

Minuta de Contrato regida pela Lei Federal 14.133/2021

**CONTRATO DE AQUISIÇÃO DE LICENÇAS DE
ANTIVÍRUS E SUÍTE DE SEGURANÇA PARA
ESTAÇÕES DE TRABALHO E SERVIDORES
WINDOWS E LINUX, INCLUINDO TREINAMENTO,
SERVIÇOS DE SUPORTE 24X7 E ATUALIZAÇÕES
DE VERSÃO POR 12 (DOZE) MESES, QUE ENTRE
SI CELEBRAM [nome do contratante] – E A
[contratada]**

PROCESSO ADMINISTRATIVO XXXXXXXXX

PROCESSO LICITATÓRIO Nº XXXXXXXXX

PREGÃO ELETRÔNICO Nº XXXXX/XXXX

ATA DE REGISTRO DE PREÇOS Nº XXX/XXXXX

A *[Nome do Participante]*, estabelecida na *[endereço completo]*, CNPJ nº *[nº do CNPJ]*, doravante denominada **CONTRATANTE**, neste ato representada por *[Cargo e Responsável Legal da Entidade]*, e a *[Razão social da CONTRATADA]*, CNPJ/MF nº *[nº do CNPJ]*, estabelecida na *[endereço completo]*, neste ato representada por seu Representante Legal *[nome completo do Representante Legal]*, CPF nº *[nº do CPF]*, doravante denominada **CONTRATADA**, celebram, em decorrência da Ata de Registro de Preços xxxxxxxx, o presente Contrato, conforme cláusulas e condições a seguir especificadas, reciprocamente estipuladas e aceitas. Este Contrato vincula-se ao Edital de Licitação Pregão Eletrônico xxxxxxxx parte integrante deste instrumento independente de transcrição e é regulado pelas suas cláusulas e pelas Leis Federais 14.133/2021, 12.846/2013 e Decretos Municipais 11.245/2003, 18.096/2022.

1. DO OBJETO

- 1.1. Constitui objeto do presente instrumento a aquisição de licenças de antivírus e suíte de segurança para estações de trabalho e servidores Windows e Linux, incluindo treinamento, serviços de suporte 24x7 e atualizações de versão por 12 (doze) meses, conforme detalhado neste Contrato, em seu Anexo I e no Termo de Referência.

2. ESPECIFICAÇÃO DO OBJETO

2.1. A CONTRATADA deverá fornecer o objeto deste Contrato conforme especificações descritas no Anexo I deste instrumento e no quadro abaixo:

LOTE 1			
Item	Descrição	Unidade de Medida	Quantidade
1	Licença de antivírus e suíte de segurança para estações de trabalho e servidores Windows e Linux com suporte no regime 24x7.	UN	XXX
2	Treinamento Hands-on (por participante)	UN	XXX

3. DAS CONDIÇÕES DE RECEBIMENTO DO OBJETO

3.1. O objeto que trata este Contrato será recebido conforme especificações técnicas, destacando-se o seguinte:

- 3.1.1. **Provisoriamente**, para efeito de posterior verificação da sua conformidade com as especificações e quantidades no prazo de 05 (cinco) dias úteis a contar da data do recebimento dos equipamentos pela CONTRATANTE;
- 3.1.2. **Definitivamente**, após a verificação da observância pela CONTRATADA à integralidade das condições estabelecidas no Anexo I deste termo, incluindo o treinamento.
- 3.1.3. Os itens que compõem o objeto devem ser novos, sem uso anterior e compatíveis com as especificações técnicas deste contrato;
- 3.1.4. Poderão ser realizados testes pela CONTRATANTE ou equipe por ela indicada para averiguação do cumprimento da especificação técnica, no prazo de até 10 (dez) dias úteis contados da entrega, após o que será emitido o Termo de Aceite Definitivo e o respectivo ateste da Nota Fiscal;
- 3.1.5. Encontrando irregularidades, o produto deverá ser reparado no prazo de até 10 (dez) dias corridos, contados da data da notificação

pela CONTRATANTE. Aprovado, será(ão) recebido(s) definitivamente, mediante ateste aposto na Nota Fiscal respectiva.

- 3.1.6. A CONTRATADA é obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o item do objeto em que se verificarem vícios, defeitos ou incorreções.

4. DA VIGÊNCIA

- 4.1. O prazo de vigência deste Contrato será de xx (xxxxxxxxxx) meses, sem prejuízo da garantia, contados da data de sua assinatura.
- 4.2. Respeitados os limites da Lei 14.133/2021, o presente contrato poderá ser prorrogado, por acordo entre as partes.

5. DA EXECUÇÃO DO OBJETO

- 5.1. Licenciamento:
- 5.1.1. A solução deverá ser fornecida, em sua versão mais atual, disponibilizada no mercado, pelo fabricante.
- 5.1.2. A CONTRATADA deverá disponibilizar token ou arquivo de ativação da licença da solução contratada por meio eletrônico (link para download) sem ônus para a CONTRATANTE.
- 5.1.3. O objeto deverá ser entregue, conforme Especificação Técnica detalhada no ANEXO I deste Contrato.
- 5.1.4. O treinamento online para 10 (dez) pessoas, em tempo real, no idioma Português, sendo gravado e disponibilizado a gravação ao final do treinamento, com carga horária mínima de 24 horas/aula. O treinamento deverá receber dos alunos avaliação média mínima de 60% relativos aos itens: conteúdo programático, material didático (apostila, vídeos, etc.), didática do instrutor, conhecimento técnico do instrutor. Caso a avaliação do treinamento seja inferior a 60%, o treinamento deverá ser aplicado novamente para os mesmos alunos

6. DO PRAZO DE ENTREGA

- 6.1. O prazo máximo para disponibilização do objeto contratado é de até 45 (quarenta e cinco) dias corridos, contados a partir do recebimento pela CONTRATADA da NOTA DE EMPENHO, devidamente assinada pela CONTRATANTE.
- 6.2. A solução deverá ser entregue mediante Nota Fiscal de Venda, de acordo com as especificações técnicas do ANEXO I, deste contrato.

7. DO LOCAL DE ENTREGA

- 7.1. Em caso de entrega física, a CONTRATADA deverá realizar a entrega do objeto no endereço xxx.
- 7.2. Entregas eletrônicas deverão ser realizadas no email fornecido pela contratante
- 7.3. É necessário realizar aviso de entrega, com antecedência de 48 (quarenta e oito) horas, agendando data e horário, sob pena de não recebimento por parte da CONTRATANTE.

8. DAS CONDIÇÕES DE GARANTIA E ASSISTÊNCIA TÉCNICA DO OBJETO

- 8.1. Garantir o suporte e apoio técnico para instalação e configuração da solução e o atendimento para manutenção corretiva e identificação de falhas ou inconsistências detectadas no objeto, incluindo ainda, o esclarecimento de dúvidas, de forma a garantir o funcionamento da solução por toda a vigência contratual;
- 8.2. Também é responsabilidade da CONTRATADA, durante o período de garantia, promover:
 - 8.2.1. Correções de segurança;
 - 8.2.2. Atualizações necessárias ao funcionamento da solução.
- 8.3. A CONTRATADA deverá proceder à substituição, reparo ou correção no prazo máximo de 15 (quinze) dias corridos, contados do recebimento da notificação respectiva que também poderá ser enviada por e-mail, sem prejuízo da aplicação das sanções previstas na Lei, Decreto, Regulamento de Licitações e Contratos da CONTRATANTE e no código de Defesa do Consumidor.
- 8.4. A CONTRATADA deverá garantir o pleno funcionamento do objeto durante toda a vigência contratual.

9. DO SLA

- 9.1. As solicitações da CONTRATANTE deverão ser resolvidas nos prazos previstos na tabela do item 9.2 deste contrato.
- 9.2. Os prazos de resolução dos incidentes a serem cumpridos pela CONTRATADA para os atendimentos aos incidentes/eventos são:

Tabela: Prazos de resolução dos incidentes.

Severidade	Classificação	Prazo para primeiro atendimento
Emergencial	São consideradas como tipo "Emergencial" todas as falhas cujas consequências geram indisponibilidade do serviço da solução e/ou degradação severa de tráfego e/ou recursos.	Até 4 (quatro) horas corridas, contados da abertura da solicitação.
Grave	Problemas que não geram indisponibilidade do ambiente, mas que reduzem ou inibem alguma funcionalidade da solução.	Até 8 (oito) horas, contados da abertura da solicitação.
Informação	Solicitação de informações sobre o funcionamento da solução, configurações ou orientações.	Até 5 (cinco) dias corridos, contados da abertura da solicitação.

9.2.1. A severidade classificada como INFORMAÇÃO contempla o atendimento por parte da CONTRATADA quanto a novas configurações técnicas que a CONTRATANTE queira realizar na solução durante a vigência contratual.

9.2.1.1. A CONTRATADA poderá orientar os técnicos da CONTRATANTE em todo o passo a passo para implementar a solicitação requerida.

9.2.1.2. Caso a solicitação da CONTRATANTE não seja suportada pela solução adquirida, deverá a CONTRATADA elencar todos os motivos e indicar possível solução que execute a tarefa solicitada.

9.2.2. A CONTRATADA poderá solicitar a dilação dos prazos previstos na tabela acima, justificando com detalhes o motivo da impossibilidade de cumprimento.

9.2.3. Caberá a CONTRATANTE analisar as solicitações de dilação de prazo apresentadas pela CONTRATADA, deferindo-as ou não, sujeitando-a à aplicação das penalidades cabíveis nos casos em que se verifique o descumprimento contratual.

9.2.4. Um chamado só poderá ser reclassificado pela CONTRATADA se houver entendimento e concordância por parte da CONTRATANTE. Caso contrário, a severidade deve levar em conta o fator que foi usado na sua abertura e seguir esse mesmo critério até a sua completa solução.

10. DO PREÇO

10.1. Pelo objeto contratado a CONTRATANTE pagará à CONTRATADA o valor global de R\$XX (XXXXXXX) conforme tabela abaixo:

Item	Descrição / Especificação	Unidade	Qtde	Valor Unitário	Valor Total
1	Licença de antivírus e suíte de segurança para estações de trabalho e servidores Windows e Linux com suporte no regime 24x7.	UN	X	R\$XX,XX	R\$XX,XX
2	Treinamento Hands-on (por participante)	UN	x	R\$XX,XX	R\$XX,XX

10.2. Estão consideradas no preço previsto no 10.1. todas as despesas diretas e indiretas decorrentes da execução contratual, 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.

11. DA FORMA DE PAGAMENTO

- 11.1. O pagamento será realizado pela CONTRATANTE em até 30 (trinta) dias corridos contados do adimplemento da obrigação. Considera-se adimplida a obrigação, a entrega do objeto com seu aceite definitivo pela CONTRATANTE.
- 11.2. Os itens deverão ser entregues mediante apresentação da Nota Fiscal, de acordo com as especificações deste Contrato e ANEXO I.
- 11.3. No preço apresentado deverá estar incluído todos os custos tais como impostos, taxas e quaisquer outros que se fizerem necessários para o perfeito cumprimento do objeto deste termo.
- 11.4. A CONTRATADA deverá entregar a Nota Fiscal eletrônica e fazer constar, no mínimo, o número do Processo Administrativo, do instrumento contratual e da Nota de Empenho, descrição dos itens e período da licença, preço unitário e o valor total da nota, dados bancários, além de todas as informações exigidas pela legislação vigente;

- 13.2.3. Para fins de cálculo do reajuste, será utilizada a variação acumulada do IPCA — Índice Nacional de Preços ao Consumidor Amplo, divulgado pelo Instituto Brasileiro de Geografia e Estatística — IBGE, referente ao período de 12 (doze) meses, ou de outro índice oficial que venha a substituí-lo.
- 13.2.4. O reajuste somente será analisado pela CONTRATANTE mediante solicitação expressa da CONTRATADA.
- 13.2.5. Os efeitos financeiros do reajuste serão devidos a partir da data de apresentação da solicitação pela CONTRATADA, não produzindo efeitos financeiros retroativos em relação ao período anterior ao requerimento.

14. DA GARANTIA CONTRATUAL

- 14.1. A CONTRATADA obriga-se a apresentar garantia à CONTRATANTE, no valor de 5% (cinco por cento) do valor total do Contrato, conforme determina o § 1º do art. 96 da Lei Federal 14.133/2021.
- 14.2. A prestação da garantia deverá observar o CAPÍTULO II da Lei Federal n.º 14.133/2021
- 14.3. A garantia contratual deverá ser mantida enquanto vigor o Contrato.
- 14.4. Em se tratando de garantia prestada através de caução em dinheiro, ela deverá ser recolhida em conta corrente a ser informada pela CONTRATANTE no momento da assinatura do Contrato.
- 14.5. A Apólice de Seguro deverá ser emitida por Instituição autorizada pela SUSEP a operar no mercado securitário e deverá prever expressamente:
 - 14.5.1. Responsabilidade da seguradora por todas e quaisquer multas de caráter sancionatório aplicadas à CONTRATADA.
- 14.6. A Carta de Fiança deverá ser emitida por Instituição financeira autorizada pelo Banco Central do Brasil - BACEN para funcionar no Brasil, prevendo expressamente:
 - 14.6.1. Renúncia expressa, pelo fiador, ao benefício de ordem disposto no artigo 827 do Código Civil.
- 14.7. Se a garantia for utilizada em pagamento de qualquer obrigação, a CONTRATADA obriga-se a fazer a respectiva reposição no prazo máximo de 05 (cinco) dias úteis contados da data em que for notificada pela CONTRATANTE.
- 14.8. Em caso de alteração do valor contratual, prorrogação do prazo de vigência, utilização total ou parcial da garantia pela CONTRATANTE, ou em

situações outras que impliquem em perda ou insuficiência da garantia, a CONTRATADA deverá providenciar a complementação ou substituição da garantia prestada no prazo determinado pela CONTRATANTE, observadas as condições originais para aceitação da garantia estipuladas neste item.

- 14.9. A garantia prestada pela CONTRATADA será liberada ou restituída após a execução e cumprimento integral do presente Contrato, nos termos da Lei 14.133/2021 e do Decreto 19.552/2026.
- 14.10. A garantia na modalidade caução em dinheiro será atualizada monetariamente pelo índice da caderneta de poupança quando da sua restituição, não contemplando remuneração *pro rata die*.

15. DAS OBRIGAÇÕES DA CONTRATADA

15.1. Compete à CONTRATADA:

- 15.1.1. Manter, durante a vigência do Contrato, todas as condições exigidas quando da contratação, comprovando-as sempre que solicitado pela CONTRATANTE;
- 15.1.2. Comunicar a imposição de penalidade que acarrete o impedimento de contratar com a CONTRATANTE, bem como a eventual perda dos pressupostos para a participação de licitação, nos termos da Lei 13.303/2016;
- 15.1.3. Cumprir as obrigações dentro dos prazos assinalados;
- 15.1.4. Responder pela qualidade e execução do objeto, observando as normas éticas e técnicas aplicáveis;
- 15.1.5. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, o objeto deste contrato em que se verificarem vícios, defeitos ou incorreções;
- 15.1.6. Apresentar as informações solicitadas e os documentos comprobatórios do adequado cumprimento das obrigações;
- 15.1.7. Prestar todos os esclarecimentos técnicos que lhe forem solicitados pela CONTRATANTE, relacionados ao objeto;
- 15.1.8. Reparar todos os danos e prejuízos causados à CONTRATANTE ou a terceiros, não restando excluída ou reduzida esta responsabilidade pela presença de fiscalização ou pelo acompanhamento da execução por parte da CONTRATANTE;
- 15.1.9. Não infringir quaisquer direitos autorais, patentes ou registros, inclusive marcas, know-how ou trade-secrets, durante a execução do objeto contratado, sendo responsável pelos prejuízos, inclusive honorários de advogado, custas e despesas decorrentes de qualquer

- medida ou processo judicial ou administrativo iniciado em face da CONTRATANTE, por acusação da espécie;
- 15.1.10. Garantir como “segredos comerciais e confidenciais” quaisquer informações, dados, processos, fórmulas, utilizando-os apenas para as finalidades previstas neste contrato, não podendo revelá-los ou facilitar sua revelação a terceiros;
- 15.1.11. Responsabilizar-se pelo cumprimento dos requisitos definidos pela Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), no que se refere ao tratamento de dados pessoais, à proteção dos direitos fundamentais de liberdade e de privacidade e livre desenvolvimento da personalidade da pessoa natural, bem como ao cumprimento no disposto na RESOLUÇÃO CD/ANPD Nº 19, de 23 de agosto de 2024;
- 15.1.12. Permitir acompanhamento e fiscalização da execução do objeto contratual pelo fiscal;
- 15.1.13. Fornecer o suporte e apoio técnico para instalação, configuração e operação da solução, identificando falhas ou inconsistência, incluindo ainda o esclarecimento de dúvidas, de forma a garantir o funcionamento da solução;
- 15.1.14. Garantir assistência técnica e atualização contínua;
- 15.1.15. Designar 01 (um) preposto como responsável pelo Contrato para participar de eventuais reuniões e ser o interlocutor da CONTRATADA, zelando pelo fiel cumprimento das obrigações previstas neste Instrumento;
- 15.1.16. Entregar a solução com todos os acessórios/recursos necessários para uso imediato.

16. DAS OBRIGAÇÕES DA CONTRATANTE

16.1. Compete à CONTRATANTE:

- 16.1.1. Fiscalizar e avaliar a execução do contrato, por meio do fiscal designado;
- 16.1.2. Realizar o recebimento do objeto, quando ele estiver conforme;
- 16.1.3. Realizar os pagamentos devidos à CONTRATADA, nas condições estabelecidas neste Contrato;
- 16.1.4. Exigir da CONTRATADA o cumprimento do objeto nas idênticas condições assumidas quando da celebração do contrato;

- 16.1.5. Solicitar, acompanhar, fiscalizar, exercer controle, administração e gestão do contrato assinado com a CONTRATADA para o cumprimento do objeto deste Contrato.
- 16.1.6. Notificar a CONTRATADA, por escrito, fixando-lhe prazo para corrigir defeitos ou irregularidades ocorridas no recebimento do(s) item(ns) adquirido(s), sob pena de aplicação das penalidades previstas em contrato.

17. DAS DISPOSIÇÕES LEGAIS

- 17.1. Este Contrato é regulado pelas suas cláusulas, pela Lei 14.133/2021 e Decretos Municipais 11.245/2003 e 18.096/2022.

18. DA DOCUMENTAÇÃO INTEGRANTE

- 18.1. Constituem partes integrantes do presente Contrato a proposta apresentada pela CONTRATADA, o edital da licitação Pregão Eletrônico xxxxx/xxxx e seus, independentemente de transcrição, nos termos da Lei Federal 14.133/2021.
- 18.2. Em caso de divergência ou contradição entre as disposições dos documentos mencionados no item 18.1 e as deste Contrato, prevalecerão as regras contidas no edital da licitação.

19. DA SUBCONTRATAÇÃO

- 19.1. Não será permitida a subcontratação para o objeto deste Contrato..

20. DA GESTÃO E FISCALIZAÇÃO

- 20.1. A designação do Gestor e Fiscal do Contrato será realizada através de Portaria publicada no Diário Oficial do Município - DOM, nos termos do Decreto Municipal de Belo Horizonte 18.324/2023.
- 20.2. Todo o objeto será acompanhado pelo Fiscal do Contrato, que será responsável por verificar e fazer cumprir a execução do objeto de acordo com as exigências contratuais, especificações, normas técnicas, instruções técnicas e padrões de qualidade, desde o início até o recebimento definitivo, podendo, inclusive, questionar detalhes de execução ou executados, materiais em utilização ou já utilizados, sujeitando-os a análise e aprovação.
- 20.3. O Fiscal deverá analisar e decidir sobre proposições da CONTRATADA que visem melhorar a execução, recomendar aplicação de advertências, multas ou outras penalidades no Contrato.
- 20.4. O Fiscal realizará a validação do objeto executado e tomará todas as

providências e ações necessárias ao bom andamento da execução do objeto, submetendo todos os questionamentos ao Gestor do Contrato, comunicando em tempo hábil, qualquer ocorrência que requeira tomada de decisões ou providências que ultrapassem o seu âmbito de competência.

21. DAS ALTERAÇÕES CONTRATUAIS

- 21.1. Desde que não altere a natureza do objeto contratado ou descumpra o dever de licitar, o presente Contrato poderá ser alterado, por acordo entre as partes, para melhor adaptar suas previsões ao interesse da CONTRATANTE, nos termos e limites da Lei 14.133/2021.
- 21.2. As alterações contratuais serão formalizadas por meio de Termo Aditivo e Termo de Apostila, quando admitido.

22. DA CESSÃO DO CONTRATO

- 22.1. O presente Contrato não poderá ser cedido ou utilizado sob qualquer hipótese como título de circulação comercial, caução, cessão de crédito e/ou documento exequível a ser apresentado contra a CONTRATANTE por terceiros.
- 22.2. Fica vedado à CONTRATADA transferir ou ceder, a qualquer título, os direitos e obrigações assumidos neste Contrato.

23. DA PROTEÇÃO E TRANSMISSÃO DE INFORMAÇÃO, DADOS PESSOAIS E/OU BASE DE DADOS

- 23.1. Aplicar-se-á a este instrumento a Lei Geral de Proteção de Dados Pessoais - LGPD.
- 23.2. A CONTRATADA obriga-se ao dever de proteção, confidencialidade e sigilo de toda informação, dados pessoais e/ou base de dados a que tenha acesso, inclusive em razão de licenciamento ou da operação dos programas/sistemas, nos termos da Lei 13.709/2018, suas alterações e regulamentações posteriores, durante o cumprimento do objeto descrito no presente instrumento contratual.
- 23.3. A CONTRATADA obriga-se a implementar medidas técnicas e administrativas suficientes visando a segurança, a proteção, à confidencialidade e o sigilo de toda informação, dados pessoais e/ou base de dados a que tenha acesso a fim de evitar acessos não autorizados, acidentes, vazamentos acidentais ou ilícitos que causem destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento não

previstos.

- 23.4. A CONTRATADA deve assegurar-se de que todos os seus colaboradores, consultores e/ou prestadores de serviços que, no exercício das suas atividades, tenham acesso e/ou conhecimento da informação e/ou dos dados pessoais, respeitem o dever de proteção, confidencialidade e sigilo.
- 23.5. A CONTRATADA não poderá utilizar-se de informação, dados pessoais e/ou base de dados a que tenha acesso, para fins distintos ao cumprimento do objeto deste instrumento contratual.
- 23.6. A CONTRATADA não poderá disponibilizar e/ou transmitir a terceiros, sem prévia autorização escrita, informação, dados pessoais e/ou base de dados a que tenha acesso em razão do cumprimento do objeto deste instrumento contratual.
- 23.7. A CONTRATADA obriga-se a fornecer informação, dados pessoais e/ou base de dados estritamente necessários caso quando da transmissão autorizada a terceiros durante o cumprimento do objeto descrito neste instrumento contratual.
- 23.8. A CONTRATADA fica obrigada a devolver todos os documentos, registros e cópias que contenham informação, dados pessoais e/ou base de dados a que tenha tido acesso durante a execução do cumprimento do objeto deste instrumento contratual no prazo de 30 (trinta) dias corridos, contados da data da ocorrência de qualquer uma das hipóteses de extinção do contrato, restando autorizada a conservação apenas nas hipóteses legalmente previstas.
- 23.9. A CONTRATADA não será permitida deter cópias ou backups, informações, dados pessoais e/ou base de dados a que tenha tido acesso durante a execução do cumprimento do objeto deste instrumento contratual.
- 23.10. A CONTRATADA deverá eliminar os dados pessoais a que tiver conhecimento ou posse em razão do cumprimento do objeto deste instrumento contratual tão logo não haja necessidade de realizar seu tratamento.
- 23.11. A CONTRATADA deverá notificar, imediatamente, a CONTRATANTE no caso de vazamento, perda parcial ou total de informação, dados pessoais e/ou base de dados.
- 23.12. A notificação não eximirá a CONTRATADA das obrigações e/ou sanções que possam incidir em razão da perda de informação, dados pessoais e/ou base de dados.
- 23.13. A CONTRATADA que descumprir nos termos da Lei 13.709/2018 suas alterações e regulamentações posteriores, durante ou após a execução do

objeto descrito no presente instrumento contratual fica obrigado a assumir total responsabilidade e ao ressarcimento por todo e qualquer dano e/ou prejuízo sofrido, incluindo sanções aplicadas pela autoridade competente.

- 23.14. A CONTRATADA fica obrigada a manter preposto para comunicação com a CONTRATANTE para os assuntos pertinentes à Lei 13.709/2018 suas alterações e regulamentações posteriores.
- 23.15. O dever de sigilo e confidencialidade, e as demais obrigações descritas na presente cláusula, permanecerão em vigor após a extinção das relações entre a CONTRATADA e a CONTRATANTE, bem como, entre a CONTRATADA e os seus colaboradores, subcontratados, consultores e/ou prestadores de serviços sob pena das sanções previstas na Lei 13.709/2018, suas alterações e regulamentações posteriores, salvo decisão judicial contrária.
- 23.16. O não cumprimento de quaisquer das obrigações descritas nesta cláusula sujeitará a CONTRATADA a processo administrativo para apuração de responsabilidade e, consequente, sanção, sem prejuízo de outras.

24. DO SIGILO E DA CONFIDENCIALIDADE

- 24.1. As partes se obrigam ao dever de proteção, confidencialidade e sigilo de toda informação, dados pessoais e/ou base de dados a que tenha acesso, inclusive em razão de licenciamento ou da operação dos programas/sistemas, nos termos da Lei nº 13.709/2018, suas alterações e regulamentações posteriores.
- 24.2. As disposições desta Cláusula permanecerão válidas mesmo após o término da vigência deste instrumento.

25. DA FRAUDE E CORRUPÇÃO

- 25.1. As partes interessadas se obrigam a cumprir e a fazer cumprir as normas contra fraude e corrupção na qual estão asseguradas medidas adequadas para proteção do interesse público.
- 25.2. Para a participação neste instrumento contratual, nenhuma das partes poderá oferecer, dar ou se comprometer a dar a quem quer que seja, ou aceitar ou se comprometer a aceitar de quem quer que seja, tanto por conta própria quanto através de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou não financeiras ou benefícios de qualquer espécie que constituam prática ilegal ou de corrupção sob as leis de qualquer país, seja de forma direta ou indireta quanto ao objeto deste Contrato, ou de outra forma que não relacionada a este instrumento,

devendo garantir, ainda, que seus prepostos e colaboradores ajam da mesma forma.

- 25.3. A ocorrência de qualquer das hipóteses acima elencadas será denunciada à Controladoria Geral do Município - CTGM, para adoção das medidas cabíveis, nos termos do Decreto Municipal 16.954/2018.

26. DAS SANÇÕES ADMINISTRATIVAS

- 26.1. No caso de eventuais infrações cometidas ou de inadimplemento contratual, serão aplicadas as sanções previstas na Lei Federal n.º 14.133/2021, Decretos Municipais n.º 16.954/2018, n.º 16.538/2016, n.º 17.317/2020 e n.º 18.096/2022.

27. DA EXTINÇÃO DO CONTRATO

- 27.1. O presente Contrato extinguir-se-á ao seu término, sem necessidade de qualquer notificação ou interpelação ou judicial ou extrajudicial, podendo, no entanto, ser rescindido a qualquer tempo.
- 27.2. O presente contrato poderá ser rescindido nas hipóteses previstas na legislação, desde que formalmente motivado nos autos do processo, assegurado o contraditório e a ampla defesa, bem como nas hipóteses de a CONTRATADA:
- 27.2.1. Infringir quaisquer das cláusulas ou condições do presente contrato;
 - 27.2.2. Entrar em regime de falência, dissolver-se ou extinguir-se;
 - 27.2.3. Transferir ou ceder o presente contrato a terceiros, no todo ou em parte;
 - 27.2.4. Recusar-se a receber qualquer ordem ou instrução para melhor execução deste contrato, insistindo em fazê-lo com imperícia ou desleixo;
 - 27.2.5. Deixar de comprovar o regular cumprimento de suas obrigações trabalhistas, tributárias e sociais;
 - 27.2.6. Ser declarada inidônea e/ou suspensa e/ou impedida do direito de licitar ou contratar com a Administração Municipal;
 - 27.2.7. Subcontratar, ceder ou transferir, total ou parcialmente o objeto contratado, exceto na hipótese de serviço secundário que não integre a essência do objeto, desde que expressamente autorizada pelo CONTRATANTE, mantida em qualquer caso a integral responsabilidade da CONTRATADA;
 - 27.2.8. Associar-se com outrem, bem como realizar fusão, cisão,

incorporação ou integralização de capital, salvo com expressa autorização do CONTRATANTE.

27.3. A rescisão do contrato poderá ser:

27.3.1. Determinada por ato unilateral e escrito da Administração, nos casos enumerados no subitem anterior;

27.3.2. Amigável, por acordo entre as partes, reduzida a termo no processo da licitação, desde que haja conveniência para a CONTRATANTE;

27.3.3. Judicial, nos termos da legislação.

27.4. Este contrato poderá ser rescindido por ato unilateral do CONTRATANTE, devidamente justificado, quando o interesse público assim o exigir, sem indenização à CONTRATADA, a não ser em caso de dano efetivo disso resultante.

28. DOS CASOS OMISSOS

28.1. Os casos omissos serão decididos pela CONTRATANTE, segundo as disposições contidas na Lei 14.133/2021 e demais normas aplicáveis.

29. DAS DISPOSIÇÕES GERAIS

29.1. A tolerância da CONTRATANTE com qualquer atraso ou inadimplência por parte da CONTRATADA, não importará de forma alguma em alteração ou novação da obrigação.

29.2. A CONTRATADA autoriza a CONTRATANTE a descontar o valor correspondente aos referidos danos ou prejuízos diretamente das faturas pertinentes aos pagamentos que lhe forem devidos, independentemente de qualquer procedimento judicial ou extrajudicial, assegurada a prévia defesa.

29.3. A ausência ou omissão da fiscalização da CONTRATANTE não eximirá a CONTRATADA das responsabilidades previstas neste Contrato.

29.4. Todas as alterações que se fizerem necessárias serão registradas por intermédio de lavratura de Termo Aditivo ou Termo de Apostila, quando couber.

29.5. Os direitos decorrentes deste Contrato, não poderão em hipótese alguma, ser negociados com instituições financeiras, não se responsabilizando a CONTRATANTE por quaisquer consequências oriundas de tais transações, respondendo, ainda, o Fornecedor por perdas e danos.

ANEXO I - ESPECIFICAÇÃO TÉCNICA

1. CARACTERÍSTICAS GERAIS E ARQUITETURA DA SOLUÇÃO

- 1.1. Todos os componentes de software que integram a solução de segurança para servidores e estações de trabalho devem ser fornecidos por um único fabricante, garantindo uniformidade e integridade tecnológica.
- 1.2. A solução deve ser fornecida em arquitetura de agente único instalado nos hosts, consolidando todos os recursos de segurança contra ameaças (antivírus, firewall, IPS, controle de dispositivos e capacidades de EDR) sem a necessidade de instalação de módulos de agentes adicionais.
- 1.3. O gerenciamento e a monitoração da solução devem ser centralizados por meio de uma plataforma baseada na web e operada em modelo de nuvem (SaaS - Software as a Service).
- 1.4. A CONTRATADA deverá disponibilizar todas as atualizações de vacinas, assinaturas, inteligência de ameaças e novas versões dos agentes e da console de gerenciamento sem qualquer custo adicional para a CONTRATANTE durante toda a vigência do contrato.
- 1.5. Caso a arquitetura adotada pelo proponente exija componentes de infraestrutura local para servidores de cache de vacinas ou relays de comunicação interna, o fornecedor deverá entregar todas as licenças de bancos de dados proprietários ou componentes adicionais necessários para a sustentação, sem ônus para a CONTRATANTE.
- 1.6. A solução proposta deve estar em total conformidade com a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018), garantindo mecanismos adequados de segurança, criptografia e conformidade legal para o tratamento e armazenamento dos dados coletados, sendo admitido o uso de consoles de nuvem hospedadas no exterior, desde que assegurados os requisitos legais de transferência internacional de dados.
- 1.7. O fabricante da solução deverá ser membro ativo do programa Microsoft Active Protection Program (MAPPP), visando garantir o acesso antecipado a informações críticas de vulnerabilidades

2. CONSOLE DE ADMINISTRAÇÃO E GERENCIAMENTO UNIFICADO

- 2.1. A interface de gerenciamento deve dispor de um painel de controle (dashboard) interativo e em tempo real com o resumo do status de integridade, saúde da solução e conformidade dos dispositivos e usuários.

- 2.2. A console deve permitir a organização e a divisão dos computadores e servidores em grupos lógicos e estruturados na forma de árvore de diretórios parametrizável pelo administrador.
- 2.3. Deve permitir a sincronização nativa com o Microsoft Active Directory (AD) e Microsoft Entra ID (Azure AD) para fins de importação da estrutura organizacional, gestão de usuários e aplicação automatizada de políticas de proteção.
- 2.4. Deve suportar login federado com provedores de identidade externos com suporte a múltiplos fatores de autenticação (MFA), incluindo OpenID Connect e Microsoft AD FS.
- 2.5. Deve permitir a atribuição de regras e perfis diferenciados de acesso à administração da console, contendo no mínimo os perfis de: administrador global, permissão seletiva para grupos específicos e usuário de apenas leitura (read-only).
- 2.6. A console deve manter registros detalhados de auditoria (logs de ações) contendo as atividades executadas pelos administradores da plataforma por um período mínimo de 30 dias.
- 2.7. A console deve reter o histórico de eventos de segurança, tentativas de ataque e não conformidade por equipamento por um período mínimo de 90 dias, permitindo consultas mesmo para dispositivos que estejam temporariamente offline ou que tenham sido descontinuados.
- 2.8. Deve possuir mecanismos de comunicação via APIs públicas expostas por endpoints HTTP RESTful acessíveis pela Internet, permitindo a integração nativa com soluções do tipo SIEM (Security Information and Event Management) e a exportação programática de alertas nos formatos JSON, CEF ou KeyValue.
- 2.9. A console deve permitir a configuração e a distribuição de servidores locais de cache de atualizações dentro da rede interna, visando reduzir o consumo de largura de banda de internet dos links principais da CONTRATANTE.
- 2.10. Deve permitir a automação do deploy e a instalação do agente remotamente, gerando pacotes dedicados ou fornecendo suporte para distribuição via políticas de grupo (GPO) e ferramentas de deploy de terceiros.
- 2.11. Permitir a geração e exportação de relatórios gerenciais e estatísticos técnicos nativos, com suporte obrigatório para os formatos PDF e CSV, e capacidade de agendamento para envio automático por e-mail.

- 2.12. A console de administração e o agente de proteção endpoint deverão suportar nativamente o idioma português.

3. RECURSOS ESSENCIAIS DO AGENTE DE PROTEÇÃO

- 3.1. Realizar a varredura e verificação em tempo real de arquivos locais, mapeamentos de rede e mídias removíveis durante operações de acesso, modificação ou downloads em andamento.
- 3.2. Contar com capacidades de inteligência artificial e aprendizado de máquina (Machine Learning / Deep Learning) para a detecção preditiva de arquivos maliciosos em pré-execução, sem dependência exclusiva de arquivos de assinaturas tradicionais.
- 3.3. Executar a desinfecção e limpeza automatizada do sistema após detecções, removendo elementos secundários e artefatos deixados por códigos maliciosos ou aplicações potencialmente indesejadas (PUA).
- 3.4. Possuir recursos de proteção dedicados a navegadores de internet (Safe Browsing), impedindo a infecção e o abuso de funções críticas do navegador por meio de web exploits.
- 3.5. Dispor de proteção contra adulteração (Anti-Tamper) baseada em senha única por dispositivo, impedindo que usuários finais ou administradores locais desabilitem, modifiquem ou desinstalem o agente sem autorização da console central.
- 3.6. Possuir capacidade de proteção contra Ransomware baseada em análise de comportamento em tempo de execução, sendo capaz de identificar processos executando criptografia massiva e não autorizada de arquivos, interromper a ameaça imediatamente e reverter automaticamente os arquivos afetados ao seu estado original.
- 3.7. Proteger o registro mestre de inicialização (MBR) do sistema contra modificações e ataques avançados direcionados ao disco rígido.
- 3.8. Suportar a integração nativa com a tecnologia AMSI (Antimalware Scan Interface) da Microsoft, garantindo a inspeção de scripts ofuscados ou maliciosos executados em PowerShell, VBScript e assemelhados.
- 3.9. Capacidade de analisar a reputação de downloads em tempo real, cruzando informações de origem, frequência global de download e inteligência de ameaças em nuvem do fabricante para bloquear arquivos suspeitos antes da execução.

4. PROTEÇÃO CONTRA VULNERABILIDADES E TÉCNICAS DE EXPLORAÇÃO

- 4.1. A solução deverá aplicar mecanismos de proteção em tempo de execução por meio de análise comportamental avançada e mitigação de exploits, blindando processos e áreas críticas de memória contra técnicas comuns de evasão e abuso de vulnerabilidades de dia zero.
- 4.2. A solução proposta deve fornecer detecção, mitigação e proteção em tempo de execução contra técnicas avançadas de exploração de memória e processos mapeadas no framework MITRE ATT&CK, cobrindo obrigatoriamente as seguintes categorias de ameaças:
 - 4.2.1. Abuso e estouro de memória (Buffer Overflow, Heap Spray, Stack Pivot, Stack Exec/MemProt);
 - 4.2.2. Técnicas de desvio de execução e manipulação de código (mecanismos ROP - Return-Oriented Programming);
 - 4.2.3. Injeção de processos e manipulação de código em execução (Process Hollowing, DLL Injection, Shellcode);
 - 4.2.4. Técnicas de evasão de defesas e bypass de ferramentas nativas do sistema operacional (AppLocker Bypass, abusos de scripts e macros legítimas);
 - 4.2.5. Proteção contra roubo de credenciais em memória (ex: extração ilícita do processo LSASS) e escalonamento de privilégios.
- 4.3. A solução proposta deverá contar com mecanismos de resposta e contenção automática baseados em análise comportamental, capazes de elevar dinamicamente os níveis de restrição, bloqueio de processos ou isolamento temporário do host afetado sempre que uma atividade de intrusão persistente ou ataque ativo ("hands-on-keyboard") for detectada pelo motor de segurança.
- 4.4. Possuir capacidade de realizar varredura ativa de memória para identificar códigos maliciosos que permaneçam residentes em processos legítimos sem gerar arquivos em disco (fileless malware).
- 4.5. Impedir de maneira automatizada e centralizada a reinicialização dos dispositivos protegidos em modo de segurança como tática de evasão ou tentativa de desativação dos agentes.

5. CONTROLE DE DISPOSITIVOS, APLICAÇÕES, WEB E PREVENÇÃO DE PERDA DE DADOS

- 5.1. A proteção deverá permitir o monitoramento, auditoria e bloqueio de periféricos e dispositivos removíveis conectados aos hosts, contemplando no mínimo: armazenamento em massa USB, discos rígidos externos,

interfaces de rede sem fio (Wi-Fi), modems, conexões Bluetooth, câmeras e protocolos de transferência de mídia (MTP e PTP), permitindo isenções customizadas por ID de modelo ou instância.

- 5.2. A solução deverá incluir capacidades de Web Control integradas para restringir o acesso a páginas web com base em categorias de conteúdo, contemplando no mínimo 14 categorias de sites inadequados ou perigosos, como phishing, malware, hacking ou comando e controle, permitindo criar listas brancas e negras customizadas.
- 5.3. Dispor de capacidades de Application Control integradas no mesmo agente para inventariar, limitar e bloquear a execução de aplicações não autorizadas, inseguras ou indesejadas pelo administrador, permitindo o bloqueio explícito via hash SHA-256.
- 5.4. A proteção deverá contar com capacidades de prevenção de vazamento de informações (DLP) em nível de endpoint, permitindo o monitoramento ou restrição da transferência de arquivos sensíveis baseados em regras corporativas.
- 5.5. A solução deverá suportar a criação de regras personalizadas de controle baseadas em conteúdo e/ou tipo de arquivo, permitindo o uso de expressões regulares (Regex) ou dicionários configuráveis para detectar e alertar/bloquear a transferência de identificadores pessoais e financeiros sensíveis alinhados ao cenário nacional (tais como estruturas numéricas de CPF, CNPJ, dados bancários e dados pessoais sensíveis regulados pela LGPD).
- 5.6. Permitir o monitoramento e a auditoria de configurações do Firewall nativo do sistema operacional Windows diretamente pela console centralizado, aplicando diretivas para hosts específicos ou grupos.

6. CAPACIDADES DE DETECÇÃO E RESPOSTA EM ENDPOINT (EDR)

- 6.1. Identificar, correlacionar e apresentar de forma clara atividades anômalas, suspeitas ou maliciosas ocorridas nos dispositivos do parque tecnológico, mapeando as detecções diretamente às táticas e técnicas do framework MITRE ATT&CK.
- 6.2. Oferecer uma visualização gráfica intuitiva da árvore de processos (análise de causa raiz), evidenciando a cadeia cronológica do ataque, processos originadores, arquivos afetados, conexões de rede estabelecidas e chaves de registro manipuladas.

- 6.3. Fornecer acesso remoto seguro e criptografado via linha de comando (Shell remoto) diretamente a partir da console de nuvem para a execução de investigações avançadas e remediações manuais em hosts específicos.
- 6.4. Suportar o armazenamento e a consulta de telemetria histórica agregada em um repositório centralizado na nuvem (Data Lake) por um período mínimo de 30 dias, permitindo a execução de consultas proativas (threat hunting) e buscas por indicadores de comprometimento (IoC) agendadas ou manuais.
- 6.5. Permitir que o administrador execute ações remotas e imediatas de resposta ao incidente a partir da console de nuvem, incluindo: encerramento forçado de processos, exclusão de arquivos maliciosos e isolamento de rede do endpoint suspeito (mantendo ativa apenas a comunicação com a console de gerenciamento).
- 6.6. O mecanismo de isolamento de rede do host afetado deve ser suportado nativamente nas plataformas Windows e Linux cobertas pela solução.
- 6.7. Fornecer relatórios resumidos com análises estáticas e dinâmicas de arquivos suspeitos interceptados, detalhando hashes, reputação global e recomendações práticas para a resposta (playbooks integrados).

7. SUPORTE A AMBIENTES DE SERVIDORES E CONTAINERS (CWPP OTIMIZADO)

- 7.1. A solução deve possuir suporte nativo e otimizado para a proteção de servidores e cargas de trabalho em ambientes físicos, virtuais ou instanciados em nuvens públicas (IaaS).
- 7.2. Fornecer recursos de proteção para plataformas Windows Server e Linux, contemplando motores antivírus, comportamento anti-ransomware, capacidades de monitoramento em tempo real e isolamento de rede centralizado.
- 7.3. O agente de monitoramento para sistemas operacionais Linux deve possuir a capacidade de fornecer visibilidade e proteção contra ameaças que operem em ambientes de containers (ex: Docker, Kubernetes ou OpenShift) a nível de sistema operacional hospedeiro (host), detectando anomalias comportamentais como mineração de criptomoedas não autorizada, tentativas de escalada de privilégios dentro do container e execuções de comandos suspeitos que tentem adulterar funções internas do kernel.
- 7.4. A solução deve fornecer monitoramento de integridade de arquivos (FIM - File Integrity Monitoring) para sistemas operacionais Windows Server e

servidores Linux de alta criticidade (como balanceadores de carga baseados em HAProxy, Nginx e equivalentes), detectando e alertando sobre criação, modificação ou exclusão não autorizada de arquivos e pastas críticos de configuração do sistema.

8. COMPATIBILIDADE DE SISTEMAS OPERACIONAIS

8.1. A solução fornecida deve garantir total compatibilidade e suporte técnico oficial do fabricante para as seguintes plataformas mínimas:

8.1.1. Plataformas Microsoft Windows Desktop: Windows 10 (64 bits) e Windows 11 (64 bits).

8.1.2. Plataformas Microsoft Windows Server: Windows Server 2012, 2012 R2, 2016, 2019, 2022 e 2025 (edições Essentials, Standard e Datacenter).

8.1.2.1. Fica estabelecido que, para atendimento aos servidores legados Windows Server 2008 R2 com o último Service Pack, será aceito o fornecimento de uma versão simplificada ou de ciclo de vida estendido de proteção do mesmo fabricante, desde que integralmente gerenciada pela mesma console unificada.

8.1.3. Plataformas Linux: Suporte nativo e homologado para as distribuições: Red Hat Enterprise Linux (RHEL) versões 7, 8, 9 e superiores; CentOS 7 / CentOS Stream; Oracle Linux 8 e 9; Ubuntu LTS versões 20.04, 22.04 e 24.04 (e superiores); Debian GNU Linux versões 11, 12 e superiores; e SUSE Linux Enterprise Server 15.

8.1.3.1. Fica estabelecido que, para o atendimento a servidores legados operando em versões inferiores às listadas no item anterior (tais como Debian 10 e Ubuntu 18.04 ou equivalentes), será aceito o fornecimento de agentes de proteção em versões de ciclo de vida estendido (Extended Lifecycle) ou com escopo simplificado de recursos do mesmo fabricante, desde que tais ativos sejam integralmente monitorados e visíveis através da mesma console centralizada de gerenciamento.

9. IMPLANTAÇÃO, TREINAMENTO E SUPORTE TÉCNICO

- 9.1. Na fase de implantação, a CONTRATADA deverá realizar a instalação, configuração e customização inicial da console de gerência, criação de políticas personalizadas com base em melhores práticas e geração dos pacotes automatizados para início pleno das operações, seguindo o cronograma acordado.
- 9.2. A CONTRATADA deverá apoiar a distribuição técnica de licenças e a remoção de ferramentas legadas de antivírus in loco ou de forma online em todo o parque de equipamentos da CONTRATANTE, sem custos adicionais.
- 9.3. O fabricante da solução deverá possuir infraestrutura oficial (portal web) para o envio contínuo de amostras de arquivos suspeitos ou falsos positivos, comprometendo-se a emitir um parecer técnico ou disponibilizar vacinas/exclusões no prazo máximo de até 48 horas corridas após a abertura do chamado de análise.
- 9.4. O atendimento do suporte técnico fornecido de forma direta pela CONTRATADA e pelo fabricante (suporte oficial em modalidade corporativa/premium) deverá seguir rigorosamente o regime de 24 horas por dia, 7 dias por semana (24x7).
- 9.5. Os canais para abertura de chamados técnicos críticos devem incluir telefone dedicado, e-mail e portal eletrônico com fornecimento automático de protocolo formal de atendimento.
- 9.6. O SLA de atendimento inicial técnico para chamados de alta criticidade será de, no máximo, 4 (quatro) horas após a sua abertura.
- 9.7. Caso a natureza do problema técnico impeça a resolução por acesso remoto ou demande apoio especializado local, a CONTRATADA deverá prestar suporte técnico presencial (on-site) nas dependências da CONTRATANTE por solicitação do fiscal do contrato sem custos adicionais à CONTRATANTE.
- 9.8. A CONTRATADA emitirá relatórios mensais consolidados com o sumário de chamados abertos e resolvidos, bem como relatórios pós-atendimento assinados pelas partes detalhando o escopo dos problemas corrigidos.
- 9.9. A CONTRATADA deverá realizar treinamento técnico especializado focado na administração, investigação de alertas de EDR e operação da console para até 10 (dez) participantes indicados pela CONTRATANTE, de forma virtual, com o fornecimento de material digital didático.