamenta-se na natureza do objeto contratado, que consiste em solução tecnológica especializada, de execução integrada, com dependência técnica do fornecedor da plataforma e necessidade de manutenção de responsabilidade contratual centralizada, fatores que exigem interlocução técnica única e gestão operacional unificada durante toda a execução contratual.

Adicionalmente, a formação de consórcio, no presente caso, não ampliaria a competitividade nem traria benefícios técnicos ou econômicos à Administração, considerando:

- a existência de fornecedor tecnicamente apto à execução integral do objeto de forma individual;
- a natureza integrada e contínua da prestação do serviço;
- a necessidade de preservação da governança contratual;
- a criticidade institucional da solução;
- e a dependência tecnológica inerente ao ambiente operacional da plataforma.

A admissão de consórcio, nessas condições, poderia introduzir riscos desnecessários à coordenação técnica da execução contratual, à responsabilização objetiva da contratada e à rastreabilidade das atividades executadas, sem contrapartida de vantagem para a Administração.

A presente vedação observa as boas práticas de planejamento da contratação pública previstas na Lei nº 14.133/2021 e encontra-se alinhada às orientações dos órgãos de controle externo quanto à necessidade de justificativa técnica para admissão ou restrição da participação em consórcio, especialmente em contratações com solução tecnológica proprietária ou com execução centralizada pelo fornecedor.



32. GARANTIA CONTRATUAL

Nos termos do art. 96 da Lei nº 14.133/2021, não será exigida garantia contratual para a presente contratação.

A dispensa fundamenta-se na análise das características do objeto e do modelo de execução contratual, especialmente:

- na natureza continuada e monitorada da prestação do serviço;
- na existência de níveis mínimos de serviço (SLA) sujeitos à verificação pela fiscalização contratual;
- no pagamento condicionado ao recebimento definitivo da solução;
- na responsabilidade integral da contratada pela execução do objeto;
- na reduzida exposição da Administração ao risco de inadimplemento contratual;
- na dependência tecnológica do fornecedor da solução;
- e na inexistência de benefícios técnicos ou econômicos relevantes decorrentes da exigência de garantia.

Adicionalmente, a exigência de garantia contratual, no presente caso, não se mostra proporcional ao risco da contratação nem necessária à proteção do interesse público, podendo representar apenas ônus administrativo adicional sem ganho efetivo de segurança contratual.

A decisão administrativa observa os princípios da proporcionalidade, eficiência, economicidade e adequação ao risco da contratação, conforme previsto na Lei nº 14.133/2021 e nas boas práticas de governança recomendadas pelos órgãos de controle externo.

33. ADEQUAÇÃO ORÇAMENTÁRIA

As despesas decorrentes da presente contratação correrão à conta de dotação orçamentária própria consignada no orçamento vigente da Secretaria Municipal de Fazenda, em conformidade com a Lei nº 4.320/1964 e com a Lei Complementar nº 101/2000, observadas as regras de responsabilidade fiscal, planejamento e equilíbrio das contas públicas.

A despesa encontra-se devidamente classificada na estrutura programática institucional, conforme segue:

- **Programa de Trabalho:** 02.006.04.126.0002.2.016
- **Natureza da Despesa:** 3.3.90.40
- **Ficha:** 1388
- **Fonte de Recursos:** 1704

O enquadramento orçamentário acima demonstra a compatibilidade da contratação com as ações de manutenção e sustentação da infraestrutura tecnológica institucional



necessária ao funcionamento dos sistemas corporativos da Secretaria Municipal de Fazenda.

O presente registro orçamentário está alinhado ao planejamento administrativo da unidade demandante e destina-se a viabilizar a Contratação do licenciamento da solução de segurança corporativa utilizada na proteção dos ativos digitais, garantindo:

- continuidade operacional dos sistemas estruturantes;
- integridade e disponibilidade das informações institucionais;
- manutenção das políticas de segurança da informação;
- mitigação de riscos cibernéticos no ambiente tecnológico da Secretaria.

A indicação da dotação orçamentária observa as boas práticas de planejamento da contratação pública previstas na Lei nº 14.133/2021 e constitui requisito formal para a adequada instrução dos documentos subsequentes da fase preparatória da contratação.

34. ELABORAÇÃO DO TERMO DE REFERÊNCIA

O presente Termo de Referência foi elaborado pelos servidores abaixo identificados, responsáveis pelo planejamento da contratação e pela consolidação das informações técnicas necessárias à instrução do processo administrativo.

- 1) **LEANDRO MACEDO TRINDADE** Matrícula 801665
- 2) **MARCELO ALVARO DE ALBERNAZ JÚNIOR** Portaria 324/2025
- 3) **RODRIGO DE ABREU COSTA** Matrícula 66865

Compete aos responsáveis pela elaboração:

- definir as especificações técnicas do objeto;
- justificar a necessidade da contratação;
- indicar os parâmetros técnicos e operacionais da solução;
- assegurar a aderência às normas legais e regulamentares aplicáveis.

Cabo Frio, 27 de Maio de 2026

Responsáveis pelo planejamento

Documento assinado digitalmente
gov.br LEANDRO DE MACEDO TRINDADE
Data: 01/06/2026 16:06:10-0300
Verifique em <https://validar.iti.gov.br>

LEANDRO MACEDO TRINDADE
Matrícula 801665

Documento assinado digitalmente
gov.br MARCELO ALVARO DE ALBERNAZ JUNIOR
Data: 01/06/2026 16:12:05-0300
Verifique em <https://validar.iti.gov.br>

**MARCELO ALVARO DE
ALBERNAZ JÚNIOR**
Portaria 324/2025

Documento assinado digitalmente
gov.br RODRIGO DE ABREU COSTA
Data: 01/06/2026 16:48:47-0300
Verifique em <https://validar.iti.gov.br>

**RODRIGO DE ABREU
COSTA**
Matrícula 66865



35. APROVAÇÃO DO TERMO DE REFERÊNCIA

Nos termos da legislação vigente e considerando a regular instrução processual, **aprovo o presente Termo de Referência e autorizo o prosseguimento da contratação**, na modalidade de inexigibilidade de licitação, com fundamento no art. 75, inciso II, da Lei Federal nº 14.133/2021.

Cabo Frio/RJ, 01 de junho de 2026.

KLEBER FERREIRA DE SOUZA
Secretário Municipal de Fazenda
Ordenador de Despesas



KLEBER FERREIRA DE SOUZA
Secretário de Fazenda



ANEXO I – PLANILHA DE PREÇOS

Item	Unid.	Quant.	Descrição	Valor Unitário (36 meses)	Valor Unitário Anual	Valor Total Anual	Valor Total (36 meses)
1	Unidade	136	Contratação do licenciamento de uso da solução corporativa de proteção de endpoints Bitdefender GravityZone Business Security Enterprise, com console de gerenciamento centralizado em nuvem (Cloud Console), disponibilizada no modelo Software como Serviço (SaaS), incluindo atualização automática de assinaturas, gerenciamento remoto dos endpoints protegidos, suporte técnico especializado e direito às atualizações oficiais do fabricante pelo período de 36 (trinta e seis) meses para estações de trabalho.				
2	Unidade	20	Contratação do licenciamento de uso da solução corporativa de proteção de endpoints Bitdefender GravityZone Business Security Enterprise, com console de gerenciamento centralizado em nuvem (Cloud Console), disponibilizada no modelo Software como Serviço (SaaS), incluindo atualização automática de assinaturas, gerenciamento remoto dos endpoints protegidos, suporte técnico especializado e direito às atualizações oficiais do fabricante pelo período de 36 (trinta e seis) meses para servidores.				



ANEXO II - RELATÓRIO DE PRESTAÇÃO DE CONTAS

Cliente: **Prefeitura de Cabo Frio**

Período de apuração: ____/____/20____ a ____/____/20____

RELATÓRIO DE FATURAMENTO - ÚNICO

Item faturável	Valor unitário (R\$)	Quantidade	Valor total (R\$)
Contratação do licenciamento de uso da solução corporativa de proteção de endpoints Bitdefender GravityZone Business Security Enterprise, com console de gerenciamento centralizado em nuvem (Cloud Console), disponibilizada no modelo Software como Serviço (SaaS), incluindo atualização automática de assinaturas, gerenciamento remoto dos endpoints protegidos, suporte técnico especializado e direito às atualizações oficiais do fabricante pelo período de 36 (trinta e seis) meses para estações de trabalho.	R\$	136	R\$
Contratação do licenciamento de uso da solução corporativa de proteção de endpoints Bitdefender GravityZone Business Security Enterprise, com console de gerenciamento centralizado em nuvem (Cloud Console), disponibilizada no modelo Software como Serviço (SaaS), incluindo atualização automática de assinaturas, gerenciamento remoto dos endpoints protegidos, suporte técnico especializado e direito às atualizações oficiais do fabricante pelo período de 36 (trinta e seis) meses para servidores.	R\$	20	R\$
Subtotal mensal dos serviços			R\$
Desconto apurado por descumprimento de Níveis de Serviço (SLA)			(-) R\$
Valor final para faturamento			R\$

Observações técnicas

- O faturamento será realizado em pagamento único, após disponibilização das licenças.
- Todos os valores devem estar em conformidade com a Planilha de Preços (Anexo I).