DOCUMENTO DE FORMALIZAÇÃO DA DEMANDA – DFD

CONTRATAÇÃO DE SOLUÇÃO CORPORATIVA DE ANTIVÍRUS

SETOR REQUISITANTE (UNIDADE ADMINISTRATIVA):	
Diretoria Administrativa	
Responsável pela formalização da demanda:	**Matricula:**
Francisco Lira Mororó	112.0271
E-mail:	**Telefone/Ramal:**
administrativo@ipmpparagominas.pa.gov.br	(91) 98200-2322

1. DADOS GERAIS SOBRE O SERVIÇO

1.1. Objeto

1.1.1. Contratação de solução corporativa de antivírus, baseada em software, destinada a prover proteção avançada, detecção e resposta a ameaças digitais no ambiente computacional do Instituto de Previdência Municipal de Paragominas – IPMP pelo prazo de 24 (vinte e quatro) meses, incluindo o licenciamento e a prestação dos serviços de atualização e suporte para garantir a continuidade da proteção proativa e a integridade dos sistemas de Tecnologia da Informação e Comunicação (TIC) da Autarquia contra softwares maliciosos, tais como vírus, trojans, worms e, especialmente, ransomwares.

1.2 Descrição da Solução

1.2.1. A solução corporativa de antivírus constitui um sistema integrado de proteção contra ameaças cibernéticas, composto por:

a) Software Antivírus Corporativo: Aplicação de proteção em tempo real, instalada em estações de trabalho e servidores, operando continuamente para detectar e neutralizar ameaças antes que comprometam os sistemas.

b) Atualização Contínua de Assinaturas: Sistema automático de atualização de definições de vírus e malwares, com frequência mínima diária, garantindo proteção contra ameaças mais recentes.

c) Detecção Comportamental e Heurística: Capacidade de identificar ameaças zero-day e ransomwares sofisticados através de análise comportamental de arquivos e processos.

d) Resposta Automática a Ameaças: Isolamento automático de sistemas comprometidos, quarentena de arquivos suspeitos e bloqueio de atividades maliciosas.

e) Suporte Técnico Especializado: Assistência técnica durante toda a vigência do contrato para resolução de incidentes de segurança e orientação sobre melhores práticas.

f) Relatórios de Segurança: Geração de relatórios detalhados sobre ameaças detectadas, atividades de proteção e status de segurança dos sistemas, facilitando auditoria e conformidade.

2. JUSTIFICATIVA DA NECESSIDADE DA CONTRATAÇÃO

2.1. O Instituto de Previdência Municipal de Paragominas – IPMP é uma autarquia responsável pela gestão de benefícios previdenciários e processamento de dados sensíveis de beneficiários. Sua infraestrutura de Tecnologia da Informação e Comunicação (TIC) é crítica para a continuidade dos serviços institucionais.

2.2. Atualmente, o parque tecnológico do IPMP enfrenta riscos significativos de comprometimento por ameaças cibernéticas, particularmente ransomwares, que representam uma das maiores ameaças à segurança de dados e continuidade operacional de instituições públicas.

2.3. Justificativas Específicas:

2.3.1. Proteção de Dados Sensíveis: O IPMP processa informações pessoais e financeiras de beneficiários, que devem ser protegidas contra acesso não autorizado e roubo de dados. Ataques cibernéticos podem comprometer a confidencialidade, integridade e disponibilidade desses dados.

2.3.2. Continuidade Operacional: Ataques por ransomware podem paralisar completamente as operações do Instituto, impedindo o pagamento de benefícios e prestação de serviços essenciais. A proteção preventiva é fundamental para garantir continuidade.

2.3.3. Conformidade Regulatória: Instituições públicas têm obrigação legal de implementar medidas adequadas de segurança da informação, conforme normas como ABNT NBR ISO/IEC 27001 e exigências de órgãos de controle.

2.3.4. Redução de Riscos Financeiros: Ataques cibernéticos bem-sucedidos podem resultar em perdas financeiras significativas, custos de recuperação de dados, pagamento de resgate (no caso de ransomware) e indenizações por vazamento de dados.

2.3.5. Reputação Institucional: Incidentes de segurança comprometem a confiança de beneficiários e da sociedade na instituição. A proteção proativa demonstra compromisso com segurança.

2.3.6. Ausência de Solução Atual: O IPMP não dispõe atualmente de solução corporativa adequada de antivírus, deixando o parque tecnológico exposto a riscos inaceitáveis.

3. DO GRAU DE PRIORIDADE DA CONTRATAÇÃO

3.1. Grau de Prioridade: ALTA

3.2. Justificativa:

3.2.1. A contratação de solução corporativa de antivírus é considerada de alta prioridade pelos seguintes motivos:

a) Criticidade da Infraestrutura: Os sistemas de TIC do IPMP são críticos para a continuidade operacional da Autarquia. Qualquer comprometimento impacta diretamente na prestação de serviços previdenciários essenciais.

b) Ameaças Crescentes: O cenário de ameaças cibernéticas está em constante evolução. Ransomwares sofisticados e ataques direcionados a instituições públicas aumentam significativamente a cada ano.

c) Impacto Potencial Severo: Um ataque bem-sucedido poderia resultar em paralisação total das operações, perda irreversível de dados, exposição de informações sensíveis e danos financeiros e reputacionais graves.

d) Obrigação Legal: A implementação de medidas de segurança da informação é obrigação legal, não opcional. A ausência de proteção adequada expõe a Autarquia a responsabilidades legais.

e) Previsão no Plano Anual: A contratação está prevista no Plano de Contratações Anual do IPMP, confirmando sua importância estratégica.

f) Urgência Operacional: Quanto mais tempo o parque tecnológico permanecer desprotegido, maior o risco de comprometimento. A implementação deve ocorrer com brevidade.

4. DIMENSIONAMENTO DO SERVIÇO A SER CONTRATADO

4.1 Escopo de Cobertura

4.1.1. A solução corporativa de antivírus deve cobrir toda a infraestrutura de TIC do IPMP, incluindo:

a) Estações de trabalho (computadores de mesa e notebooks);

b) Servidores de aplicação e banco de dados;

c) Servidores de arquivo e armazenamento;

d) Demais equipamentos que processem dados institucionais.

4.2. Quantidade Estimada de Licenças

4.2.1. Baseado no levantamento do parque tecnológico do IPMP, estima-se a necessidade de licenciamento para aproximadamente **15 a 20 equipamentos** (estações de trabalho e servidores), podendo este número ser ajustado conforme inventário final realizado previamente à contratação.

4.3. Período de Vigência

4.3.1. A solução será contratada pelo período de **24 (vinte e quatro) meses contínuos**, a contar da data de assinatura do contrato.

4.4. Nível de Serviço Esperado

4.4.1. Disponibilidade: Mínimo 99% do tempo de operação;

4.4.2. Atualização de Assinaturas: Mínimo diariamente;

4.4.3. Tempo de Resposta a Incidentes: Máximo 4 horas para problemas críticos;

4.4.4. Resolução de Chamados de Suporte: Máximo 48 horas para problemas críticos.

5. PARTICULARIDADE DO SERVIÇO A SER EXECUTADO

5.1 Características Específicas

5.1.1. A solução corporativa de antivírus apresenta as seguintes particularidades:

a) Serviço Contínuo: Trata-se de serviço contínuo de proteção, que deve funcionar ininterruptamente durante toda a vigência do contrato, 24 horas por dia, 7 dias por semana.

b) Atualização Automática: A solução deve atualizar automaticamente suas definições de vírus e malwares, sem necessidade de intervenção manual constante.

c) Integração com Infraestrutura Existente: A solução deve integrar-se adequadamente com os sistemas operacionais e aplicações já em uso no IPMP, sem causar conflitos ou incompatibilidades.

d) Suporte Técnico Especializado: O fornecedor deve disponibilizar suporte técnico especializado em segurança cibernética, capaz de resolver incidentes complexos.

e) Conformidade com Normas: A solução deve estar em conformidade com normas de segurança da informação aplicáveis, particularmente ABNT NBR ISO/IEC 27001.

f) Relatórios e Auditoria: A solução deve gerar relatórios detalhados que permitam auditoria de segurança e demonstração de conformidade com requisitos regulatórios.

5.2. Requisitos de Execução

5.2.1. Instalação e configuração inicial sem custo adicional;

5.2.2. Treinamento básico para usuários finais;

5.2.3. Documentação técnica completa;

5.2.4. Garantia de continuidade de serviço sem interrupções não autorizadas.

6. DESCRIÇÃO DOS SERVIÇOS

6.1. Serviços Principais

6.1.1. Licenciamento de Software Antivírus: Fornecimento de licenças de software antivírus corporativo para instalação em todos os equipamentos designados do IPMP.

6.1.2. Instalação e Configuração Inicial: Instalação e configuração do software em todos os equipamentos, incluindo parametrização de políticas de proteção conforme requisitos do IPMP.

6.1.3. Proteção em Tempo Real: Operação contínua do software para detecção e neutralização de ameaças em tempo real, incluindo:

a) Varredura de arquivos ao acesso;

b) Monitoramento de atividades suspeitas;

c) Bloqueio automático de malwares conhecidos;

d) Detecção de comportamentos anormais.

6.1.4. Atualização Contínua: Atualização automática de assinaturas de vírus e definições de segurança, com frequência mínima diária, garantindo proteção contra ameaças mais recentes.

6.1.5. Detecção e Resposta a Ameaças: Capacidade de detectar e responder automaticamente a ameaças, incluindo:

a) Detecção comportamental e heurística;

b) Isolamento de sistemas comprometidos;

c) Quarentena de arquivos suspeitos;

d) Bloqueio de atividades maliciosas.

6.1.6. Suporte Técnico Especializado: Prestação de serviços de suporte técnico especializado, incluindo:

a) Assistência para resolução de incidentes de segurança;

b) Orientação sobre melhores práticas de segurança;

c) Resposta a dúvidas técnicas;

d) Gestão centralizada de políticas de proteção.

6.1.7. Relatórios de Segurança: Geração de relatórios periódicos sobre:

a) Ameaças detectadas e neutralizadas;

b) Atividades de proteção realizadas;

c) Status de segurança dos sistemas;

d) Recomendações de melhorias.

6.1.8. Serviços Complementares

a) Treinamento básico para usuários finais sobre funcionalidades do software;

b) Documentação técnica completa e manual de procedimentos;

c) Suporte para integração com sistemas existentes;

d) Assistência para resolução de conflitos com outras aplicações.

7. ESTIMATIVA DA QUANTIDADE

7.1. Quantidade de Licenças: 15 a 20 licenças de software antivírus corporativo.

7.2. Justificativa: Estimativa baseada no levantamento preliminar do parque tecnológico do IPMP, considerando estações de trabalho, servidores e demais equipamentos que processem dados institucionais. A quantidade final será confirmada mediante inventário detalhado realizado previamente à contratação.

7.3. Período de Cobertura: 24 (vinte e quatro) meses contínuos

7.4. Escopo: Toda a infraestrutura de TIC do Instituto de Previdência Municipal de Paragominas – IPMP.

8. ESTIMATIVA PRELIMINAR DO VALOR DA CONTRATAÇÃO

8.1. O valor global estimado para a contratação é de R$ 8.144,88 (oito mil cento e quarenta e quatro reais e oitenta e oito centavos), para o período de 24 (vinte e quatro) meses, correspondendo ao valor mensal aproximado de R$ 339,37 (trezentos e trinta e nove reais e trinta e sete centavos).

8.2. A estimativa foi elaborada com base em pesquisa de mercado, considerando o porte do parque tecnológico do IPMP, o período de vigência contratual, bem como a inclusão de licenciamento, atualizações e suporte técnico da solução.

8.3. Foram utilizados como referência valores praticados por fornecedores de softwares corporativos similares, conforme demonstrado abaixo:

Software	Descrição	Qd	Valor Unitário	Total
Alus It Security	KL4066KAMDP – Kaspersky Next EDR Optimum Brazilian Edition. 2 year Public Sector License	15	R$ 279,60	R$ 6.710,40
AIM7	KL4066 Kaspersky Next EDR Optimum – 2 anos	15	R$ 369,13	R$ 8.859,00
Kaspersky	Kaspersky Next EDR Optimum	15	R$ 369,38	R$ 8.865,00
		MÉDIA	**R$ 339,37**	**R$ 8.144,88**

8.4. O valor estimado poderá ser validado mediante pesquisa de preços junto a fornecedores do ramo, em conformidade com a Lei nº 14.133/2021.

9. PERÍODO DE VIGÊNCIA

9.1. O período de vigência do contrato é de **24 (vinte e quatro) meses contínuos**, contados a partir da data de assinatura do contrato. Durante toda a vigência, o fornecedor deverá garantir continuidade ininterrupta da proteção contra ameaças cibernéticas, sem lacunas ou períodos de vulnerabilidade.
9.2. Conforme legislação aplicável e avaliação de desempenho da solução, poderá haver renovação do contrato por períodos adicionais, mediante novo processo de contratação.

10. PRAZO DE EXECUÇÃO

10.1. A contratada deverá iniciar a execução no prazo de **10 (dez) dias úteis** contados a partir da data de assinatura do contrato.

10.2. Durante este período inicial, deverá realizar o levantamento detalhado do parque tecnológico do IPMP e confirmação de quantidade de equipamentos (dias 1-3), instalação do software antivírus em

todos os equipamentos designados conforme cronograma acordado (dias 4-7), e configuração final, testes de funcionamento, treinamento básico de usuários e documentação técnica (dias 8-10).

10.3. Ao final dos 10 dias úteis, a solução corporativa de antivírus deverá estar em plena operação em todos os equipamentos, com proteção ativa e contínua.

10.4. Após este período inicial, a solução deverá funcionar continuamente durante toda a vigência do contrato de 24 meses, com atualização automática de assinaturas de vírus, detecção de ameaças, suporte técnico permanente e geração de relatórios periódicos de segurança.

Paragominas/PA, 19 de maio de 2026.

Elaborado por:

ELIZAMARA SILVA COSTA:99982536249
Assinado de forma digital por ELIZAMARA SILVA COSTA:99982536249
Dados: 2026.05.20 17:03:34 -03'00'

Elizamara Silva Costa
Auxiliar Adm. do IPMP

Revisado por:

FRANCISCO LIRA MORORO:93139756291
Assinado de forma digital por FRANCISCO LIRA MORORO:93139756291

Francisco Lira Mororó
Diretor Administrativo

Aprovado do por:

CARMELINA FELIX DE MORAES BRANDAO:37678116268
Assinado de forma digital por CARMELINA FELIX DE MORAES BRANDAO:37678116268
Dados: 2026.06.26 10:28:51 -03'00'

Carmelina Felix de Moraes Brandão
Presidente do IPMP