Aviso de

CONTRATAÇÃO DIRETA 64/2026

CONTRATANTE (UASG): 928000 – Conselho Regional de Fisioterapia e Terapia Ocupacional da 5° Região – Crefito-5

OBJETO: Contratação de licenças de subscrição de solução corporativa de antivírus Kaspersky Endpoint Security, do tipo EDR (*Endpoint Detection and Response*), com gerenciamento centralizado por meio de console baseada em nuvem (*cloud*), visando à proteção integral da rede lógica e dos ativos de Tecnologia da Informação (estações de trabalho, servidores, *notebooks* e dispositivos móveis) localizados na Sede e nas seccionais do CREFITO-5. A solução deverá obrigatoriamente oferecer proteção proativa contra *malwares* (vírus, *worms* e *trojans*), defesa especializada contra *ransomware* com capacidade de reversão de ações mal-intencionadas, além de funcionalidades de segurança para arquivos, e-mails e navegação *web*, garantindo a segurança cibernética e a preservação da integridade dos dados e informações geridos pelo Conselho, conforme condições e exigências estabelecidas neste instrumento.

VALOR TOTAL DA CONTRATAÇÃO: R$ 16.278,40

DATA DA SESSÃO: Dia **24/07/2026**

HORÁRIO DA FASE DE LANCES: Das 8h às 14h

CRITÉRIO DE JULGAMENTO: Menor preço

EXCLUSIVA ME/EPP/EQUIPARADAS: Sim

CONSELHO REGIONAL DE FISIOTERAPIA E TERAPIA OCUPACIONAL DA 5° REGIÃO – CREFITO-5

AVISO DE CONTRATAÇÃO DIRETA Nº 64/2026

(Processo Administrativo SEI nº 05.0524.000002/2026-13)

Torna-se público que o Conselho Regional de Fisioterapia e Terapia Ocupacional da 5° Região (Crefito-5), por meio do setor responsável pelas contratações, realizará Dispensa Eletrônica, com critério de julgamento menor preço, na hipótese do art. 75, inciso II, nos termos da Lei n.º 14.133, de 1º de abril de 2021, da Instrução Normativa Seges/ME nº 67, de 2021, e demais normas aplicáveis.

Data da sessão: 24/07/2026

Horário da Fase de Lances: 08h às 14h

Link: https://www.comprasnet.gov.br/seguro/loginPortal.asp

Critério de Julgamento: Menor preço global

1. OBJETO DA CONTRATAÇÃO DIRETA

1.1. O objeto é a contratação de licenças de subscrição de solução corporativa de antivírus Kaspersky Endpoint Security, do tipo EDR (Endpoint Detection and Response), com gerenciamento centralizado por meio de console baseada em nuvem (cloud), visando à proteção integral da rede lógica e dos ativos de Tecnologia da Informação (estações de trabalho, servidores, notebooks e dispositivos móveis) localizados na Sede e nas seccionais do CREFITO-5. A solução deverá obrigatoriamente oferecer proteção proativa contra malwares (vírus, worms e trojans), defesa especializada contra ransomware com capacidade de reversão de ações mal-intencionadas, além de funcionalidades de segurança para arquivos, e-mails e navegação web, garantindo a segurança cibernética e a preservação da integridade dos dados e informações geridos pelo Conselho, conforme condições e exigências estabelecidas neste instrumento.

1.2. O critério de julgamento adotado será o menor preço global, observadas as exigências contidas neste Aviso de Contratação Direta e seus Anexos quanto às especificações do objeto.

2. PARTICIPAÇÃO NA DISPENSA ELETRÔNICA

2.1. A participação na presente dispensa eletrônica ocorrerá por meio do Sistema de Dispensa Eletrônica, ferramenta informatizada integrante do Sistema de Compras do Governo Federal – Compras.gov.br, disponível no Portal de Compras do Governo Federal, no endereço eletrônico www.gov.br/compras.

2.1.1. O procedimento será divulgado no Compras.gov.br e no Portal Nacional de Contratações Públicas - PNCP, e encaminhado automaticamente aos fornecedores registrados no Sistema de Registro Cadastral Unificado - Sicaf, por mensagem eletrônica, na correspondente linha de fornecimento que pretende atender.

2.1.2. O Compras.gov.br poderá ser acessado pela web ou pelo aplicativo Compras.gov.br.

2.1.3. O fornecedor é o responsável por qualquer transação efetuada diretamente ou por seu representante no Sistema de Dispensa Eletrônica, não cabendo ao provedor do Sistema ou ao órgão entidade promotor do procedimento a responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros não autorizados.

2.2. Para o lote, a participação é exclusiva a microempresas e empresas de pequeno porte, nos termos do art. 49, inciso IV, c/c o art. 48, inciso I, da Lei Complementar nº 123, de 14 de dezembro de 2006.

2.2.1. A obtenção do benefício a que se refere o item anterior fica limitada às microempresas e às empresas de pequeno porte que, no ano-calendário de realização do procedimento, ainda não tenham celebrado contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte.

2.2.2. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as sociedades cooperativas mencionadas no artigo 16 da Lei nº 14.133, de 2021, para o agricultor familiar, o produtor rural pessoa física e para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006 e do Decreto n.º 8.538, de 2015.

2.3. Não poderão participar desta dispensa de licitação os fornecedores:

2.3.1. que não atendam às condições deste Aviso de Contratação Direta e seu(s) anexo(s);

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

2.3.3. que se enquadrem nas seguintes vedações:

a) autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a contratação versar sobre obra, serviços ou fornecimento de bens a ele relacionados;

b) empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou do projeto executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto, responsável técnico ou subcontratado, quando a contratação versar sobre obra, serviços ou fornecimento de bens a ela necessários;

c) pessoa física ou jurídica que se encontre, ao tempo da contratação, impossibilitada de contratar em decorrência de sanção que lhe foi imposta;

d) aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na dispensa de licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

e) empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;

f) pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do aviso, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista.

2.3.3.1. Equiparam-se aos autores do projeto as empresas integrantes do mesmo grupo econômico;

2.3.3.2. O disposto na alínea "c" aplica-se também ao fornecedor que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do fornecedor;

2.3.4. organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição (Acórdão nº 746/2014-TCU-Plenário); e

2.4. Será permitida a participação de cooperativas, desde que apresentem demonstrativo de atuação em regime cooperado, com repartição de receitas e despesas entre os cooperados e atendam ao art. 16 da Lei nº 14.133, de 2021.

2.4.1. Em sendo permitida a participação de cooperativas, serão estendidas a elas os benefícios previstos para as microempresas e empresas de pequeno porte quando elas atenderem ao disposto no art. 34 da Lei n.º 11.488, de 15 de junho de 2007.

2.5. Não poderá participar, direta ou indiretamente, da dispensa eletrônica ou da execução do contrato agente público do órgão ou entidade contratante, devendo ser observadas as situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria, conforme § 1º do art. 9º da Lei n.º 14.133, de 2021.

3. INGRESSO NA DISPENSA ELETRÔNICA E CADASTRAMENTO DA PROPOSTA INICIAL

3.1. O ingresso do fornecedor na disputa da dispensa eletrônica ocorrerá com o cadastramento de sua proposta inicial, na forma deste item.

3.2. O fornecedor interessado, após a divulgação do Aviso de Contratação Direta, encaminhará, exclusivamente por meio do Sistema de Dispensa Eletrônica, a proposta com a descrição do objeto ofertado, a marca do produto, quando for o caso, e o preço ou o desconto, até a data e o horário estabelecidos para abertura do procedimento.

3.3. Todas as especificações do objeto contidas na proposta, em especial o preço ou o desconto ofertados, vinculam a Contratada.

3.4. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto;

3.4.1. A proposta deverá conter declaração de que compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

3.4.2. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de

exclusiva responsabilidade do fornecedor, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

3.5. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será aquela correspondente à média dos efetivos recolhimentos da empresa nos últimos doze meses.

3.6. Independentemente do percentual do tributo que constar da planilha, no pagamento serão retidos na fonte os percentuais estabelecidos pela legislação vigente.

3.7. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar os serviços nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

3.8. O prazo de validade da proposta não será inferior a 60 (sessenta) dias**,** a contar da data de sua apresentação.

3.9. No cadastramento da proposta inicial, o fornecedor deverá, também, assinalar Termo de Aceitação, em campo próprio do sistema eletrônico, relativo às seguintes declarações:

3.9.1. que inexistem fatos impeditivos para sua habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores;

3.9.2. que está ciente e concorda com as condições contidas no Aviso de Contratação Direta e seus anexos;

3.9.3. que se responsabiliza pelas transações que forem efetuadas no sistema, assumindo-as como firmes e verdadeiras;

3.9.4. que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, de que trata o art. 93 da Lei nº 8.213, de 1991.

3.9.5. 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 7°, XXXIII, da Constituição;

3.10. O fornecedor organizado em cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 16 da Lei nº 14.133, de 2021.

3.11. O fornecedor enquadrado como microempresa, empresa de pequeno porte ou sociedade cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos §§ 1º ao 3º do art. 4º, da Lei n.º 14.133, de 2021.

3.12. Desde que disponibilizada a funcionalidade no sistema, fica facultado ao fornecedor, ao cadastrar sua proposta inicial, a parametrização de valor final mínimo, com o registro do seu lance final aceitável (menor preço ou maior desconto, conforme o caso).

3.12.1. Feita essa opção os lances serão enviados automaticamente pelo sistema, respeitados os limites cadastrados pelo fornecedor e o intervalo mínimo entre lances previsto neste aviso.

3.12.1.1. Sem prejuízo do disposto acima, os lances poderão ser enviados manualmente, na forma da seção respectiva deste Aviso de Contratação Direta;

3.12.2. O valor final mínimo poderá ser alterado pelo fornecedor durante a fase de disputa, desde que não assuma valor superior a lance já registrado por ele no sistema.

3.12.3. O valor mínimo parametrizado possui caráter sigiloso aos demais participantes do certame e para o órgão ou entidade contratante. Apenas os lances efetivamente enviados poderão ser conhecidos dos fornecedores na forma da seção seguinte deste Aviso.

4. FASE DE LANCES

4.1. A partir da data e horário estabelecidos neste Aviso de Contratação Direta, a sessão pública será automaticamente aberta pelo sistema para o envio de lances públicos e sucessivos, exclusivamente por meio do sistema eletrônico, sendo encerrado no horário de finalização de lances também já previsto neste aviso.

4.2. Iniciada a etapa competitiva, os fornecedores deverão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

4.2.1. O lance deverá ser ofertado pelo **valor global** do lote.

4.3. O fornecedor somente poderá oferecer valor inferior ou percentual de desconto superior ao último lance por ele ofertado e registrado pelo sistema.

4.3.1. O fornecedor poderá oferecer lances sucessivos iguais ou superiores ao lance que esteja vencendo o certame, desde que inferiores ao menor por ele ofertado e registrado pelo sistema, sendo tais lances definidos como “lances intermediários” para os fins deste Aviso de Contratação Direta.

4.3.2. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao que cobrir a melhor oferta é de R$ 0,01 (um) centavo.

4.4. Havendo lances iguais ao menor já ofertado, prevalecerá aquele que for recebido e registrado primeiro no sistema.

4.5. Caso o fornecedor não apresente lances, concorrerá com o valor de sua proposta.

4.6. Durante o procedimento, os fornecedores serão informados, em tempo real, do valor do menor lance ou do maior desconto registrado, vedada a identificação do fornecedor.

4.7. Imediatamente após o término do prazo estabelecido para a fase de lances, haverá o seu encerramento, com o ordenamento e divulgação dos lances, pelo sistema, em ordem crescente de classificação.

4.7.1. O encerramento da fase de lances ocorrerá de forma automática pontualmente no horário indicado, sem qualquer possibilidade de prorrogação e não havendo tempo aleatório ou mecanismo similar.

5. JULGAMENTO E ACEITAÇÃO DAS PROPOSTAS

5.1. Encerrada a fase de lances, quando a proposta do primeiro colocado permanecer acima do preço máximo ou abaixo do desconto definido para a contratação, o agente de

contratação poderá negociar condições mais vantajosas.

5.1.1. Neste caso, será encaminhada contraproposta ao fornecedor que tenha apresentado o menor preço ou o maior desconto, para que seja obtida a melhor proposta compatível em relação ao estipulado pela Administração.

5.1.2. A negociação poderá ser feita com os demais fornecedores classificados, exclusivamente por meio do sistema, respeitada a ordem de classificação, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo ou abaixo do desconto definido para a contratação.

5.2. Em qualquer caso, concluída a negociação, se houver, o resultado será divulgado a todos e registrado na ata do procedimento da dispensa eletrônica, devendo esta ser anexada aos autos do processo de contratação.

5.3. Constatada a compatibilidade entre o valor da proposta e o estipulado para a contratação, será solicitado ao fornecedor o envio da proposta adequada ao último lance ofertado ou ao valor negociado, se for o caso, acompanhada dos documentos complementares, quando necessários.

5.4. Encerrada a etapa de negociação, se houver, o agente de contratação verificará se o fornecedor provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133/2021, legislação correlata e nos itens 2.3 e seguintes deste Aviso, especialmente quanto à existência de sanção que impeça a participação no processo de contratação direta ou a futura contratação, mediante a consulta aos seguintes cadastros:

5.4.1. SICAF;

5.4.2. Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/ceis); e

5.4.3. Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/cnep).

5.5. A consulta aos cadastros será realizada em nome da empresa fornecedora e também de seu sócio majoritário, por força da vedação de que trata o artigo 12 da Lei n° 8.429, de 1992.

5.6. Caso conste na Consulta de Situação do fornecedor a existência de Ocorrências Impeditivas Indiretas, o órgão diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas. (IN nº 3/2018, art. 29, caput)

5.6.1. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros. (IN nº 3/2018, art. 29, §1º).

5.6.2. O fornecedor será convocado para manifestação previamente a uma eventual desclassificação. (IN nº 3/2018, art. 29, §2º).

5.6.3. Constatada a existência de sanção, o fornecedor será reputado inabilitado, por falta de condição de participação.

5.7. Verificadas as condições de participação, o gestor examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação

ao máximo estipulado para contratação neste Aviso de Contratação Direta e em seus anexos.

5.8. Será desclassificada a proposta vencedora que:

5.8.1. contiver vícios insanáveis;

5.8.2. não obedecer às especificações técnicas pormenorizadas neste aviso ou em seus anexos;

5.8.3. apresentar preços inexequíveis ou que permanecerem acima do preço máximo definido para a contratação;

5.8.4. não tiver sua exequibilidade demonstrada, quando exigido pela Administração;

5.8.5. apresentar desconformidade com quaisquer outras exigências deste aviso ou seus anexos, desde que insanável.

5.9. Quando o fornecedor não conseguir comprovar que possui ou possuirá recursos suficientes para executar a contento o objeto, será considerada inexequível a proposta de preços ou menor lance que:

5.9.1. for insuficiente para a cobertura dos custos da contratação, apresente preços global ou unitários simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos, ainda que o ato convocatório da dispensa não tenha estabelecido limites mínimos, exceto quando se referirem a materiais e instalações de propriedade do próprio fornecedor, para os quais ele renuncie a parcela ou à totalidade da remuneração.

5.9.2. apresentar um ou mais valores da planilha de custo que sejam inferiores àqueles fixados em instrumentos de caráter normativo obrigatório, tais como leis, medidas provisórias e convenções coletivas de trabalho vigentes.

5.10. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, para que o fornecedor comprove a exequibilidade da proposta.

5.11. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo fornecedor, no prazo indicado pelo sistema, desde que não haja majoração do preço.

5.11.1. O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas;

5.11.2. Considera-se erro no preenchimento da planilha passível de correção a indicação de recolhimento de impostos e contribuições na forma do Simples Nacional, quando não cabível esse regime.

5.12. Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita do setor requisitante do serviço ou da área especializada no objeto.

5.13. Se a proposta ou lance vencedor for desclassificado, será examinada a proposta ou lance subsequente, e, assim sucessivamente, na ordem de classificação.

5.14. Havendo necessidade, a sessão será suspensa, informando-se no “chat” a nova data e horário para a sua continuidade.

5.15. Encerrada a análise quanto à aceitação da proposta, será iniciada a fase de habilitação, observado o disposto neste Aviso de Contratação Direta.

6. HABILITAÇÃO

6.1. Os documentos a serem exigidos para fins de habilitação, **nos termos dos arts. 62 a 70 da Lei nº 14.133, de 2021,** constam no Termo de Referência e serão solicitados do fornecedor melhor classificado na fase de lances.

6.2. A habilitação dos fornecedores será verificada por meio do SICAF, nos documentos por ele abrangidos.

6.2.1. É dever do fornecedor atualizar previamente as comprovações constantes do SICAF para que estejam vigentes na data da abertura da sessão pública, ou encaminhar, quando solicitado, a respectiva documentação atualizada.

6.2.2. O descumprimento do subitem acima implicará a inabilitação do fornecedor, exceto se a consulta aos sítios eletrônicos oficiais emissores de certidões lograr êxito em encontrar a(s) certidão(ões) válida(s).

6.3. Na hipótese de necessidade de envio de documentos complementares, indispensáveis à confirmação dos já apresentados para a habilitação, ou de documentos não constantes do SICAF, o fornecedor será convocado a encaminhá-los, em formato digital, por meio do sistema, no prazo de 2 (duas) horas, sob pena de inabilitação. (art. 19, § 3º, da IN Seges/ME nº 67, de 2021).

6.4. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital.

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

6.6. 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, e no caso daqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

6.7. 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.

6.8. O fornecedor provisoriamente vencedor em um item, que estiver concorrendo em outro item, ficará obrigado a comprovar os requisitos de habilitação cumulativamente, isto é, somando as exigências do item em que venceu às do item em que estiver concorrendo, e assim sucessivamente, sob pena de inabilitação, além da aplicação das sanções cabíveis.

6.8.1. Não havendo a comprovação cumulativa dos requisitos de habilitação, a inabilitação recairá sobre o(s) item(ns) de menor(es) valor(es) cuja retirada(s) seja(m) suficiente(s) para a habilitação do fornecedor nos remanescentes.

6.9. Havendo necessidade de analisar minuciosamente os documentos exigidos, a sessão será suspensa, sendo informada a nova data e horário para a sua continuidade.

6.10. Será inabilitado o fornecedor que não comprovar sua habilitação, seja por não

apresentar quaisquer dos documentos exigidos, ou apresentá-los em desacordo com o estabelecido neste Aviso de Contratação Direta.

6.10.1. Na hipótese de o fornecedor não atender às exigências para a habilitação, o órgão ou entidade examinará a proposta subsequente, e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda às especificações do objeto e as condições de habilitação

6.11. Constatado o atendimento às exigências de habilitação, o fornecedor será habilitado.

7. CONTRATAÇÃO

7.1. Após a homologação e adjudicação, caso se conclua pela contratação, será firmado Termo de Contrato ou emitido instrumento equivalente.

7.2. O adjudicatário terá o prazo de 5 (cinco) dias úteis, contados a partir da data de sua convocação, para assinar o Termo de Contrato **ou** aceitar instrumento equivalente, conforme o caso (Nota de Empenho/Carta Contrato/Autorização), sob pena de decair o direito à contratação, sem prejuízo das sanções previstas neste Aviso de Contratação Direta.

7.2.1. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura do Termo de Contrato, a Administração poderá encaminhá-lo para assinatura, mediante correspondência postal com aviso de recebimento (AR), disponibilização de acesso à sistema de processo eletrônico para esse fim ou outro meio eletrônico, para que seja assinado e devolvido no prazo de 5 (cinco) dias, a contar da data de seu recebimento ou da disponibilização do acesso ao sistema de processo eletrônico.

7.2.2. O prazo previsto no subitem anterior poderá ser prorrogado, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

7.3. O Aceite da Nota de Empenho ou do instrumento equivalente, emitida ao fornecedor adjudicado, implica o reconhecimento de que:

7.3.1. referida Nota está substituindo o contrato, aplicando-se à relação de negócios ali estabelecida as disposições da Lei nº 14.133, de 2021;

7.3.2. a contratada se vincula à sua proposta e às previsões contidas no Aviso de Contratação Direta e seus anexos;

7.3.3. a contratada reconhece que as hipóteses de rescisão são aquelas previstas nos artigos 137 e 138 da Lei nº 14.133, de 2021 e reconhece os direitos da Administração previstos nos artigos 137 a 139 da mesma Lei.

7.4. O prazo de vigência da contratação é o estabelecido no Termo de Referência.

7.5. Na assinatura do contrato ou do instrumento equivalente será exigida a comprovação das condições de habilitação e contratação consignadas neste aviso, que deverão ser mantidas pelo fornecedor durante a vigência do contrato.

8. INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

8.1. Comete infração administrativa o fornecedor que praticar quaisquer das hipóteses previstas no art. 155 da Lei nº 14.133, de 2021, quais sejam:

8.1.1. dar causa à inexecução parcial do contrato;

8.1.2. dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

8.1.3. dar causa à inexecução total do contrato;

8.1.4. deixar de entregar a documentação exigida para o certame;

8.1.5. não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

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

8.1.7. ensejar o retardamento da execução ou da entrega do objeto da contratação direta sem motivo justificado;

8.1.8. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a dispensa eletrônica ou a execução do contrato;

8.1.9. fraudar a dispensa eletrônica ou praticar ato fraudulento na execução do contrato;

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

8.1.10.1. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os fornecedores, em qualquer momento da dispensa, mesmo após o encerramento da fase de lances.

8.1.11. praticar atos ilícitos com vistas a frustrar os objetivos deste certame.

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

8.2. O fornecedor que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

a) Advertência pela falta do subitem 8.1.1 deste Aviso de Contratação Direta, quando não se justificar a imposição de penalidade mais grave;

b) Multa de 5% (cinco por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do fornecedor, por qualquer das infrações dos subitens 8.1.1 a 8.1.12;

c) Impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, nos casos dos subitens 8.1.2 a 8.1.7 deste Aviso de Contratação Direta, quando não se justificar a imposição de penalidade mais grave;

d) Declaração de inidoneidade para licitar ou contratar, que impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, nos casos dos subitens 8.1.8 a 8.1.12, bem como nos demais casos que justifiquem a imposição da penalidade mais grave;

8.3. A aplicação das sanções previstas neste Aviso de Contratação Direta não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Contratante (art. 156, §9º)

8.4. Todas as sanções previstas neste Aviso poderão ser aplicadas cumulativamente com a multa (art. 156, §7º).

8.5. Antes da aplicação da multa, será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157)

8.6. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente (art. 156, §8º).

8.7. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 15 (quinze) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

8.8. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no **caput** e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

8.9. Na aplicação das sanções serão considerados (art. 156, §1º):

8.10. a natureza e a gravidade da infração cometida;

8.11. as peculiaridades do caso concreto;

8.12. as circunstâncias agravantes ou atenuantes;

8.13. os danos que dela provierem para o Contratante;

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

8.15. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 1º de agosto de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159).

8.16. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160)

8.17. O Contratante deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ele aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal. (Art. 161)

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

2021.

8.19. As sanções por atos praticados no decorrer da contratação estão previstas nos anexos a este Aviso.

9. DAS DISPOSIÇÕES GERAIS

9.1. No caso de todos os fornecedores restarem desclassificados ou inabilitados (procedimento fracassado), a Administração poderá:

9.1.1. republicar o presente aviso com uma nova data;

9.1.2. valer-se, para a contratação, de proposta obtida na pesquisa de preços que serviu de base ao procedimento, se houver, privilegiando-se os menores preços, sempre que possível, e desde que atendidas às condições de habilitação exigidas.

9.1.2.1. No caso do subitem anterior, a contratação será operacionalizada fora deste procedimento.

9.1.3. fixar prazo para que possa haver adequação das propostas ou da documentação de habilitação, conforme o caso.

9.2. As providências dos subitens 9.1.1 e 9.1.2 também poderão ser utilizadas se não houver o comparecimento de quaisquer fornecedores interessados (procedimento deserto).

9.3. Havendo a necessidade de realização de ato de qualquer natureza pelos fornecedores, cujo prazo não conste deste Aviso de Contratação Direta, deverá ser atendido o prazo indicado pelo agente competente da Administração na respectiva notificação.

9.4. Caberá ao fornecedor acompanhar as operações, ficando responsável pelo ônus decorrente da perda do negócio diante da inobservância de quaisquer mensagens emitidas pela Administração ou de sua desconexão.

9.5. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário.

9.6. Os horários estabelecidos na divulgação deste procedimento e durante o envio de lances observarão o horário de Brasília-DF, inclusive para contagem de tempo e registro no Sistema e na documentação relativa ao procedimento.

9.7. No julgamento das propostas e da habilitação, a Administração poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.

9.8. As normas disciplinadoras deste Aviso de Contratação Direta serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

9.9. Os fornecedores assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos,

independentemente da condução ou do resultado do processo de contratação.

9.10. Em caso de divergência entre disposições deste Aviso de Contratação Direta e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Aviso.

9.11. Da sessão pública será divulgada Ata no sistema eletrônico.

9.12. Integram este Aviso de Contratação Direta, para todos os fins e efeitos, os seguintes anexos:

9.12.1. ANEXO I – Termo de Referência.

9.12.2. ANEXO II – Minuta de Contrato

Eduardo Freitas da Rosa

Assinatura da autoridade competente

Crefito 5 | Conselho Regional de Fisioterapia e Terapia Ocupacional

Termo de Referência nº 16/2026

Processo Administrativo SEI n° 05.0524.000002/2026-13

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. O objeto consiste na contratação de licenças de subscrição de solução corporativa de antivírus Kaspersky Endpoint Security, do tipo EDR (*Endpoint Detection and Response*), com gerenciamento centralizado por meio de console baseada em nuvem (*cloud*), visando à proteção integral da rede lógica e dos ativos de Tecnologia da Informação (estações de trabalho, servidores, *notebooks* e dispositivos móveis) localizados na Sede e nas seccionais do CREFITO-5. A solução deverá obrigatoriamente oferecer proteção proativa contra *malwares* (vírus, *worms* e *trojans*), defesa especializada contra *ransomware* com capacidade de reversão de ações mal-intencionadas, além de funcionalidades de segurança para arquivos, e-mails e navegação *web*, garantindo a segurança cibernética e a preservação da integridade dos dados e informações geridos pelo Conselho, conforme condições e exigências estabelecidas neste instrumento.

ITEM	ESPECIFICAÇÃO	CATSER	UNIDADE DE MEDIDA	QNT.	VALOR UNITÁRIO (36 MESES)	VALOR TOTAL (36 MESES)

11	Licenças de subscrição de solução corporativa de antivírus **Kaspersky Endpoint Security**, do tipo EDR (*Endpoint Detection and Response*), com gerenciamento centralizado por meio de console baseada em nuvem (*cloud*), proteção proativa contra *malwares* (vírus, *worms* e *trojans*), defesa especializada contra *ransomware* com capacidade de reversão de ações mal-intencionadas, além de funcionalidades de segurança para arquivos, e-mails e navegação *web*.	27502	Licenças	80,00	R$ 203,48	**R$ 16.278,40**

1.2. O prazo de vigência da contratação será de **03 (três) anos** contados da assinatura do Contrato, prorrogável por até 10 (dez) anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

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

1.3. O serviço, objeto desta contratação, é caracterizado como comum, conforme justificativa constante do Estudo Técnico Preliminar.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. A presente contratação fundamenta-se na necessidade imperiosa de garantir a manutenção da proteção integral da infraestrutura tecnológica do CREFITO-5. A aquisição de uma solução do tipo EDR (*Endpoint Detection and Response*) é indispensável para a manutenção dos padrões de segurança, permitindo a detecção de ameaças conhecidas e desconhecidas por meio de análise comportamental e detecção de anomalias.

2.2. O quantitativo de 80 (oitenta) licenças foi dimensionado para atender não apenas os 60 dispositivos atualmente protegidos, mas também a expansão planejada de 20 novas máquinas (computadores e notebooks). Essa ampliação é necessária para suprir os postos de trabalho a serem ocupados pelos novos empregados públicos oriundos do Concurso Público em andamento.

2.3. A opção pela manutenção da solução Kaspersky justifica-se pela busca da maior eficiência administrativa e economia de recursos. A permanência da marca atual preserva a cultura operacional já adquirida pelo Conselho e aproveita a infraestrutura de distribuição e gerenciamento em nuvem plenamente implantada. A substituição por um fabricante distinto exigiria elevados custos de migração, novos treinamentos e importantes horas técnicas para a reconfiguração de políticas de segurança em todos os terminais, o que elevaria o Custo Total de Propriedade (TCO) sem um benefício técnico incremental que justifique tal dispêndio.

2.4. A contratação assegura ao Conselho o direito a atualizações contínuas de software e dos mecanismos de proteção (motores de detecção e vacinas), essenciais para enfrentar o dinamismo do cenário de cibercrimes. Ainda, visa garantir o acesso ao suporte técnico especializado do fabricante ou parceiro certificado para a

resolução de incidentes complexos, mitigando riscos de interrupção dos serviços públicos prestados pelo Conselho.

2.5. A proteção robusta dos terminais e servidores é condição *sine qua non* para o cumprimento das diretrizes da Lei Geral de Proteção de Dados (LGPD). O interesse público é atendido ao assegurar que o tratamento de dados sensíveis ocorra em um ambiente computacional íntegro, inviolável e auditável, preservando a confidencialidade das informações geridas pela autarquia.

2.6. O objeto da contratação está previsto no Plano de Contratações Anual 2026, conforme consta das informações básicas deste termo de referência.

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

3.1. Em observância ao disposto no art. 18, § 1º, inciso III, da Lei nº 14.133/2021, a contratação de licenças de subscrição da solução corporativa de antivírus Kaspersky Endpoint Security do tipo EDR foi planejada sob a ótica da governança pública e do ciclo de vida completo do objeto, estruturada conforme as fases seguintes:

3.1.1. Fase I – Do Planejamento:

3.1.1.1. O quantitativo de 80 (oitenta) licenças foi dimensionado com base nos ativos de Tecnologia da Informação existentes na Sede e nas seccionais do CREFITO-5, acrescido de uma margem técnica preditiva de 20 licenças, a qual visa suprir a expansão planejada de novas máquinas (computadores e notebooks) destinadas aos postos de trabalho a serem ocupados pelos empregados que serão admitidos pelo Concurso Público em andamento, mitigando riscos de subdimensionamento ou custos extraordinários.

3.1.1.2. Optou-se pelo modelo de subscrição temporária (SaaS - Software as a Service), eliminando a necessidade de investimentos iniciais de capital para aquisição de infraestrutura física dedicada local (servidores de gerência), convertendo o investimento em despesas operacionais periódicas.

3.1.1.3. A implantação iniciar-se-á com a emissão e entrega formal das chaves de subscrição originais fornecidas por meio de canal oficial do parceiro certificado Kaspersky, nos níveis Platinum ou Gold. Em seguida, proceder-se-á com a ativação e homologação do tenant institucional do Conselho junto à console centralizada baseada em cloud.

3.1.1.4. A opção estratégica pela manutenção tecnológica da solução Kaspersky preserva a infraestrutura de distribuição plenamente implantada e a cultura operacional interna. Com isso, o esforço de migração e homologação é residual, eliminando custos associados a atritos operacionais, horas técnicas excessivas de reconfiguração de políticas e riscos de lacunas de segurança que ocorreriam na troca por um fabricante distinto.

3.1.2. Fase II Operação:

3.1.2.1. A fase de operação terá vigência inicial de 03 (três) anos contados da assinatura do Contrato. Este período viabiliza a amortização do esforço operacional da TI, além de garantir estabilidade orçamentária e previsibilidade técnica à autarquia, sendo juridicamente passível de prorrogação continuada por até 10 (dez) anos.

3.1.2.2. Durante toda a vigência contratual, a solução efetuará de forma contínua a atualização de motores de detecção de próxima geração, mecanismos de machine learning (estático e dinâmico) e bases de dados de assinaturas. Tais atualizações ocorrerão de forma automática diretamente a partir da infraestrutura em nuvem, sem demandar intervenção manual rotineira ou sobrecarga de alocação da equipe de TI do Conselho.

3.1.2.3. Eventuais incidentes complexos ou anomalias de segurança cibernética serão mitigados pelo acionamento direto do suporte técnico especializado da Contratada ou do próprio fabricante. O atendimento será balizado pelos Acordos de Nível de Serviço (SLA) fixados no instrumento contratual, assegurando a resiliência e a continuidade dos serviços públicos prestados pela autarquia.

3.1.3. Fase III – Sustentabilidade:

3.1.3.1. A sustentabilidade econômico-financeira do objeto fundamenta-se na proteção do patrimônio tecnológico e na redução do Custo Total de Propriedade. Ao barrar proativamente infecções por malwares complexos, ransomwares com capacidade de reversão e ataques direcionados, a solução protege os ativos digitais e evita prejuízos financeiros severos decorrentes da interrupção de sistemas ou indisponibilidade de serviços. A console centralizada em nuvem elimina gastos com energia elétrica, refrigeração e reposição de hardware local que seriam exigidos em uma estrutura on-premise.

3.1.3.2. Tratando-se de um ativo digital e intangível (licenciamento lógico), a contratação possui impacto ambiental físico nulo. O fornecimento eletrônico de chaves de acesso elimina por completo a geração de resíduos sólidos (como descarte de mídias plásticas de instalação, manuais impressos e embalagens), reduzindo a pegada de carbono logística e alinhando o CREFITO-5 com as diretrizes federais de ecoeficiência.

3.1.4. Fase IV – Encerramento:

3.1.4.1. Ao término do prazo da relação contratual, as licenças de subscrição serão descontinuadas pela desativação das chaves, cessando os direitos de atualização e monitoramento ativo por parte do fornecedor.

3.1.4.2. Como salvaguarda legal e técnica para o estrito cumprimento da Lei Geral de Proteção de Dados (LGPD), a Contratada deverá garantir a eliminação definitiva e segura de todos os dados privados do CREFITO-5 que porventura estejam residentes na console em nuvem (logs de auditoria, históricos de ameaças interceptadas, relatórios de inventário e cadastros de usuários). A exclusão deve adotar métodos que impeçam qualquer modalidade de recuperação ou vazamento de informações geridas pela autarquia, mediante emissão de declaração formal de descarte definitivo.

3.1.4.3. Fica resguardado ao CREFITO-5 o direito de, antes do encerramento completo da subscrição, programar centralizadamente via console a desinstalação segura e silenciosa dos agentes nos terminais. A Administração poderá realizar a exportação integral de relatórios, inventários e logs históricos de incidentes acumulados durante a execução do contrato, garantindo uma transição técnica controlada, segura e sem lacunas protetivas para a nova solução que vier a suceder o objeto.

4. DOS REQUISITOS TÉCNICOS DA CONTRATAÇÃO

4.1. A contratação consiste em licenças de subscrição de solução corporativa de antivírus Kaspersky Endpoint Security, do tipo EDR (Endpoint Detection and Response), ou superior, com gerenciamento centralizado por meio de console baseada em nuvem (cloud), visando à proteção integral da rede lógica e dos ativos de Tecnologia da Informação (estações de trabalho, servidores, notebooks e dispositivos móveis) localizados na Sede e nas seccionais do CREFITO-5.

4.1.1. A solução deverá obrigatoriamente oferecer proteção proativa contra malwares (vírus, worms e trojans), defesa especializada contra ransomware com capacidade de reversão de ações mal-intencionadas, além de funcionalidades de segurança para arquivos, e-mails e navegação web, garantindo a segurança cibernética e a preservação da integridade dos dados e informações geridos pelo Conselho, e atender, no mínimo, os requisitos técnicos dispostos neste tópico.

4.1.2. Poderão ser ofertadas licenças de subscrição com recursos técnicos comprovadamente superiores, desde que não represente quaisquer ônus adicionais ao Conselho, direta ou indiretamente.

4.2. DOS REQUISITOS TÉCNICOS GERAIS

4.2.1. A solução proposta deve ser capaz de detectar os seguintes tipos de ameaças: *malwares, worms, trojans, backdoors, rootkits, spyware, adware, ransomware, keyloggers, crimeware, sites e links de phishing*, vulnerabilidades do tipo zero-day e outros *softwares* maliciosos e indesejados.

4.2.2. A solução proposta deve ser de um único fornecedor e suportar todos os módulos descritos neste Termo de Referência.

4.2.3. A solução proposta deve suportar integração com a *Anti-Malware Scan Interface* (AMSI).

4.2.4. A solução proposta deve possuir capacidade de integração com a Central de Segurança do Windows Defender.

4.2.5. A solução proposta deve suportar o subsistema Linux no Windows.

4.2.6. A solução proposta deve fornecer tecnologias de proteção de próxima geração, incluindo, no mínimo, proteção contra ameaças sem arquivos (*fileless*), bem como proteção baseada em machine learning em múltiplas camadas e análise comportamental em diferentes estágios da cadeia de ataque.

4.2.7. A solução proposta deve fornecer varredura de memória para estações de trabalho Windows e varredura de memória do kernel para estações de trabalho Linux.

4.2.8. A solução proposta deve permitir alternância para modo em nuvem, reduzindo o consumo de memória RAM e disco rígido em máquinas com recursos limitados.

4.2.9. A solução proposta deve possuir componentes dedicados para monitorar, detectar e bloquear atividades em *endpoints* (Windows, Linux e Mac) e servidores (Windows e Linux), com foco na proteção contra-ataques remotos de criptografia.

4.2.10. A solução proposta deve incluir mecanismos sem assinatura capazes de detectar ameaças mesmo sem atualizações frequentes, utilizando machine learning estático (pré-execução) e dinâmico (pós-execução), tanto em *endpoints* quanto em ambientes em nuvem.

4.2.11. A solução proposta deve fornecer análise comportamental baseada em *machine learning*.

4.2.12. A solução proposta deve permitir configurar e gerenciar *firewall* integrado aos sistemas operacionais Windows Server e Linux por meio de console centralizado.

4.2.13. A solução proposta deve incluir, no sensor de *endpoint*, os seguintes componentes: controle de aplicativos, controle web e de dispositivos, HIPS e firewall, descoberta de vulnerabilidades e patches, gerenciamento de criptografia e controle adaptativo para detecção de anomalias.

4.2.14. A solução proposta deve detectar e bloquear *hosts* não confiáveis ao identificar atividades semelhantes à criptografia em recursos compartilhados.

4.2.15. A solução proposta deve possuir mecanismo de autoproteção com senha, impedindo a interrupção do processo *antimalware* independentemente do nível de privilégio do usuário.

4.2.16. A solução proposta deve possuir bancos de reputação locais e globais.

4.2.17. A solução proposta deve verificar tráfego HTTPS, HTTP, SMTP e FTP contra *malwares*.

4.2.18. A solução proposta deve incluir módulo com funcionalidades de bloqueio de aplicativos por categorização, controle de tráfego por IP, portas e protocolos, e gerenciamento de sub-redes e permissões.

4.2.19. A solução proposta deve impedir a conexão de dispositivos USB reprogramados que emulem teclados e controlar o uso de teclados virtuais mediante autorização.

4.2.20. A solução proposta deve bloquear ataques de rede e reportar a origem da infecção.

4.2.21. A solução proposta deve manter armazenamento local nos *endpoints* para cópia segura de arquivos desinfectados, sem risco de reativação de ameaça.

4.2.22. A solução proposta deve incluir funcionalidade de limpeza remota de dispositivos, com modos silencioso, abrangendo discos rígidos, dispositivos removíveis e contas de usuários, com opções de exclusão imediata ou programada, utilizando métodos seguros de eliminação de dados.

4.2.23. A solução proposta deve adotar abordagem proativa para impedir exploração de vulnerabilidades.

4.2.24. A solução proposta deve suportar tecnologia AM-PPL (*Anti-Malware Protected Process Light*).

4.2.25. A solução proposta deve incluir proteção contra ataques baseados em falsificação ARP.

4.2.26. A solução proposta deve possuir mecanismo de aprendizado comportamental de usuários e dispositivos, com capacidade de detectar e bloquear atividades anômalas.

4.2.27. A solução proposta deve oferecer funcionalidade *Anti-Bridging* para impedir conexões simultâneas não autorizadas.

4.2.28. A solução proposta deve incluir verificação de conexões criptografadas, com capacidade de descriptografar e inspecionar tráfego seguro.

4.2.29. A solução proposta deve permitir exclusão automática de recursos web com falha de verificação criptográfica, de forma isolada por *endpoint*.

4.2.30. A solução proposta deve permitir exclusão remota de dados em caso de ausência de comunicação com o servidor.

4.2.31. A solução proposta deve suportar detecção multicamada (assinatura, heurística, *machine learning* e nuvem).

4.2.32. A solução proposta deve gerar alertas, realizar limpeza e exclusão de ameaças detectadas.

4.2.33. A solução proposta deve monitorar e bloquear comportamentos atípicos na rede corporativa.

4.2.34. A solução proposta deve otimizar verificações ignorando objetos não alterados.

4.2.35. A solução proposta deve permitir exclusões específicas de arquivos, pastas, aplicações e certificados nas verificações.

4.2.36. A solução proposta deve verificar automaticamente mídias removíveis ao serem conectadas.

4.2.37. A solução proposta deve controlar o uso de dispositivos USB, permitindo bloqueio ou liberação seletiva.

4.2.38. A solução proposta deve distinguir diferentes tipos de dispositivos periféricos.

4.2.39. A solução proposta deve controlar acesso web com base em categorias de conteúdo, incluindo bloqueio de banners e controle por políticas de usuário.

4.2.40. A solução proposta deve permitir configuração de redes Wi-Fi em dispositivos móveis com base em parâmetros técnicos.

4.2.41. A solução proposta deve suportar políticas baseadas em usuário para controle de dispositivos, web e aplicações.

4.2.42. A solução proposta deve possuir integração com nuvem para atualização contínua de ameaças.

4.2.43. A solução proposta deve permitir controle de acesso a mídias removíveis e dispositivos ópticos.

4.2.44. A solução proposta deve monitorar uso de portas personalizadas por aplicações.

4.2.45. A solução proposta deve suportar listas de permissão e negação para execução de aplicações.

4.2.46. A solução proposta deve possuir controle de aplicações integrado à nuvem.

4.2.47. A solução proposta deve incluir filtragem de tráfego web e verificação de links baseada em categorização em nuvem.

4.2.48. A solução proposta deve incluir controle de scripts, inclusive PowerShell.

4.2.49. A solução proposta deve possuir modo de teste com geração de relatórios.

4.2.50. A solução proposta deve controlar acesso a dispositivos de áudio e vídeo.

4.2.51. A solução proposta deve permitir verificação de reputação de arquivos.

4.2.52. A solução proposta deve analisar scripts diversos, incluindo WSH.

4.2.53. A solução proposta deve proteger contra *malware* desconhecido por análise comportamental e remediação automática.

4.2.54. A solução proposta deve incluir *firewall* com prevenção de intrusão.

4.2.55. A solução proposta deve suportar IPv6.

4.2.56. A solução proposta deve permitir verificação de áreas críticas do sistema.

4.2.57. A solução proposta deve incluir autoproteção contra manipulação indevida.

4.2.58. A solução proposta deve permitir seleção de componentes de proteção.

4.2.59. A solução proposta deve realizar verificação e desinfecção de arquivos compactados, inclusive protegidos por senha.

4.2.60. A solução proposta deve utilizar análise heurística para detecção de ameaças desconhecidas.

4.2.61. A solução proposta deve notificar administradores por e-mail sobre eventos relevantes.

4.2.62. A solução proposta deve permitir criação de pacotes de instalação personalizados.

4.2.63. A solução proposta deve incluir proteção contra *ransomware* em servidores e estações de trabalho.

4.2.64. A solução proposta deve bloquear automaticamente máquinas que executem atividades típicas de *ransomware*.

4.2.65. A solução proposta deve permitir instalação sem necessidade de reinicialização.

4.2.66. A solução proposta deve permitir instalação integrada de módulos de proteção e EDR.

4.2.67. A solução proposta deve suportar autenticação em duas etapas.

4.2.68. A solução proposta deve permitir administração centralizada completa, incluindo instalação, atualização e geração de relatórios.

4.2.69. A solução proposta deve permitir remoção centralizada de softwares incompatíveis.

4.2.70. A solução proposta deve suportar instalação remota via RPC, GPO e agentes.

4.2.71. A solução proposta deve garantir atualização automática de bases antivírus.

4.2.72. A solução proposta deve detectar vulnerabilidades em sistemas e aplicações.

4.2.73. A solução proposta deve permitir controle de instalação e execução de programas.

4.2.74. A solução proposta deve controlar dispositivos de entrada e saída.

4.2.75. A solução proposta deve controlar navegação dos usuários.

4.2.76. A solução proposta deve suportar ambientes virtualizados.

4.2.77. A solução proposta deve distribuir automaticamente licenças.

4.2.78. A solução proposta deve exportar relatórios em formatos PDF, CSV e XLS.

4.2.79. A solução proposta deve permitir gerenciamento centralizado de quarentena e backups.

4.2.80. A solução proposta deve permitir autenticação de administradores com contas internas.

4.2.81. A solução proposta deve permitir gerenciamento remoto de dispositivos móveis.

4.2.82. A solução proposta deve permitir exclusão de atualizações baixadas.

4.2.83. A solução proposta deve apresentar relatórios de vulnerabilidades de forma clara.

4.2.84. A interface deve suportar idiomas português e inglês.

4.2.85. A solução proposta deve possuir painel customizável com estatísticas em tempo real.

4.2.86. A solução proposta deve suportar distribuição de atualizações e pacotes em ambientes locais e remotos.

4.2.87. Os relatórios devem conter informações detalhadas sobre ameaças e tecnologias de detecção.

4.2.88. A solução proposta deve permitir uso em nuvem, sem custo adicional.

4.2.89. A solução proposta deve garantir integridade das atualizações por assinatura digital.

4.2.90. A solução proposta deve permitir monitoramento contínuo de vulnerabilidades e geração de relatórios detalhados.

4.3. **DOS REQUISITOS TÉCNICOS ESPECÍFICOS:**

4.3.1. Do módulo de proteção de *endpoint*:

4.3.1.1. Suporte para atualizações de durante toda a vigência do contrato, atendendo aos requisitos técnicos descritos o os seus respectivos avanços tecnológicos.

4.3.1.2. A solução proposta deverá proteger todas as versões disponíveis para os sistemas:

4.3.1.2.1.Sistemas operacionais Miscrosoft Windows: Windows 10 e Windows 11.

4.3.1.2.2.Sistemas operacionais Linux de 32 bits: CentOS 6.7 e posterior; Debian GNU/Linux;11.0 e posterior; Debian GNU/Linux 12.0 e posterior; Red Hat Enterprise Linux 6.7 e posterior.

4.3.1.2.3.Sistemas operacionais Linux de 64 bits: Amazon Linux 2; CentOS 6.7 e posterior*;* CentOS 7.2 e posterior; CentOS Stream 8; CentOS Stream 9; Debian GNU/Linux 11.0 e posterior; Debian GNU/Linux 12.0 e posterior; Linux Mint 20.3 e superior; Linux Mint 21.1 e posterior; openSUSE Leap 15.0 e posterior; Oracle Linux 7.3 e posterior; Oracle Linux 8.0 e posterior; Oracle Linux 9.0 e posterior; Red Hat Enterprise Linux 6.7 e posterior; Red Hat Enterprise Linux 7.2 e posterior; Red Hat Enterprise Linux 8.0 e posterior; Red Hat Enterprise Linux 9.0 e posterior; Rocky Linux 8.5 e posterior; Rocky Linux 9.1; SUSE Linux Enterprise Server 12.5 ou posterior; SUSE Linux Enterprise Server 15 ou posterior; Ubuntu 20.04 LTS; Ubuntu 22.04 LTS.

4.3.1.2.4.Sistemas operacionais ARM de 64 bits: 24.

4.3.1.2.5.Sistemas operacionais macOS: macOS 12-14 e posteriores;

4.3.1.2.6.Ferramentas de virtualização macOS:

4.3.1.2.6.1. Parallels Desktop 16 para Mac Business Edition ou superior

4.3.1.2.6.2. VMware Fusion 11.5 Profissional ou superior

4.3.1.2.7.A solução proposta deverá proteger todas as versões disponíveis dos sistemas operacionais para servidores, inclusive servidores de terminal: Microsoft Windows Server 2016 em diante.

4.3.1.3. A solução proposta deverá suportar as seguintes plataformas virtuais: VMware Workstation; VMware ESXi; Microsoft Hyper-V Server; Citrix Virtual Apps e Desktop; Citrix Provisioning.

4.3.2. Quanto ao Módulo de Gerenciamento Avançado:

4.3.2.1. A solução proposta deve suportar arquitetura *cloud-native*.

4.3.2.2. Deve incluir suporte para implantação baseada em nuvem por meio de: Amazon Web Services; Microsoft Azure; Google Cloud.

4.3.2.3. Integração SIEM e MDR deve incluir as seguintes opções de integração SIEM: HP (Micro Focus) ArcSight; IBM QRadar; Splunk; Kaspersky KUMA.

4.3.2.4. Deve fornecer a capacidade de integração com as soluções *Managed Endpoint Detection and Response* (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes.

4.3.2.5. O servidor de gerenciamento deve ser capaz de enviar logs para servidores SIEM e SYSLOG nos formatos CEF e LEEF.

4.3.2.6. A solução proposta deve suportar integração com soluções APT e com o serviço Managed Detection and Response.

4.3.3. Do Controle e Permissões de Aplicações:

4.3.3.1. Deve ter a capacidade de permitir aplicações baseadas em seus certificados de assinatura digital, MD5, SHA256, metadados, caminho do arquivo e categorias de segurança predefinidas.

4.3.3.2. Deve suportar Single Sign-On (SSO) usando NTLM e Kerberos.

4.3.3.3. Deve incluir controle de acesso baseado em funções (*Role Based Access Control - RBAC*) com funções predefinidas personalizáveis, permitindo que as restrições sejam replicadas em todos os servidores de gerenciamento na hierarquia.

4.3.3.4. O servidor de gestão deverá incluir funções de segurança predefinidas para o Auditor, Supervisor e Oficial de Segurança.

4.3.4. Gestão e Inventário de Dispositivos na Rede:

4.3.4.1. O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede.

4.3.4.2. As informações sobre o equipamento deverão ser atualizadas após cada nova pesquisa na rede, abrangendo:

4.3.4.2.1. Dispositivos Desktop/Servidores

4.3.4.2.2. Dispositivos móveis

4.3.4.2.3. Dispositivos de rede

4.3.4.2.4. Dispositivos virtuais

4.3.4.2.5. Componentes OEM

4.3.4.2.6. Periféricos de computador

4.3.4.2.7. Dispositivos IoT conectados

4.3.4.2.8. Telefones VoIP

4.3.4.2.9. Repositórios de rede

4.3.4.3. Deve ser capaz de recuperar informações sobre os equipamentos detectados durante uma pesquisa na rede, gerando um inventário completo de todos os equipamentos conectados à rede da organização.

4.3.4.4. A funcionalidade "Dispositivo desativado" deve estar disponível para ocultar tais equipamentos da lista ativa de equipamentos.

4.3.4.5. Deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários, bem como inventário em scripts e arquivos (como .dll, .exe, .bat, etc.).

4.3.5. Políticas, Perfis e Etiquetagem (*Tagging*):

4.3.5.1. O servidor de gerenciamento deve ter funcionalidade para criar múltiplos perfis dentro de uma política de proteção com diferentes configurações de proteção que possam estar simultaneamente ativas em um único ou múltiplos dispositivos com base em:

4.3.5.1.1. Status do dispositivo

4.3.5.1.2. Tag

4.3.5.1.3. Diretório Ativo (Active Directory)

4.3.5.1.4. Proprietários de dispositivos

4.3.5.1.5. Hardware

4.3.5.1.6. Deve ter a capacidade de etiquetar/marcar computadores com base em:

4.3.5.1.6.1. Atributos de rede

4.3.5.1.6.2. Nome

4.3.5.1.6.3. Domínio e/ou Sufixo de Domínio

4.3.5.1.6.4. Endereço IP

4.3.5.1.6.5. Endereço IP para o servidor de gerenciamento

4.3.5.1.6.6. Localização no Active Directory

4.3.5.1.6.7. Unidade Organizacional (OU)

4.3.5.1.6.8. Grupo

4.3.5.1.6.9. Sistema operacional

4.3.5.1.6.10. Número do pacote de serviço (Service Pack)

4.3.5.1.6.11. Arquitetura Virtual

4.3.5.1.6.12. Registro de aplicativos

4.3.5.1.6.13. Nome da aplicação

4.3.5.1.6.14. Versão do aplicativo

4.3.5.1.6.15. Fabricante

4.3.5.1.6.16. Tipo e versão

4.3.5.1.6.17. Arquitetura

4.3.5.2. Deve ter a capacidade de criar/definir configurações com base na localização de um computador na rede, e não apenas no grupo ao qual pertence no servidor de gestão.

4.3.5.3. Deve distribuir automaticamente as contas de computador por grupo de gerenciamento caso novos computadores apareçam na rede, permitindo definir as regras de transferência de acordo com o endereço IP, tipo de sistema operacional e localização nas OUs do Active Directory.

4.3.5.4. Deve possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base em:

4.3.5.5. Estruturas de domínios e grupos de trabalho do Windows

4.3.5.6. Estruturas de grupos do Active Directory

4.3.5.7. Conteúdo de um arquivo de texto criado manualmente pelo administrador

4.3.6. Diagnóstico, Comunicação e Otimização:

4.3.6.1. Deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas dos endpoints sem exigir acesso físico ao computador.

4.3.6.2. Deve incorporar no sensor de endpoint distribuição/retransmissão para transferir ou fazer proxy de solicitações de reputação de ameaças dos terminais para o servidor de gerenciamento.

4.3.6.3. Deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.

4.3.6.4. O servidor de gerenciamento primário deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.

4.3.6.5. Deve suportar os seguintes canais de entrega de notificação:

4.3.6.5.1. E-mail

4.3.6.5.2. Registro de sistema (Syslog)

4.3.6.5.3. SMS

4.3.6.6. Deve ter a funcionalidade de adicionar um mediador de conexão unidirecional entre o servidor de gerenciamento e o endpoint conectado pela internet/rede pública.

4.3.6.7. O servidor de gerenciamento deve manter um histórico de revisões das políticas, tarefas, pacotes e grupos de gerenciamento criados para que modificações possam ser revisadas.

4.3.6.8. Deve ter a capacidade de definir um intervalo de endereços IP de forma a limitar o tráfego do cliente para o servidor de gestão com base no tempo e na velocidade.

4.3.6.9. Deve permitir ao administrador criar um túnel de conexão entre um dispositivo cliente remoto e o servidor de gerenciamento caso a porta usada para conexão não esteja disponível no dispositivo.

4.3.6.10. Deve incluir múltiplas formas de notificar o administrador sobre eventos importantes (notificação por e-mail, anúncio sonoro, janela pop-up, entrada de log).

4.3.6.11. Deve permitir especificar qualquer computador da organização como centro de retransmissão de atualizações/pacotes ou centro de encaminhamento de eventos do sensor de endpoint, a fim de reduzir a carga de rede no servidor principal.

4.3.7. Ações e Rotinas de Verificação (*Scanning*):

4.3.7.1. Deve permitir ao administrador criar categorias/grupos de aplicação com base em:

4.3.7.1.1. Nome da aplicação

4.3.7.1.2. Caminho do aplicativo

4.3.7.1.3. Metadados do aplicativo

4.3.7.1.4. Certificado digital do aplicativo

4.3.7.1.5. Categorias de aplicativos predefinidas pelo fornecedor

4.3.7.1.6. SHA256 e MD5

4.3.7.1.7. Deve permitir realizar as seguintes ações para endpoints:

4.3.7.1.8. Verificação manual;

4.3.7.1.9. Verificação no acesso;

4.3.7.1.10. Verificação por demanda;

4.3.7.1.11. Verificação de arquivos compactados;

4.3.7.1.12. Verificação de arquivos individuais, pastas e unidades;

4.3.7.1.13. Bloqueio e verificação de scripts;

4.3.7.1.14. Proteção contra alteração de registros;

4.3.7.1.15. Proteção contra estouro de buffer;

4.3.7.1.16. Verificação em segundo plano/inativa;

4.3.7.1.17. Verificação de unidade removível na conexão com o sistema.

4.3.7.2. Deve suportar a instalação do sensor de endpoint juntamente com soluções de terceiros, utilizando somente o módulo de EDR ou antimalware.

4.3.7.3. Deve ter a capacidade de priorizar rotinas de varredura personalizadas e sob demanda para estações de trabalho Linux.

4.3.8. Segurança, Resiliência e Controle de Dispositivos Externos:

4.3.8.1. Deve prever a criação de uma cópia de segurança (backup) do sistema de administração com o auxílio de ferramentas integradas do próprio sistema.

4.3.8.2. Deve suportar Windows Failover Cluster e ter um recurso de *clustering* integrado.

4.3.8.3. Deve incluir alguma forma de sistema para controlar epidemias de vírus.

4.3.8.4. Deve permitir especificamente o bloqueio dos seguintes dispositivos:

4.3.8.4.1. Bluetooth

4.3.8.4.2. Dispositivos móveis

4.3.8.4.3. Modems externos

4.3.8.4.4. CD/DVD

4.3.8.4.5. Câmeras e scanners

4.3.8.4.6. MTPs

4.3.8.4.7. E a transferência de dados para dispositivos móveis

4.3.8.5. Deve ser capaz de registrar operações de arquivos (escrita e exclusão) e bloquear a execução de qualquer executável a partir de dispositivos de armazenamento USB.

4.3.9. Firewall, Prevenção e Controle de Aplicações:

4.3.9.1. Deve contar com filtragem de firewall por endereço local, interface física e Time-To-Live (TTL) de pacotes.

4.3.9.2. Deve possuir controles para o download de DLLs e drivers.

4.3.9.3. Deve ter a capacidade de restringir as atividades do aplicativo dentro do sistema de acordo com o nível de confiança atribuído a ele e limitar os direitos dos aplicativos de acessar determinados recursos (incluindo arquivos do sistema e do usuário) utilizando um módulo específico de prevenção de intrusão (HIPS).

4.3.9.4. Deve ter a capacidade de excluir automaticamente as regras de controle de aplicativos se um aplicativo não for iniciado durante um intervalo especificado e configurável.

4.3.9.5. Deve incluir Controle de inicialização de aplicativos para o sistema operacional Windows Server.

4.3.10. Atualizações, Relatórios e Virtualização:

4.3.10.1. Deve permitir o teste de atualizações baixadas por meio do software de administração centralizado antes de distribuí-las às máquinas dos clientes e a entrega imediata das atualizações após recebê-las.

4.3.10.2. Deve permitir a criação de uma hierarquia de servidores de administração a um nível arbitrário e a capacidade de geri-la centralmente a partir do nível superior.

4.3.10.3. Deve suportar o Modo de Serviços Gerenciados (MSP) para servidores de administração, para que instâncias isoladas logicamente possam ser configuradas para diferentes usuários e grupos.

4.3.10.4. Deve dar acesso aos serviços em nuvem do fornecedor de segurança antimalware através do servidor de administração.

4.3.10.5. Deve ter um mecanismo de notificação para informar os usuários sobre eventos e configurações antimalware, distribuindo também alertas por e-mail.

4.3.10.6. Deve permitir a instalação centralizada de aplicativos de terceiros em todos ou em computadores selecionados.

4.3.10.7. Deve ser capaz de gerar relatórios gráficos para eventos de software antimalware e dados sobre inventário de hardware e software, licenciamento, etc..

4.3.10.8. Deve permitir que o administrador defina configurações restritas de política/perfil para que uma tarefa de verificação de vírus seja acionada automaticamente quando um determinado número configurável de vírus for detectado durante um período de tempo definido.

4.3.10.9. Deve permitir ao administrador personalizar relatórios.

4.3.10.10. Deve ter a funcionalidade de detectar máquinas virtuais não persistentes e excluí-las automaticamente (junto com seus dados relacionados) do servidor de gerenciamento quando desligadas.

4.3.10.11. Deve permitir ao administrador definir um período de tempo após o qual um computador não conectado e seus dados relacionados serão automaticamente excluídos do servidor.

4.3.10.12. Deve permitir ao administrador definir diferentes condições de mudança de status para grupos de endpoints.

4.3.10.13. Deve permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento.

4.3.10.14. O relatório da solução proposta deve incluir detalhes sobre quais componentes de proteção de endpoint estão ou não instalados em dispositivos clientes, independentemente do perfil de proteção aplicado/existente.

4.3.10.15. O servidor de gerenciamento primário deve ser capaz de recuperar relatórios de informações detalhadas sobre o status de integridade dos terminais gerenciados pelos servidores secundários.

4.3.11. Sistemas Operacionais, Bancos de Dados e Plataformas Virtuais Suportados para a Console On-Premise:

4.3.11.1. Deve permitir instalar o módulo de gerenciamento on-premise nos seguintes sistemas operacionais: Windows e Linux.

4.3.11.2. Deverá suportar os seguintes servidores de banco de dados:

4.3.11.2.1. Windows: Microsoft SQL Server, Microsoft Banco de Dados SQL do Azure, MySQL Standard e Enterprise, MariaDB e PostgreSQL.

4.3.11.2.2. Linux: MySQL, MariaDB e PostgreSQL.

4.3.11.2.3. Deverá suportar as seguintes plataformas virtuais:

4.3.11.2.4. Windows: VMware vSphere 6.7 e 7.0, VMware Workstation 16 Pro, Microsoft Hyper-V Server (2012, 2012 R2, 2016, 2019 e 2022 de 64 bits), Citrix XenServer 7.1 LTSR, Citrix XenServer 8.x e Oracle VM VirtualBox 6.x.

4.3.11.2.5. Linux: VMware vSphere 6.7 e 7.0, VMware Desktop 16 Pro e 17 Pro, Microsoft Hyper-V Server (2012, 2012 R2, 2016, 2019 e 2022 de 64 bits), Citrix XenServer 7.1 e 8.x, e Oracle VM VirtualBox 6.x e 7.x.

4.3.12. Módulos Integrados de Criptografia:

4.3.12.1. Deve suportar criptografia em vários níveis (criptografia completa do disco - incluindo disco do sistema, criptografia de arquivos e pastas, criptografia de mídia removível) e gerenciamento de criptografia BitLocker e MacOS FileVault2.

4.3.12.2. Deve oferecer funcionalidade integrada de criptografia em nível de arquivo (File Level Encryption - FLE) em unidades locais e removíveis, permitindo a criação de listas por extensão, regras por

padrão ou individuais, modos portátil e transparente, além de gerenciar chaves centralmente com múltiplas opções de recuperação.

4.3.12.3. Deve permitir o bloqueio do acesso a arquivos criptografados por aplicativos ou permitir o acesso apenas como texto cifrado, além de restaurar dispositivos se o disco ou unidade estiver corrompido.

4.3.12.4. Deve oferecer a funcionalidade Full Disk Encryption (FDE) para discos rígidos e mídias removíveis, com gerenciamento centralizado de usuários autorizados (adição, remoção e redefinição de senha).

4.3.12.5. Deverá suportar a encriptação automática de dispositivos de armazenamento removíveis e impedir a cópia de dados para suportes não encriptados, proporcionando a criação de contêineres protegidos por senha para intercâmbio com usuários externos.

4.3.12.6. O servidor administrador/gerenciador deve ter a capacidade de descriptografar todos os dados, independentemente da localização e/ou usuário.

4.3.12.7. Deve suportar layouts de teclado QWERTY e AZERTY para autorização de pré-inicialização, incluindo autenticação em ambientes touchscreen (ex: Microsoft Surface Tablets).

4.3.12.8. Deve fornecer a funcionalidade para personalizar as configurações de criptografia do Microsoft BitLocker (uso de TPM, senhas e criptografia de hardware/software).

4.3.13. Gerenciamento Remoto e de Patches (*Patch Management*):

4.3.13.1. Deverá incluir recursos para gerenciar computadores remotamente, incluindo:

4.3.13.2. Instalação remota de software de terceiros

4.3.13.3. Relatórios sobre software e hardware existentes

4.3.13.4. Monitoramento para instalação de software não autorizado

4.3.13.5. Remoção de software não autorizado

4.3.13.6. Deverá incluir recursos de gerenciamento de patches totalmente automatizados para sistemas operacionais Windows e para aplicativos de terceiros instalados (com suporte a mais de 150 aplicações), capazes de detectar, baixar e enviar patches ausentes com base em sua criticidade ou gravidade.

4.3.13.7. Deve detectar vulnerabilidades em sistemas operacionais e outros aplicativos instalados, respondendo de forma automatizada e fornecendo relatórios abrangentes com informações CVE e dados sobre exploração (Exploit) ou ameaça encontrada para a vulnerabilidade.

4.3.13.8. O servidor de gerenciamento deve ser configurável como fonte de atualizações para Microsoft Updates e aplicativos de terceiros, permitindo ao administrador selecionar o produto e os idiomas desejados.

4.3.13.9. Deve incluir aconselhamento sobre vulnerabilidades do fornecedor de aplicativos e do fornecedor de segurança, permitindo ao administrador aprovar atualizações.

4.3.13.10. Deve identificar patches ausentes e enviar apenas os necessários, suportando a agregação de patches para minimizar reinicializações e notificando o administrador assim que as informações estiverem disponíveis.

4.3.13.11. Deverá proporcionar a possibilidade de gerir separadamente e corrigir vulnerabilidades existentes em qualquer endpoint ou apenas em pontos específicos.

4.3.13.12. Deve detectar/instalar automaticamente todos os patches perdidos anteriormente que são necessários como dependências e ter funcionalidade de suporte ao modo de teste de patch (patch testing).

4.3.13.13. Deve permitir que o administrador restrinja ou especifique a capacidade dos usuários finais de aplicar eles próprios as atualizações da Microsoft, além de permitir visualizar atualizações não relacionadas aos dispositivos clientes.

4.3.13.14. Deve ser capaz de fornecer correções de vulnerabilidades aos computadores clientes mesmo sem instalar as atualizações completas.

4.3.13.15. Deve ser capaz de enviar/implantar remotamente arquivos .EXE, .MSI, .bat, .cmd, .MSP e permitir definir parâmetros de linha de comando.

4.3.13.16. Deve ser capaz de desinstalar aplicativos remotamente (não se limitando a antivírus incompatíveis) e permitir a remoção/desinstalação de atualizações específicas de sistemas operacionais.

4.3.13.17. Deve permitir utilizar uma única tarefa para definir diferentes regras ou critérios de correção de vulnerabilidades da Microsoft e de terceiros.

4.3.13.18. Deve permitir configurar regras de instalação para:

4.3.13.19. Iniciar a instalação ao reiniciar ou desligar o computador.

4.3.13.20. Instalar todos os pré-requisitos necessários do sistema.

4.3.13.21. Permitir a instalação de novas versões de aplicativos durante as atualizações.

4.3.13.22. Baixar atualizações para o dispositivo sem instalá-las imediatamente.

4.3.13.23. Deve testar a instalação de atualizações em uma porcentagem configurável de computadores e definir o tempo alocado em horas antes da implementação completa no parque de destino.

4.3.13.24. Deve ser capaz de rastrear licenças de aplicações de terceiros e gerar notificações de quaisquer violações potenciais.

4.3.14. Implantação de Sistema Operacional e Controle Remoto Avançado:

4.3.14.1. A solução proposta deve apoiar a implantação de sistemas operacionais (OS deployment), suportando Wake-on-LAN e UEFI.

4.3.14.2. Deve ter funcionalidade integrada de compartilhamento remoto de área de trabalho (Windows Desktop Sharing). Todas as operações de arquivos executadas no endpoint remoto durante a sessão devem ser devidamente registradas em log no Servidor de Gerenciamento.

4.3.15. Do módulo de gerenciamento com interface amigável e simplificada

4.3.15.1. A solução proposta deve suportar arquitetura em nuvem (*cloud*);

4.3.15.2. A solução proposta deve incluir um console web integrado para o gerenciamento dos *endpoints*, que não deve exigir nenhuma instalação adicional;

4.3.15.3. O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque;

4.3.15.4. A solução proposta deve permitir ao administrador gerar relatórios predefinidos;

4.3.15.5. A solução proposta deve suportar a descoberta de uso de aplicações por parte do usuário e exibir informações detalhadas de uso de aplicações utilizadas por meio de navegadores e aplicações instaladas no *endpoint*;

4.3.15.6. A solução proposta deve atender às condições apontadas no item 4 e seus subitens;

4.3.15.7. A solução proposta deve suportar os sistemas operacionais Windows, Mac, Android e iOS;

4.3.15.8. A solução proposta deve incluir as seguintes informações do *endpoint*:

4.3.15.8.1. IP público de internet;

4.3.15.8.2. IP interno do dispositivo;

4.3.15.8.3. Versão do agente de proteção;

4.3.15.8.4. Última comunicação com o console, contendo data e hora;

4.3.15.8.5. Informações do sistema operacional;

4.3.15.9. A solução proposta deve permitir proteger as caixas de correio do Exchange Online, os usuários do OneDrive e os sites do SharePoint Online geridos através do Office 365;

4.3.15.10. A solução proposta deve permitir detectar informações críticas em arquivos localizados nos armazenamentos em nuvem do Office 365;

4.3.15.11. A solução proposta deve incluir treinamento em segurança cibernética.

4.4. DOS REQUISITOS DA ASSISTÊNCIA TÉCNICA E DOS NÍVEIS DE SERVIÇO (SLA)

4.4.1. A Contratada deverá garantir a prestação de suporte técnico especializado para a solução, executado diretamente pelo fabricante ou por intermédio de parceiro certificado nos níveis Platinum ou Gold, assegurando a plena disponibilidade e eficácia da proteção cibernética.

4.4.2. O suporte técnico deverá ser prestado de forma remota, em idioma português, abrangendo o auxílio na configuração de políticas de segurança complexas, tratamento de incidentes críticos, remediação de ameaças e realização de diagnósticos remotos via console de nuvem, sem a necessidade de deslocamento físico de técnicos.

4.4.3. Para fins de aferição da qualidade e eficiência do atendimento, a Contratada deverá observar os seguintes Acordos de Nível de Serviço (SLA), contados a partir da abertura do chamado pelo setor de TI do Conselho:

4.4.3.1. Incidentes Críticos (Gravidade Alta): Caracterizados pela indisponibilidade da console de gestão ou infecção massiva por *ransomware* na rede. Tempo de Resposta: até 02 (duas) horas. Tempo de Resolução: até 08 (oito) horas.

4.4.3.2. Incidentes de Gravidade Média: Falhas em módulos específicos de proteção em estações de trabalho ou erros de atualização de assinaturas. Tempo de Resposta: até 04 (quatro) horas. Tempo de Resolução: até 24 (vinte e quatro) horas.

4.4.3.3. Requisições de Suporte (Gravidade Baixa): Dúvidas operacionais, auxílio em configurações rotineiras ou geração de relatórios customizados. Tempo de Resposta: até 08 (oito) horas. Tempo de Resolução: até 48 (quarenta e oito) horas.

4.4.4. A manutenção será de natureza evolutiva e corretiva, garantindo ao CREFITO-5 o direito a todas as atualizações de versões de software, motores de detecção e bases de dados de vacinas lançadas durante a vigência contratual, de modo a manter a proteção contra ameaças de dia zero (*Zero-Day*).

4.4.5. O descumprimento injustificado dos níveis de serviço estipulados sujeitará a Contratada ao redimensionamento no pagamento (glosa), conforme previsto no Instrumento de Medição de Resultado (IMR), e à aplicação de sanções administrativas, uma vez que a agilidade na resposta é fator crítico para a preservação da integridade dos dados institucionais sob a égide da LGPD.

4.4.6. A Contratada deverá disponibilizar canais formais de comunicação (e-mail institucional e/ou portal de chamados) e telefone de suporte com funcionamento em regime comercial, devendo confirmar o recebimento de qualquer solicitação em até 24 (vinte e quatro) horas.

4.5. **DA INDICAÇÃO DE MARCAS OU MODELOS** ***(art. 41, inciso I, da Lei nº 14.133, de 2021)***

4.5.1. O produto indicado como sendo a solução mais adequada às necessidades do CREFITO-5 é o: **Kaspersky Endpoint Security.**

4.5.2. A indicação do produto fundamenta-se nas exceções previstas no art. 41, inciso I, da Lei nº 14.133/2021, que permite à Administração indicar marcas ou modelos desde que formalmente justificado. No caso em tela, a escolha ampara-se especificamente nas hipóteses das alíneas "a" e "b" do referido dispositivo, que versam sobre a necessidade de padronização do objeto e a manutenção da compatibilidade com plataformas e padrões já adotados pela autarquia.

4.5.3. Sob a ótica da viabilidade técnica, a solução Kaspersky já se encontra plenamente implantada, configurada e em operação no Conselho, tendo demonstrado eficácia na proteção dos ativos de TI em ciclos anteriores. O Setor de TI já detém o domínio operacional e a cultura adquirida sobre a ferramenta, o que garante agilidade imediata na resposta a incidentes críticos, como ataques de *ransomware*. A manutenção da marca preserva a infraestrutura de distribuição e a console de gerenciamento em nuvem já estabelecidas, eliminando o risco de janelas de vulnerabilidade que ocorreriam inevitavelmente durante um processo de migração tecnológica entre fabricantes distintos.

4.5.4. Do ponto de vista da vantajosidade econômica, a indicação da marca visa a otimização do Custo Total de Propriedade (TCO). A substituição do software atual exigiria o dispêndio de recursos humanos e financeiros extraordinários para a desinstalação em 80 ativos, reinstalação da nova solução, reconfiguração completa das políticas de segurança e treinamento da equipe, o que resultaria em prejuízo à eficiência administrativa. Assim, a renovação da subscrição do produto vigente configura a alternativa mais racional e econômica para o erário, aproveitando integralmente os investimentos lógicos já realizados.

4.5.5. Adicionalmente, a indicação está em estrita consonância com a Súmula nº 270 do Tribunal de Contas da União (TCU), que estabelece ser possível a indicação de marca em licitações de software quando estritamente necessária para atender exigências de padronização e mediante prévia justificativa técnica. Resta demonstrado, portanto, que a marca Kaspersky é a única capaz de satisfazer o interesse público no presente cenário, garantindo a proteção ininterrupta da rede lógica frente ao ingresso dos novos empregados públicos e à expansão iminente do parque computacional.

4.6. **DA SUBCONTRATAÇÃO**

4.6.1. É vedada a subcontratação total ou parcial do objeto, devendo a licitante contratada executar as obrigações sob sua exclusiva e integral responsabilidade.

4.6.1.1. Não se considera subcontratação, para fins deste item, o fornecimento de licenças de subscrição originais emitidas pelo fabricante da solução (Kaspersky), bem como o acionamento do suporte técnico de terceiro nível do próprio fabricante, desde que intermediados e gerenciados integralmente pela licitante contratada.

4.6.1.2. A licitante contratada deverá comprovar, no momento da habilitação e a qualquer tempo, à requerimento do CREFITO-5, que possui relação comercial regular com o fabricante (declaração de parceria/parceiro autorizado), garantindo o canal oficial de fornecimento, suporte e garantia da solução Kaspersky Endpoint Security EDR.

4.7. **DAS DARANTIAS**

4.7.1. Não haverá exigência da garantia para a contratação dos artigos 96 e seguintes da Lei nº 14.133, de 2021, pelas razões constantes do Estudo Técnico Preliminar.

4.7.2. No tocante aos serviços prestados (art. 40, §1º, inciso III, da Lei nº 14.133, de 2021), o prazo de garantia será aquele estabelecido na Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor).

4.8. **DA VISTORIA**

4.8.1. Não há necessidade de realização de avaliação prévia do local de execução dos serviços.

5. DO MODELO DE EXECUÇÃO DO OBJETO

5.1. A execução terá início imediato após a assinatura do contrato.

5.2. A entrega das licenças, nas quantidades indicadas pelo CREFITO-5, deverá ocorrer de forma exclusivamente eletrônica/digital, em até 10 (dez) dias corridos contatos da assinatura do contrato.

5.2.1. O fornecedor deverá disponibilizar as chaves de ativação e os certificados de licenciamento no e-mail institucional da TI (sistemas@crefito5.org.br) com indicação de acesso via painel de administração, acompanhados da respectiva Nota Fiscal e dos procedimentos técnicos detalhados para distribuição dos agentes nos *endpoints*.

5.2.2. A contratada deve comprovar o registro das licenças em nome do Conselho no portal do fabricante, garantindo o quantitativo e a vigência integral acordada.

5.2.3. A quantidade mínima inicial de licenças que poderão ser requeridas pelo CREFITO-5, não será inferior a 75% (60 licenças) do total contratado.

5.3. Após a entrega das licenças, a contratada terá o prazo de até 30 (trinta) dias para concluir os serviços de implantação (instalação, configuração de políticas de segurança) e a transferência de conhecimento para a equipe técnica do CREFITO-5.

5.3.1. Durante toda a vigência contratual, a solução deve garantir a manutenção evolutiva e corretiva, com atualizações automáticas de bases de assinaturas, motores de detecção e versões de software. O suporte técnico especializado será prestado de forma remota, obedecendo aos níveis de serviço (SLA) para pronta resposta a incidentes críticos que possam comprometer a rede lógica da autarquia.

5.4. As comunicações entre o Conselho e o fornecedor dos serviços, por meio dos seu(s) preposto(s), deverão ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

5.5. O fornecedor dos serviços contratado deverá indicar, em até 10 (dez) dias da assinatura do contrato, e manter durante a vigência do contrato, um preposto da empresa para o tratamento das questões técnicas e contratuais inerentes ao objeto.

5.5.1.1. A indicação deverá ser pela via formal e conter seguintes dados do preposto:

5.5.1.1.1. Nome completo;

5.5.1.1.2. Cargo e função na empresa;

5.5.1.1.3. Endereço de e-mail para contato;

5.5.1.1.4. Número de telefone para contato.

5.5.1.2. O CREFITO-5 poderá recusar, desde que justificadamente, a indicação ou a manutenção do(s) preposto(s) indicado(s) pela empresa, hipótese em que o fornecedor designará outro para o exercício da atividade.

5.6. A execução será acompanhada, por parte do CREFITO-5, pelo seu Fiscal Técnico, responsável por verificar a conformidade dos serviços e o cumprimento das rotinas de proteção, e pelo seu Gestor do Contrato, que coordena os atos preparatórios para pagamento e eventuais alterações.

5.6.1. Eventuais inconsistências na prestação dos serviços devem ser sanadas pela contratada em prazos compatíveis com a criticidade do objeto, sob pena de glosas ou sanções.

5.7. Para garantir a continuidade do negócio e evitar janelas de vulnerabilidade, o encerramento do contrato exige obrigações de transição técnica.

5.7.1. Em até 15 (quinze) dias antes do término da vigência, o fornecedor deverá entregar um relatório consolidado de conformidade e as ocorrências de segurança do período.

5.7.2. É obrigação da contratada realizar a transferência final de conhecimentos, devolver recursos de propriedade do Conselho e revogar todos os perfis de acesso administrativo à console em nuvem.

5.7.3. O fiel cumprimento dessas etapas de transição é condição indispensável para a liberação de garantias e para o atesto final de bom desempenho cadastral.

5.8. Local e horário da prestação dos serviços:

5.8.1. Os serviços serão prestados no seguinte endereço: **Avenida Palmeira, 27/403 - Bairro Petrópolis – Porto Alegre/RS. CEP 90470-300**.

5.8.2. Os serviços de implantação serão prestados no seguinte horário: de segunda à sexta-feira, das 8h às 17h.

5.8.2.1. Os serviços de suporte técnico deverão ocorrer na modalidade 24/7, mediante solicitação do CREFITO-5, observados os níveis de serviço (SLA) estabelecidos.

5.8.3. Os comunicados oficiais deverão ser direcionados, conforme o caso, para os e-mails do Fiscal e/ou Gestor indicados no termo de contrato e, na sua falta, ao e-mail institucional do CREFITO-5: atendimento@crefito5.org.br .

5.9. Conjuntamente com o licenciamento deverão ser entregues:

5.9.1. Fatura e Nota Fiscal correspondentes ao objeto;

5.9.2. Procedimentos técnicos detalhados para ativação e distribuição automatizada dos agentes nos *endpoints*;

5.9.3. Contatos e canais de suporte técnico do fabricante e/ou parceiro certificado;

5.9.4. Comprovação de registro do licenciamento em nome do CREFITO-5 no portal do fabricante, especificando o quantitativo e o prazo integral de validade.

5.10. Das Rotinas de Implementação e Configuração:

5.10.1. Após a disponibilização das licenças, a Contratada terá o prazo de até 30 (trinta) dias para concluir os serviços auxiliares de instalação, configuração das políticas de segurança na console em nuvem e a devida integração com os ativos da Sede e seccionais.

5.10.2. Durante esta fase, o fornecedor deverá realizar a transferência de conhecimento para a equipe técnica do Conselho, fornecendo documentação técnica atualizada sobre as políticas de segurança customizadas para o ambiente institucional.

5.11. Da Manutenção e Assistência Técnica:

5.11.1. A manutenção será de natureza evolutiva e corretiva, abrangendo a atualização automática das bases de assinaturas, motores de detecção heurística e versões de *software* durante todo o período contratual.

5.11.2. A assistência técnica deverá ser prestada de forma remota, obedecendo aos níveis de serviço (SLA) necessários para pronta resposta a incidentes críticos, como ataques de *ransomware* ou vulnerabilidades de sistema.

5.12. Das Condições e dos Prazos para Pagamento

5.12.1. O pagamento dar-se-á de acordo com o número de licenças efetivamente entregues e ativadas, após aceite definitivo, em parcelas correspondentes ao somatório dos valores unitários firmados em Contrato, observadas as condições e os prazos a seguir:

5.12.1.1. Concluída a implantação e ativação das licenças, a Contratada deverá encaminhar ao CREFITO-5 a documentação a seguir relacionada para verificação de conformidade pelo fiscal do contrato, o qual emitirá o Recebimento Provisório em até 5 (cinco) dias contados da data do protocolo:

5.12.1.1.1. Nota Fiscal/Fatura eletrônica contendo a descrição pormenorizada do objeto, os quantitativos de licenças disponibilizadas e os valores correspondentes;

5.12.1.1.2. Documentação técnica comprobatória da ativação e disponibilização das licenças (certificado de licenciamento emitido pelo fabricante Kaspersky e/ou relatório de ativação emitido via console em nuvem);

5.12.1.1.3. Comprovação de regularidade fiscal, previdenciária e trabalhista da Contratada, mediante a apresentação das certidões negativas (ou positivas com efeitos de negativa) de débitos vigentes.

5.12.1.2. A partir do Recebimento Provisório, o fiscal do contrato terá o prazo de até 10 (dez) dias para realizar os testes de conformidade técnica e, constatada a plena adequação da solução às exigências deste Termo de Referência, atestar o Recebimento Definitivo do objeto, ato que configurará a liquidação da despesa.

5.12.1.2.1. As divergências ou inconformidades encontradas durante a fiscalização do recebimento constituirão ocorrências, as quais serão formalmente notificadas à Contratada, registradas em livro próprio ou sistema eletrônico, e juntadas ao processo de execução contratual.

5.12.1.2.2. As ocorrências apontadas no âmbito da fiscalização do recebimento do objeto, se não sanadas nos prazos estabelecidos pelo CREFITO-5, poderão ensejar retenções ou glosas no pagamento até o limite da parte controversa, o que não constituirá mora por parte da Administração para fins de aplicação de quaisquer juros, multa ou correção monetária..

5.12.2. Uma vez atestado o Recebimento Definitivo, o processo será encaminhado ao setor financeiro para a efetivação do Pagamento, o qual deverá ocorrer em até 10 (dez) dias contados da data do ateste definitivo.

5.13. Da Transição e Encerramento Contratual

5.13.1. Em até 15 (quinze) dias antes do término da vigência, o fornecedor deverá entregar um relatório final consolidado das ocorrências de segurança e o status de conformidade dos *endpoints*.

5.13.2. No ato do encerramento, o fornecedor deverá:

5.13.2.1. Revogar todos os perfis de acesso administrativo e credenciais de suporte na console de gestão;

5.13.2.2. Devolver quaisquer recursos de propriedade do Conselho;

5.13.2.3. Formalizar a cessão definitiva de direitos patrimoniais sobre configurações e customizações de políticas de segurança desenvolvidas especificamente para o CREFITO-5.

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

5.15. O Crefito-5 poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

6. DA FISCALIZAÇÃO DA CONTRATAÇÃO

6.1. Competirá ao Fiscal Técnico da contratação:

6.1.1. Acompanhar a execução contratual, com a finalidade de assegurar o cumprimento integral das obrigações pactuadas e a obtenção dos melhores resultados para a Administração, nos termos do art. 22, inciso VI, do Decreto nº 11.246/2022.

6.1.2. Registrar, no histórico de gerenciamento contratual, todas as ocorrências relacionadas à execução do ajuste, promovendo as anotações necessárias à regularização de falhas, defeitos ou irregularidades observadas, nos termos do art. 117, §1º, da Lei nº 14.133/2021 e do art. 22, inciso II, do Decreto nº 11.246/2022.

6.1.3. Identificar inexatidão, irregularidade ou desconformidade na execução contratual, notificando formalmente a Contratada para saneamento da ocorrência, fixando prazo razoável para a correção, nos termos do art. 22, inciso III, do Decreto nº 11.246/2022.

6.1.4. Comunicar tempestivamente ao Gestor do Contrato quaisquer fatos ou situações que demandem providências que ultrapassem sua competência, inclusive aquelas que possam comprometer o cumprimento dos prazos contratuais ou inviabilizar a adequada execução do objeto, conforme disposto no art. 22, incisos IV e V, do Decreto nº 11.246/2022.

6.1.5. Informar ao Gestor do Contrato, em tempo hábil, o encerramento da vigência contratual sob sua fiscalização, com vistas à adoção tempestiva das providências necessárias à eventual prorrogação, renovação ou realização de nova contratação, na forma do art. 22, inciso VII, do Decreto nº 11.246/2022.

6.1.6. Verificar a manutenção das condições de habilitação da Contratada durante a execução contratual, podendo solicitar documentos comprobatórios pertinentes sempre que necessário.

6.1.7. Acompanhar os aspectos relacionados à execução financeira vinculada à prestação contratual, inclusive quanto à ocorrência de glosas, garantias contratuais e regularidade documental necessária ao processamento da despesa.

6.1.8. Em caso de constatação de descumprimento das obrigações contratuais, adotar as medidas necessárias à solução da ocorrência, comunicando imediatamente o Gestor do Contrato quando a situação ultrapassar sua competência técnica ou administrativa.

6.2. Competirá ao Gestor do Contrato:

6.2.1. Coordenar as atividades de acompanhamento e fiscalização da execução contratual, promovendo a atualização permanente do processo administrativo de gestão do contrato, inclusive quanto aos registros formais de execução, ordens de serviço, ocorrências, alterações contratuais e eventuais prorrogações, nos termos do art. 21, inciso IV, do Decreto nº 11.246/2022.

6.2.2. Acompanhar os registros realizados pelo Fiscal Técnico, bem como as providências adotadas para saneamento das ocorrências verificadas, comunicando à autoridade competente as situações que ultrapassem sua esfera de atribuições, conforme disposto no art. 21, inciso II, do Decreto nº 11.246/2022.

6.2.3. Acompanhar a manutenção das condições de habilitação da Contratada para fins de empenho, liquidação e pagamento da despesa, registrando eventuais ocorrências que possam obstar o regular fluxo da execução financeira e orçamentária do contrato, nos termos do art. 21, inciso III, do Decreto nº 11.246/2022.

6.2.4. Emitir documento comprobatório de avaliação da execução contratual, considerando o cumprimento das obrigações assumidas pela Contratada, o desempenho aferido por indicadores objetivamente estabelecidos e eventuais penalidades aplicadas, promovendo os registros pertinentes no cadastro de atesto de cumprimento de obrigações, nos termos do art. 21, inciso VIII, do Decreto nº 11.246/2022.

6.2.5. Adotar as providências necessárias à instauração de processo administrativo de responsabilização para aplicação de sanções administrativas, quando cabível, observando o disposto no art. 158 da Lei nº 14.133/2021 e no art. 21, inciso X, do Decreto nº 11.246/2022.

6.2.6. Elaborar relatório final acerca da execução contratual, contendo avaliação quanto ao atingimento dos objetivos da contratação, resultados obtidos e eventuais recomendações destinadas ao aprimoramento das atividades administrativas, nos termos do art. 21, inciso VI, do Decreto nº 11.246/2022.

6.2.7. Encaminhar ao setor competente a documentação necessária à liquidação e ao pagamento da despesa, observados os valores efetivamente aferidos pela fiscalização contratual e as condições estabelecidas no

instrumento contratual.

6.2.8. Acompanhar os procedimentos relacionados a apostilamentos, termos aditivos, repactuações, reequilíbrio econômico-financeiro, garantias contratuais e demais atos formais relacionados à gestão administrativa do ajuste.

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

7.1. O fornecedor será selecionado por meio da realização de procedimento de DISPENSA, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo MENOR PREÇO.

7.2. O regime de execução do contrato será o de serviço continuado SEM dedicação exclusiva de mão de obra.

7.3. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

7.4. Habilitação jurídica

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

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

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

7.4.4. Sociedade empresária ou Sociedade Limitada unipessoal (SLU): 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;

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

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

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

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

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

7.5. Habilitação fiscal, social e trabalhista

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

7.5.2. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas

administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

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

7.5.4. 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;

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

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

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

7.5.8. 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.

7.6. **Qualificação Econômico-Financeira**

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

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

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

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

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

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

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

7.6.4. Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido para fins de habilitação a comprovação de patrimônio líquido mínimo de 10% do valor total estimado da contratação.

7.6.4.1. A exigência e comprovação de Patrimônio Líquido mínimo equivalente a 10% (dez por cento) do valor estimado da contratação — aplicável exclusivamente às licitantes que apresentarem índices de Liquidez Geral (LG), Solvência Geral (SG) ou Liquidez Corrente (LC) iguais ou inferiores a 1 (um) — fundamenta-se no artigo 69, § 4º, da Lei nº 14.133/2021. Tal medida busca mitigar o risco de inadimplemento contratual por fragilidade financeira da fornecedora, assegurando que a empresa vencedora possua robustez patrimonial e saúde financeira suficientes para absorver eventuais oscilações econômicas durante a execução do objeto. Ademais, a regra atua como uma salvaguarda que preserva a ampla competitividade do certame, permitindo a participação e a habilitação de empresas que, embora possuam índices de liquidez momentaneamente baixos,

demonstram possuir patrimônio líquido sólido o bastante para garantir a segurança jurídica e a continuidade da prestação dos serviços de segurança cibernética essenciais ao Conselho.

7.6.5. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. (Lei nº 14.133, de 2021, art. 65, §1º).

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

7.7. **Qualificação Técnica**

7.7.1. Declaração de que o licitante tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação, em estrita observância ao art. 67, inciso VI, da Lei nº 14.133/2021.

7.7.2. Comprovação de aptidão para execução de serviço de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, por meio da apresentação de certidões ou atestados, emitidos por pessoas jurídicas de direito público ou privado.

7.7.2.1. Para fins da comprovação de que trata este subitem, os atestados deverão demonstrar a execução satisfatória de contratos com as seguintes características mínimas:

7.7.2.1.1. Fornecimento de solução corporativa de segurança cibernética (Antivírus / *Endpoint Protection*);

7.7.2.1.2. Atendimento em quantitativo mínimo de 40 (quarenta) licenças/*endpoints* simultâneos, equivalente a 50% do total estimado da contratação, preservando a segurança operacional e a competitividade do certame conforme limites de razoabilidade do TCU;

7.7.2.1.3. Será admitido, para fins de comprovação do quantitativo mínimo, o somatório de diferentes atestados executados de forma concomitante;

7.7.2.1.4. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial da empresa licitante.

7.7.2.2. O licitante deverá comprovar que detém a condição de Parceiro Certificado pelo fabricante (Kaspersky) nos níveis Platinum ou Gold, mediante documento oficial emitido pelo fabricante/desenvolvedor;

7.7.2.2.1. A exigência justifica-se pela necessidade de assegurar que o fornecedor possui canal de suporte técnico avançado e capacidade técnica homologada para garantir o cumprimento dos Acordos de Nível de Serviço (SLA) previstos para incidentes críticos;

7.7.2.3. O licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação e contatos atualizados do contratante.

8. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

8.1. O custo estimado total da contratação é de **R$ 16.278,40 (dezesseis mil duzentos e setenta e oito reais e quarenta centavos)**, conforme custos unitários apostos na tabela constante no documento de pesquisa de preços.

9. ADEQUAÇÃO ORÇAMENTÁRIA

As despesas decorrentes da presente contratação correrão à conta da rubrica: 6.2.2.1.1.01.04.04.005 – Serviços de Informática.

Porto Alegre, 07 de julho de 2026.

Samuel Moreira de Almeida

Setor de Segurança e Tecnologia da Informação

Documento assinado eletronicamente por **Samuel Moreira De Almeida**, **Gerente Executivo**, em 07/07/2026, às 16:12, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.coffito.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0439586** e o código CRC **31E0BBB9**.

Conselho Regional de Fisioterapia e Terapia Ocupacional da 5ª Região
Processo: 05.0524.000002/2026-13 - Documento: 0439586
CREFITO-5/SETIN - Setor de Tecnologia e Segurança da Informação
Avenida Palmeira, 27/403, - Bairro Petrópolis - Porto Alegre/RS
CEP 90470-300

MINUTA DE CONTRATO

Lei nº 14.133, de 1º de abril de 2021

SERVIÇOS

Termo de Contrato Administrativo n° 000x/2026

Processo Administrativo SEI n° 05.0524.000002/2026-13

CONTRATO ADMINISTRATIVO, QUE FAZEM ENTRE SI O CREFITO-5, E A EMPRESA WERNETECH INFORMÁTICA LTDA

O Conselho Regional de Fisioterapia e Terapia Ocupacional da 5° Região – CREFITO-5, com sede na Av. Palmeira, n° 27, conjunto nº 403, bairro Petrópolis, Município de Porto Alegre/RS, CEP 97.470-300, inscrito(a) no CNPJ/MF nº 90.601.147/0001-20., neste ato representado pelo Presidente Eduardo Freitas da Rosa, nomeado(a) pela Ata da Reunião Plenária nº 339, de 27 de outubro de 2023, publicada no DOU de 1° de novembro de 2023, doravante denominado CONTRATANTE, e o(a) xxxxxx, inscrito(a) no CNPJ/MF nº xxxxxxxx, sediado(a) na Rua xxxxxx, n° xxxx, Bairro: xxxxxx, xxxxx, no Município de xxxx/xxxx, doravante designado CONTRATADO, neste ato representado(a) por xxxxxx, xxxxx, conforme atos constitutivos da empresa **ou** procuração apresentada nos autos, resolvem celebrar o presente Termo de Contrato, ficando as partes sujeitas à Lei nº 14.133, de 1º de abril de 2021, e seus regulamentos, os preceitos de direito público e supletivamente os princípios da teoria geral dos contratos e as disposições de direito privado, além dos elementos que instruem o Processo Administrativo SEI nº 05.0524.000002/2026-13, ao qual se refere a contratação, e das cláusulas e condições a seguir enunciadas.

CLÁUSULA PRIMEIRA – OBJETO (art. 92, I e II)

1.1. O objeto do presente instrumento é a contratação de licenças de subscrição de solução corporativa de antivírus Kaspersky Endpoint Security, do tipo EDR (Endpoint Detection and Response), com gerenciamento centralizado por meio de console baseada em nuvem (cloud), visando à proteção integral da rede lógica e dos ativos de Tecnologia da Informação (estações de trabalho, servidores, notebooks e dispositivos móveis) localizados na Sede e nas seccionais do CREFITO-5. A solução deverá obrigatoriamente oferecer proteção proativa contra malwares (vírus, worms e trojans), defesa especializada contra ransomware com capacidade de reversão de ações mal-intencionadas, além de funcionalidades de segurança para arquivos, e-mails e navegação web, garantindo a segurança cibernética e a preservação da integridade dos dados e informações geridos pelo Conselho, nas condições estabelecidas na formalização da demanda e proposta da contratada, observados os documentos que instruem o processo administrativo originário.

ITEM	ESPECIFICAÇÃO	CATSER	UNIDADE DE MEDIDA	QTD	VALOR UNITÁRIO (36 meses)	VALOR TOTAL GLOBAL (36 meses)
1	Licenças de subscrição de solução corporativa de antivírus **Kaspersky Endpoint Security**, do tipo EDR (*Endpoint Detection and Response*), com gerenciamento centralizado por meio de console baseada em nuvem (*cloud*), proteção proativa contra *malwares* (vírus, *worms* e *trojans*), defesa especializada contra *ransomware* com capacidade de reversão de ações	27502	Licença	80	R$ xxx	R$ xxxxx

	mal-intencionadas, além de funcionalidades de segurança para arquivos, e-mails e navegação *web*.					

1.2. Vinculam esta contratação, independentemente de transcrição:

I - A Formalização da demanda;

II - A Proposta do contratado;

III - Dispensa Eletrônica n° xxxx/2026;

IV - Eventuais anexos dos documentos supracitados.

CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

2.1. O prazo de vigência da contratação é de 36 (trinta e seis) meses, contados da assinatura do contrato, prorrogável por até 10 anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

CLÁUSULA TERCEIRA – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS (art. 92, IV, VII e XVIII)

3.1. O regime de execução contratual, os modelos de gestão e de execução, assim como os prazos e condições de conclusão, entrega, observação e recebimento do objeto constam na proposta do Contratado, anexo a este Contrato.

CLÁUSULA QUARTA – SUBCONTRATAÇÃO

4.1. Não será admitida a subcontratação do objeto contratual.

CLÁUSULA QUINTA – PREÇO (art. 92, V)

5.1. O valor total da contratação é de R$ xxxxx (xxxxxx) pelo prazo de vigência do item 2.1.

5.2. No valor acima estão incluídas 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, manutenções e outros necessários ao cumprimento integral do objeto da contratação.

5.3. O aceite dos serviços prestados por força dessa contratação será feito mediante ateste das Notas Fiscais, correspondendo tão somente aos serviços efetivamente prestados.

CLÁUSULA SEXTA – PAGAMENTO (art. 92, V e VI)

6.1. O prazo para pagamento ao contratado e demais condições a ele referentes encontram-se definidos no Termo de Referência.

6.2. O pagamento será realizado conforme o quantitativo de serviços efetivamente prestados.

CLÁUSULA SÉTIMA – REAJUSTE (art. 92, V)

6.3. Após o interregno de um ano poderão os preços iniciais ser reajustados, mediante a aplicação, pelo contratante, do índice IPCA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

7.1. CLÁUSULA OITAVA - OBRIGAÇÕES DO CONTRATANTE (art. 92, X, XI e XIV)

8.1. São obrigações do Contratante:

I - Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o contrato e seus anexos;

II - Receber o objeto no prazo e condições estabelecidas na formalização da demanda;

III - Notificar o Contratado, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido,

para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas;

IV - Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo Contratado;

V - Comunicar a empresa para emissão de Nota Fiscal em relação à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei nº 14.133, de 2021;

VI - Efetuar o pagamento ao Contratado do valor correspondente à execução do objeto, no prazo, forma e condições estabelecidos no presente Contrato e na Proposta;

VII - Aplicar ao Contratado as sanções previstas na lei e neste Contrato;

VIII - Cientificar o órgão de representação judicial do Conselho para adoção das medidas cabíveis quando do descumprimento de obrigações pelo Contratado;

IX - Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste, sobre o que a Administração terá o prazo de 1 (um) mês, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período.

X - Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo contratado no prazo máximo de 1 (um) mês, admitida a prorrogação motivada por igual período.

XI - Comunicar o Contratado na hipótese de posterior alteração do projeto pelo Contratante, no caso do art. 93, §2º, da Lei nº 14.133, de 2021.

8.2. A Administração não responderá por quaisquer compromissos assumidos pelo Contratado com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do Contratado, de seus empregados, prepostos ou subordinados.

CLÁUSULA NONA - OBRIGAÇÕES DO CONTRATADO (art. 92, XIV, XVI e XVII)

9.1. O Contratado deve cumprir todas as obrigações constantes deste Contrato e de seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas:

I - Manter preposto aceito pela Administração no local do serviço para representá-lo na execução do contrato.

II - A indicação ou a manutenção do preposto da empresa poderá ser recusada pelo órgão ou entidade, desde que devidamente justificada, devendo a empresa designar outro para o exercício da atividade.

III - Atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior (art. 137, II) e prestar todo esclarecimento ou informação por eles solicitados;

IV - Alocar os empregados necessários ao perfeito cumprimento das cláusulas deste contrato, com habilitação e conhecimento adequados, fornecendo os materiais de EPI, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência;

V - Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

VI - Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com o Código de Defesa do Consumidor (Lei nº 8.078, de 1990), bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo Contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida no edital, o valor correspondente aos danos sofridos;

VII - Não contratar, durante a vigência do contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do contratante ou do fiscal ou gestor do contrato, nos termos do artigo 48, parágrafo único, da Lei nº 14.133, de 2021;

VIII - Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores –

SICAF, o contratado deverá entregar ao setor responsável pela fiscalização do contrato, até o dia trinta do mês seguinte ao da prestação dos serviços, os seguintes documentos: 1) prova de regularidade relativa à Seguridade Social; 2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade perante a Fazenda Municipal ou Distrital do domicílio ou sede do contratado; 4) Certidão de Regularidade do FGTS – CRF; e 5) Certidão Negativa de Débitos Trabalhistas – CNDT;

IX - Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, Dissídio Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo contrato, por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao Contratante;

X - Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local dos serviços.

XI - Prestar todo esclarecimento ou informação solicitada pelo Contratante ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do empreendimento.

XII - Paralisar, por determinação do Contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.

XIII - Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução do objeto, durante a vigência do contrato.

XIV - Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local dos serviços e nas melhores condições de segurança, higiene e disciplina.

XV - Submeter previamente, por escrito, ao Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo ou instrumento congênere.

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

XVII - Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação;

XVIII - Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação (art. 116);

XIX - Comprovar a reserva de cargos a que se refere a cláusula acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas (art. 116, parágrafo único);

XX - Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

XXI - Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no art. 124, II, d, da Lei nº 14.133, de 2021;

XXII - Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do Contratante;

9.2. O Contratado deve atender as demandas da sede do Crefito-5 para a execução do objeto deste contrato na sede situada na Av. Palmeira, nº 27, conjunto nº 403, bairro Petrópolis, no Município de Porto Alegre/RS.

CLÁUSULA DÉCIMA - OBRIGAÇÕES PERTINENTES À LGPD

10.1. As partes deverão cumprir a Lei nº 13.709, de 14 de agosto de 2018 (LGPD), quanto a todos os dados pessoais a que tenham acesso em razão do certame ou do contrato administrativo que eventualmente venha a ser firmado, a partir da apresentação da proposta no procedimento de contratação, independentemente de

declaração ou de aceitação expressa.

10.2. Os dados obtidos somente poderão ser utilizados para as finalidades que justificaram seu acesso e de acordo com a boa-fé e com os princípios do art. 6º da LGPD.

10.3. É vedado o compartilhamento com terceiros dos dados obtidos fora das hipóteses permitidas em Lei.

CLÁUSULA DÉCIMA PRIMEIRA – GARANTIA DE EXECUÇÃO (art. 92, XII)

11.1. Não haverá exigência de garantia contratual da execução.

CLÁUSULA DÉCIMA SEGUNDA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS (art. 92, XIV)

12.1. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o contratado que:

I - der causa à inexecução parcial do contrato;

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

III - der causa à inexecução total do contrato;

IV - ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

V - apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;

VI - praticar ato fraudulento na execução do contrato;

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

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

12.2. Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:

I - Advertência, quando o contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei nº 14.133, de 2021);

II - Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “II”, “III” e “IV” do subitem acima deste Contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);

III - Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas “V”, “VI”, “VII” e “VIII” do subitem acima deste Contrato, bem como nas alíneas “II”, “III” e “IV”, que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei nº 14.133, de 2021).

IV - Multa:

a) Moratória de 0,5% (zero vírgula cinco por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias, sendo que o atraso superior a 30 dias autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133, de 2021.

b) Para a infração descrita na alínea “I” do subitem 12.1, a multa será de 05% a 10% do valor do Contrato.

c) Para infração descrita na alínea “II” do subitem 12.1, a multa será de 10% a 15% do valor do Contrato.

d) Compensatória, para a inexecução total do contrato prevista na alínea “III” do subitem 12.1, de 15% a 20% do valor do Contrato.

e) Para infrações descritas na alínea “IV” do subitem 12.1, a multa será de 05% a 10% do valor do Contrato.

f) Compensatória, para as infrações descritas nas alíneas “V” a “VIII” do subitem 12.1, de 10% a 15% do valor do Contrato.

12.3. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante (art. 156, §9º, da Lei nº 14.133, de 2021)

12.4. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei nº 14.133, de 2021).

12.5. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157, da Lei nº 14.133, de 2021)

12.6. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente (art. 156, §8º, da Lei nº 14.133, de 2021).

12.7. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 10 (dez) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

12.8. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

12.9. Na aplicação das sanções serão considerados (art. 156, §1º, da Lei nº 14.133, de 2021):

I - A natureza e a gravidade da infração cometida;

II - As peculiaridades do caso concreto;

III - As circunstâncias agravantes ou atenuantes;

IV - Os danos que dela provierem para o Contratante;

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

12.10. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e a autoridade competente definidos na referida Lei (art. 159).

12.11. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160, da Lei nº 14.133, de 2021)

12.12. O Contratante deverá, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal. (Art. 161, da Lei nº 14.133, de 2021)

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

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

CLÁUSULA DÉCIMA TERCEIRA – DA EXTINÇÃO CONTRATUAL (art. 92, XIX)

13.1. O contrato será extinto quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes contraentes.

13.2. O contrato poderá ser extinto antes do prazo nele fixado, sem ônus para o contratante, quando esta não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

13.3. A extinção nesta hipótese ocorrerá na próxima data de aniversário do contrato, desde que haja a

notificação do contratado pelo contratante nesse sentido com pelo menos 1 (um) meses de antecedência desse dia.

13.4. Caso a notificação da não continuidade do contrato de que trata este subitem ocorra com menos de 02 (dois) meses da data de aniversário, a extinção contratual ocorrerá após 1 (um) meses da data da comunicação.

13.5. O contrato poderá ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 da Lei nº 14.133/21, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

13.5.1. Na hipótese do item 13.5, aplicam-se também os artigos 138 e 139 da mesma Lei.

13.5.2. A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a extinção se não restringir sua capacidade de concluir o contrato.

13.5.2.1. Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

13.6. O termo de extinção, sempre que possível, será precedido:

I - Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

II - Relação dos pagamentos já efetuados e ainda devidos;

III - Indenizações e multas.

13.7. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório (art. 131, caput, da Lei n.º 14.133, de 2021).

13.8. O contrato poderá ser extinto caso se constate que o contratado mantém vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que tenha desempenhado função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau (art. 14, inciso IV, da Lei n.º 14.133, de 2021).

CLÁUSULA DÉCIMA QUARTA – DOTAÇÃO ORÇAMENTÁRIA (art. 92, VIII)

14.1. As despesas decorrentes da presente contratação correrão à conta de recursos: 6.2.2.1.1.01.04.04.005 – Serviços de informática.

14.2. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

CLÁUSULA DÉCIMA QUINTA – DOS CASOS OMISSOS (art. 92, III)

15.1. Os casos omissos serão decididos pelo Contratante, segundo as disposições contidas na Lei nº 14.133, de 2021, e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor, e normas e princípios gerais dos contratos.

CLÁUSULA DÉCIMA SEXTA – ALTERAÇÕES

16.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021.

16.2. O Contratado é obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou as supressões que se fizerem necessário, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

16.3. As alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, submetido à prévia aprovação da consultoria jurídica do contratante, salvo nos casos de justificada necessidade de antecipação de seus efeitos, hipótese em que a formalização do aditivo deverá ocorrer no prazo máximo de 1 (um) mês (art. 132 da Lei nº 14.133, de 2021).

16.4. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133, de 2021.

CLÁUSULA DÉCIMA SÉTIMA – PUBLICAÇÃO

17.1. Incumbirá ao Contratante divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133, de 2021, bem como no respectivo sítio oficial na Internet, em atenção ao art. 91, caput, da Lei n.º 14.133, de 2021, e ao art. 8º, §2º, da Lei n. 12.527, de 2011, c/c art. 7º, §3º, inciso V, do Decreto n. 7.724, de 2012.

CLÁUSULA DÉCIMA OITAVA – FORO (art. 92, §1º)

18.1. Fica eleito o Foro da Justiça Federal, Seção Judiciária de Porto Alegre/RS, para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não puderem ser compostos pela conciliação, conforme art. 92, § 1º, da Lei nº 14.133, de 2021.

Porto Alegre/RS, xxx de xxxx de 2026.

_____

Eduardo Freitas da Rosa

Representante legal do CONTRATANTE

_____

xxxxxxx

Representante legal do CONTRATADO