EDITAL SIMPLIFICADO – CONTRATAÇÃO DIRETA - DISPENSA ELETRÔNICA Nº 001/2026 (PROCESSO Nº1232/2025) - ID CidadEs Contratações: 2026.069E0800001.09.0005

O **INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES DO MUNICÍPIO DE SERRA–IPS-ES, torna público para conhecimento dos interessados, que realizará contratação direta em razão do valor, com fulcro no Art. 75, II, Lei Federal nº 14.133/21, através do sítio** https://licitacoes-e2.bb.com.br. As propostas serão julgadas pelo "menor preço" GLOBAL, de acordo com as normas pertinentes à Lei Federal nº 14.133/21, bem como a Lei 123/2006 (tratamento diferenciado para EPP/ME), consoante as condições estabelecidas neste Edital e em conformidade com a solicitação do Setor Demandante.

ABERTURA PARA PROPOSTAS	26/06/2026 – 17:00 HORAS
ENCERRAMENTO DAS PROPOSTAS	02/07/2026 - 10:00 HORAS
INÍCIO DA SESSÃO	02/07/2026 - 10:00 HORAS
FIM DA SESSÃO	02/07/2026 – 18:00 HORAS

1. OBJETO DA CONTRATAÇÃO DIRETA

1.1. Contratação de **empresa para o fornecimento de licença de antivirus corporavivo, incluindo instalação e suporte**, para os exercícios de 2026-2028, conforme condições, quantidades e exigências estabelecidas neste Instrumento;

1.2. Em caso de discordância existente entre as especificações deste objeto descritas no e-licitacao e as constantes deste Termo de Referência, prevalecerão as últimas, inclusive para fins de desclassificação da proposta;

1.3. A contratação será formada por 01 (um) item em único lote, conforme tabela constante a seguir:

LOTE ÚNICO – CONTRATAÇÃO DE EMPRESA PARA O FORNECIMENTO DE LICENÇA DE ANTIVIRUS CORPORATIVO, INCLUINDO INSTALAÇÃO E SUPORTE					
ITEM	**PRODUTO**	**DESCRIÇÃO/ESPECIFICAÇÃO**	**QTD**	**UND**	**VALOR UNT.**
01	ANTIVIRUS	Solução Corporativa de Antivírus pelo período de no mínimo 36 (trinta e seis) meses.	60	Unid.	R$ 141,66
					Total – R$ 8.499,60

1.4. O critério de julgamento e seleção da melhor proposta será o de menor preço por item, observadas as exigências contidas neste Edital de Contratação Direta.

2. PARTICIPAÇÃO NA DISPENSA ELETRÔNICA

2.1. A participação na presente dispensa eletrônica se dará mediante Sistema, disponível no endereço eletrônico https://licitacoes-e2.bb.com.br.

2.1.1. Os fornecedores deverão atender aos procedimentos previstos no Manual do

Sistema de Dispensa Eletrônica, disponível no Portal eletrônico https://licitacoes-e2.bb.com.br, para acesso ao sistema e operacionalização;

2.1.2. 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. Não poderão participar desta dispensa os fornecedores:

2.2.1. Que não atendam às condições deste Edital de Contratação Direta e seu(s) anexo(s);

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

2.2.3. Que se enquadrem nas seguintes vedações:

a) Pessoa Física ou Jurídica que se encontre, ao tempo da contratação, impossibilitada de contratar em decorrência de sanção que lhe foi imposta;

b) 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 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;

c) 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.

3. INGRESSO NA DISPENSA ELETRÔNICA E CADASTRAMENTO DA PROPOSTA INICIAL

3.1. O ingresso do fornecedor na disputa da dispensa eletrônica se dará 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, até a data e o horário estabelecidos para abertura do início da etapa de lances;

3.2.1. A proposta também 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.

3.3. Todas as especificações do objeto contidas na proposta, em especial o preço, 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 prestação dos serviços;

3.4.1. 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 a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses.

3.6. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe neste aviso e seus anexos **I - Documentos de habilitação; II** - **Termo de Referência**, assumindo o proponente o compromisso de executar os serviços nos seus termos.

3.7. No cadastramento da proposta inicial, o fornecedor deverá, também, assinalar "sim" ou "não" em campo próprio do sistema eletrônico, às seguintes declarações:

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

3.7.2. 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.

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

3.7.4. Que assume a responsabilidade pelas transações que forem efetuadas no sistema, assumindo como firmes e verdadeiras;

3.7.5. 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 8.213/91;

3.7.6. 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.

4. FASE DE LANCES

4.1. A partir das **09:00h da data estabelecida neste Edital 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;

4.1.1. O lance deverá ser ofertado pelo valor de cada item.

4.2. O fornecedor somente poderá oferecer valor inferior ou maior percentual de desconto em relação ao último lance por ele ofertado e registrado pelo sistema;

4.2.1. 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$ 1,00 (um real).**

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

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

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

4.6. 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;

4.6.1. 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 DAS PROPOSTAS DE PREÇO

5.1. Encerrada a fase de lances, será verificada a conformidade da proposta classificada em primeiro lugar quanto à adequação do objeto e à compatibilidade do preço em relação ao estipulado para a contratação.

5.2. No caso de o preço da proposta vencedora estar acima do estimado pela Administração, poderá haver a negociação de condições mais vantajosas;

5.2.1. Neste caso, será encaminhada contraproposta ao fornecedor que tenha apresentado a melhor proposta, para que seja obtida melhor proposta com preço compatível ao estimado pela Administração;

5.2.2. A negociação poderá ser feita com os demais fornecedores classificados, 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 definido para a contratação;

5.2.3. Em qualquer caso, concluída a negociação, o resultado será registrado no relatório do procedimento da dispensa eletrônica.

5.3. Estando o preço compatível, será solicitado o envio da proposta e, se necessário, de documentos complementares, adequada ao último lance.

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

5.5. O critério de julgamento será o melhor preço por item.

5.6. Será desclassificada a proposta vencedora que:

5.6.1. Apresentar preços unitários ou globais acima dos valores estabelecidos como de referência máxima.

5.6.2. Contiver vícios insanáveis;

5.6.3. Não obedecer às especificações técnicas pormenorizadas neste aviso ou em seus anexos;

5.6.4. Apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;

5.6.5. Não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

5.6.6. Apresentar desconformidade com quaisquer outras exigências deste aviso ou seus anexos, desde que insanável.

5.7. 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;

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

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

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

6. HABILITAÇÃO

6.1. Os documentos a serem exigidos para fins de habilitação constam do **ANEXO I – DOCUMENTAÇÃO EXIGIDA PARA HABILITAÇÃO** deste aviso e serão solicitados do fornecedor melhor classificado da fase de lances.

7. CONTRATAÇÃO

7.1. Após a homologação e adjudicação, caso se conclua pela contratação, será emitida Nota de empenho e ordem de fornecimento.

7.2. O Aceite da Nota de Empenho ou do instrumento equivalente, emitida à empresa adjudicada, implica no reconhecimento de que:

7.2.1. Referida Nota está vinculada ao contrato, aplicando-se à relação de negócios ali estabelecida as disposições da Lei nº 14.133, de 2021;

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

7.2.3. A contratada reconhece que as hipóteses de rescisão são aquelas previstas nos artigos 137 e 138 da Lei nº 14.133/21 e reconhece os direitos da Administração previstos nos artigos 137 a 139 da mesma Lei, bem como as regras contidas no contrato.

7.3. 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 da contratação.

8. DAS DISPOSIÇÕES GERAIS

8.1. O procedimento será divulgado no Portal Nacional de Contratações Públicas - PNCP, bem como no Portal de Publicações do IPS (https://transparencia.ips.es.gov.br/licitacoes) e Diário Oficial do Estado.

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

8.2.1. Republicar o presente aviso com uma nova data;

8.2.2. 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.

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

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

8.3. Os documentos solicitados (proposta ajustada, documentos de habilitação ou documentações complementares) deverão ser enviados no prazo máximo de 1h (uma hora) após o pedido, salvo :

8.12.1 Se perto do encerramento do expediente oficial, quando o agente de contratação poderá conferir prazo maior visando prosseguir a análise em dia útil subsequente;

8.12.2 Se pela complexidade do objeto ou tamanho do lote houver necessidade conferir prazo maior;

8.4. Caberá ao fornecedor acompanhar as operações no sistema, ficando responsável pelo ônus decorrente da perda do negócio diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

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

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

8.7. Os fornecedores se submetem as sanções previstas na lei 14.133 de 2021, bem como àquelas expressamente previstas no Termo de Referência e nos anexos deste Aviso de Dispensa Eletrônica.

8.7.1. ANEXO I – Documentação exigida para Habilitação.

8.7.2. ANEXO II – Termo de Referência;

Serra/ES, 26 de junho de 2026.

Alinny Souza Tomaz
Agente de Contratações/Pregoeiro
Nos termos da Portaria IPS Nº 289, de 10 de setembro de 2025

ANEXO I
DOCUMENTAÇÃO EXIGIDA PARA HABILITAÇÃO

1. Habilitação jurídica:

1.1. No caso de empresário individual, inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

1.2. Em se tratando de Microempreendedor Individual – MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio www.portaldoempreendedor.gov.br;

1.3. No caso de sociedade empresária ou empresa individual de responsabilidade limitada - EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede;

1.4. Inscrição no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz, no caso de ser o participante sucursal, filial ou agência;

1.5. No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;

1.6. Decreto de autorização, em se tratando de sociedade empresária estrangeira em funcionamento no País;

2. Regularidade fiscal, social e trabalhista:

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

2.2. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02/10/2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

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

2.4. 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;

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

2.6. Caso o fornecedor seja considerado isento dos tributos estaduais e/ou municipais 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;

3. Qualificação Econômico-Financeira:

3.1 Apresentar Certidão Negativa de pedido de Falência, Concordata ou recuperação judicial/extrajudicial, expedida pelo(s) distribuidor(es) da sede da pessoa jurídica e quando se tratar de Sociedades Simples apresentar Certidão Negativa dos Distribuidores Cíveis, com data não superior a 60 (sessenta) dias de sua emissão, quando não for expresso sua validade.

4. Qualificação Técnica:

4.1 Comprovação de aptidão para desempenho de atividade pertinente e compatível com o objeto da dispensa de licitação fornecido por pessoa jurídica de direito público ou privado, em papel timbrado para ambos, contendo razão social, endereço, telefone, CNPJ e quantitativos dos serviços executados ou de características similares.

4.2 O proponente disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando quando requerido pela Autoridade Solicitante, dentre outros documentos, cópia do contrato e/ou Notas Fiscais que deram suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços.

ANEXO II

TERMO DE REFERÊNCIA

UNIDADE REQUISITANTE: Divisão de Tecnologia da Informação

1. DO OBJETO

O presente Termo de Referência tem por objeto a **CONTRATAÇÃO DE EMPRESA PARA O FORNECIMENTO DE LICENÇA DE ANTIVIRUS CORPORATIVO, INCLUINDO INSTALAÇÃO E SUPORTE**, conforme especificações e quantitativos abaixo.

2. DA JUSTIFICATIVA

Atualmente, o parque tecnológico do Instituto de Previdência dos Servidores do Município da Serra (IPS) conta com uma solução de proteção de *endpoint* (antivírus) cuja licença de uso possui data de expiração prevista para **27/12/2025**. A não renovação ou substituição tempestiva desta solução deixará a infraestrutura do Instituto vulnerável a ataques cibernéticos, comprometendo a continuidade dos serviços previdenciários.

A vigência da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 - LGPD) impõe às instituições públicas rigorosos padrões de governança e segurança da informação. O IPS, na qualidade de Controlador de dados, realiza o tratamento de um alto volume de informações pessoais e dados sensíveis (financeiros e de saúde) de servidores, aposentados e pensionistas. A LGPD estabelece, em seu Art. 46, que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas. Portanto, a manutenção de um software de proteção robusto não é apenas uma medida de TI, mas uma obrigação legal para garantir os princípios da confidencialidade, integridade e disponibilidade, mitigando riscos de sanções administrativas e danos à reputação institucional.

Com a contratação de licenças para 60 estações de trabalho, o Departamento de Tecnologia da Informação busca blindar o ambiente corporativo contra ameaças avançadas, exigindo uma solução que combine defesa automatizada contra malwares, ransomwares e ataques de "dia zero" — utilizando inteligência artificial e análise heurística — com ferramentas de Prevenção de Vazamento de Dados (DLP). O sistema deve oferecer gestão centralizada, preferencialmente em nuvem, para o controle integral de atualizações, dispositivos USB, tráfego de internet e políticas de segurança, garantindo assim a eficiência operacional e a continuidade dos serviços digitais prestados aos segurados ao minimizar o tempo de inatividade decorrente de incidentes de segurança.

3. DO DETALHAMENTO DO OBJETO

Será considerado como “Solução de Antivírus Corporativo” o conjunto de software capaz de varrer, detectar, analisar e remover: vírus, spyware, worms, trojans, rootkits, grayware, que tenha recursos anticryptor para barrar cryptolockers e ransomware e demais softwares maliciosos agindo de forma integrada e com gerenciamento centralizado em nuvem, provendo mecanismos de bloqueios automáticos entre conexões de rede maliciosas, segurança web (bloqueio de sites, downloads suspeitos) e de e-mails (filtros de phishing e anexos) e ainda console gerenciado em nuvem.

Para efeito deste Termo de Referência, será considerado como "Pacote de Vacinas" a relação dos arquivos de atualização das vacinas de antivírus, antispyware e qualquer antimalware no qual o sistema esteja apto a detectar e eliminar.

LOTE ÚNICO – CONTRATAÇÃO DE EMPRESA PARA O FORNECIMENTO DE LICENÇA DE ANTIVIRUS CORPORATIVO, INCLUINDO INSTALAÇÃO E SUPORTE		
ITEM	**DESCRIÇÃO**	**UNID.**
1	Solução Corporativa de Antivírus pelo período de no mínimo 36 (trinta e seis) meses	60

O software e licenças de informática deverão possuir as seguintes especificações gerais:

3.1. Servidor de Administração e Console Administrativa

3.1.1. Compatibilidade:

3.1.1.1. Microsoft Windows Server 2012 (Todas edições x64);
3.1.1.2. Microsoft Windows Server 2012 R2 (Todas edições x64);
3.1.1.3. Microsoft Windows Server 2016 x64 ou superior;
3.1.1.4. Microsoft Windows Server 2022 x64 ou superior;
3.1.1.5. Microsoft Windows 10 Pro/Enterprise x86/x64;
3.1.1.6. Microsoft Windows 11 Pro/Pro para Estações de Trabalho ou superior.

3.1.2. Suporte as seguintes plataformas virtuais:

3.1.2.1. Vmware: vSphere 5.5 e vSphere 6 ou superior.

3.1.3. Características:

3.1.3.1. A console deve ser acessada via WEB (HTTPS), MMC ou software proprietário;
3.1.3.2. Console deve ser baseada no modelo cliente/servidor;
3.1.3.3. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;
3.1.3.4. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;
3.1.3.5. Deve permitir incluir usuários do Active Directory (AD) para logarem na console de administração;
3.1.3.6. Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM;
3.1.3.7. As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;
3.1.3.8. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;
3.1.3.9. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de D;

3.1.3.10. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
3.1.3.11. Deve armazenar histórico das alterações feitas em políticas;
3.1.3.12. Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada;
3.1.3.13. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas;
3.1.3.14. A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;
3.1.3.15. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;
3.1.3.16. Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS e Android;
3.1.3.17. Capacidade de instalar remotamente qualquer “app” em smartphones e tablets de sistema iOS;
3.1.3.18. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;
3.1.3.19. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário;
3.1.3.20. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;
3.1.3.21. Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança;
3.1.3.22. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede;
3.1.3.23. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;
3.1.3.24. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;
3.1.3.25. Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;
3.1.3.26. A comunicação entre o cliente e o servidor de administração deve ser criptografada;
3.1.3.27. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;
3.1.3.28. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

- Nome do computador;
- Nome do domínio;
- Range de IP;
- Sistema Operacional;
- Máquina virtual.

3.1.3.29. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;
3.1.3.30. Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional;

3.1.3.31. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;

3.1.3.32. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção;

3.1.3.33. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;

3.1.3.34. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias, etc;

3.1.3.35. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;

3.1.3.36. Deve fornecer as seguintes informações dos computadores:

3.1.3.36.1. Se o antivírus está instalado;

3.1.3.36.2. Se o antivírus está iniciado;

3.1.3.36.3. Se o antivírus está atualizado;

3.1.3.36.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo;

3.1.3.36.5. Minutos/horas desde a última atualização de vacinas;

3.1.3.36.6. Data e horário da última verificação executada na máquina;

3.1.3.36.7. Versão do antivírus instalado na máquina;

3.1.3.36.8. Se é necessário reiniciar o computador para aplicar mudanças;

3.1.3.36.9. Data e horário de quando a máquina foi ligada;

3.1.3.36.10. Quantidade de vírus encontrados (contador) na máquina;

3.1.3.36.11. Nome do computador;

3.1.3.36.12. Domínio ou grupo de trabalho do computador;

3.1.3.36.13. Data e horário da última atualização de vacinas;

3.1.3.36.14. Sistema operacional com Service Pack;

3.1.3.36.15. Quantidade de processadores;

3.1.3.36.16. Quantidade de memória RAM;

3.1.3.36.17. Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);

3.1.3.36.18. Endereço IP;

3.1.3.36.19. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;

3.1.3.36.20. Atualizações do Windows Updates instaladas;

3.1.3.36.21. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;

3.1.3.36.22. Vulnerabilidades de aplicativos instalados na máquina.

3.1.3.37. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;

3.1.3.38. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:
3.1.3.38.1. Alteração de Gateway Padrão;
3.1.3.38.2. Alteração de subrede;
3.1.3.38.3. Alteração de domínio;
3.1.3.38.4. Alteração de servidor DHCP;
3.1.3.38.5. Alteração de servidor DNS;
3.1.3.38.6. Alteração de servidor WINS;
3.1.3.38.7. Resolução de Nome;
3.1.3.38.8. Disponibilidade de endereço de conexão SSL.

3.1.3.39. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
3.1.3.40. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
3.1.3.41. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
3.1.3.42. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
3.1.3.43. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;
3.1.3.44. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;
3.1.3.45. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;
3.1.3.46. Capacidade de gerar traps SNMP para monitoramento de eventos;
3.1.3.47. Capacidade de enviar e-mails para contas específicas em caso de algum evento;
3.1.3.48. Listar em um único local, todos os computadores não gerenciados na rede;
3.1.3.49. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes;
3.1.3.50. Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2012 Server ou superiores;
3.1.3.51. Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente;
3.1.3.52. Capacidade de ligar máquinas via Wake-on-Lan para realização de tarefas (varredura, atualização, instalação, etc), inclusive de máquinas que estejam em subnets diferentes do servidor;
3.1.3.53. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
3.1.3.54. Deve através de opções de optimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo porém sem comprometer o desempenho do computador;

3.1.3.55. Deve permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, (ex: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint);

3.1.3.56. Permitir fazer uma verificação rápida ou detalhada de um dispositivo removível assim que conectado no computador, podendo configurar a capacidade máxima em GB da verificação;

3.1.3.57. Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros;

3.1.3.58. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;

3.1.3.59. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:

- Nome do vírus;
- Nome do arquivo infectado;
- Data e hora da detecção;
- Nome da máquina ou endereço IP;
- Ação realizada.

3.1.3.60. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;

3.1.3.61. Capacidade de listar updates nas máquinas com o respectivo link para download;

3.1.3.62. Deve criar um backup de todos arquivos deletados em computadores para que possa ser restaurado através de comando na Console de administração;

3.1.3.63. Deve ter uma quarentena na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante;

3.1.3.64. Capacidade de realizar inventário de hardware de todas as máquinas clientes;

3.1.3.65. Capacidade de realizar inventário de aplicativos de todas as máquinas clientes;

3.1.3.66. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

3.2. Estações Windows

3.2.1. Compatibilidade:

3.2.1.1. Microsoft Windows 8 Professional/Enterprise x86/x64;

3.2.1.2. Microsoft Windows 8.1 Pro/Enterprise x86/x64;

3.2.1.3. Microsoft Windows 10 Pro/Enterprise x86/x64;

3.2.1.4. Microsoft Windows 11 Pro/Pro para Estações de Trabalho;

3.2.1.5. Microsoft Windows Server 2012 R2 Standard x64;

3.2.1.6. Microsoft Windows Server 2012 Foundation x64;

3.2.1.7. Microsoft Windows Server 2012 Standard x64;

3.2.1.8. Microsoft Windows Server 2016 x64 ou superior.

3.2.2. Características:

3.2.2.1. Deve prover as seguintes proteções:

3.2.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
3.2.2.1.2. Antivírus de Web (módulo para verificação de sites e downloads contra vírus);
3.2.2.1.3. Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
3.2.2.1.4. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
3.2.2.1.5. Firewall com IDS;
3.2.2.1.6. Autoproteção (contra-ataques aos serviços/processos do antivírus);
3.2.2.1.7. Controle de dispositivos externos;
3.2.2.1.8. Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc.;
3.2.2.1.9. Controle de acesso a sites por horário;
3.2.2.1.10. Controle de acesso a sites por usuários;
3.2.2.1.11. Controle de acesso a websites por dados, ex: Bloquear websites com conteúdo de vídeo e áudio;
3.2.2.1.12. Controle de execução de aplicativos;
3.2.2.1.13. Controle de vulnerabilidades do Windows e dos aplicativos instalados.

3.2.2.2. Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
3.2.2.3. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
3.2.2.4. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
3.2.2.5. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
3.2.2.6. Capacidade de adicionar aplicativos a uma lista de “aplicativos confiáveis”, onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;
3.2.2.7. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
3.2.2.8. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
3.2.2.9. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
3.2.2.10. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas;
3.2.2.11. Capacidade de verificar somente arquivos novos e alterados;
3.2.2.12. Capacidade de verificar objetos usando heurística;
3.2.2.13. Capacidade de agendar uma pausa na verificação;
3.2.2.14. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;
3.2.2.15. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;

3.2.2.16. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
3.2.2.16.1. Perguntar o que fazer, ou;
3.2.2.16.2. Bloquear acesso ao objeto:
3.2.2.16.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
3.2.2.16.2.2. Caso positivo de desinfecção:
- Restaurar o objeto para uso;

3.2.2.16.2.3. Caso negativo de desinfecção:
- Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).

3.2.2.17. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
3.2.2.18. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, IMAP, NNTP, SMTP e MAPI;
3.2.2.19. Capacidade de verificar links inseridos em e-mails contra phishings;
3.2.2.20. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox e Opera;
3.2.2.21. Capacidade de verificação de corpo e anexos de e-mails usando heurística;
3.2.2.22. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:
3.2.2.22.1. Perguntar o que fazer, ou;
3.2.2.22.2. Bloquear o e-mail:
3.2.2.22.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
3.2.2.22.2.2. Caso positivo de desinfecção:
- Restaurar o e-mail para o usuário;

3.2.2.22.2.3. Caso negativo de desinfecção:
- Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador).

3.2.2.23. Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;
3.2.2.24. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;
3.2.2.25. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;
3.2.2.26. Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc.), usando heurísticas;
3.2.2.27. Deve ter suporte total ao protocolo Ipv6;
3.2.2.28. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;
3.2.2.29. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:
3.2.2.29.1. Perguntar o que fazer, ou;
3.2.2.29.2. Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;
3.2.2.29.3. Permitir acesso ao objeto.

3.2.2.30. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:

3.2.2.30.1. Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo-real, ou;

3.2.2.30.2. Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação.

3.2.2.31. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;

3.2.2.32. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;

3.2.2.33. Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;

3.2.2.34. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas;

3.2.2.35. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://www.antiphishing.org/);

3.2.2.36. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;

3.2.2.37. Deve possuir módulo IDS (Intrusion Detection System) para proteção contra port scans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas;

3.2.2.38. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

3.2.2.38.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

3.2.2.38.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

3.2.2.39. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:

3.2.2.39.1. Discos de armazenamento locais;

3.2.2.39.2. Armazenamento removível;

3.2.2.39.3. Impressoras;

3.2.2.39.4. CD/DVD;

3.2.2.39.5. Drives de disquete;

3.2.2.39.6. Modems;

3.2.2.39.7. Dispositivos de fita;

3.2.2.39.8. Dispositivos multifuncionais;

3.2.2.39.9. Leitores de smart card;

3.2.2.39.10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc.);

3.2.2.39.11. Wi-Fi;

3.2.2.39.12. Adaptadores de rede externos;

3.2.2.39.13. Dispositivos MP3 ou smartphones;

3.2.2.39.14. Dispositivos Bluetooth;

3.2.2.39.15. Câmeras e Scanners.

3.2.2.40. Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário;
3.2.2.41. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;
3.2.2.42. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;
3.2.2.43. Capacidade de habilitar "logging" em dispositivos removíveis tais como Pendrive, Discos externos, etc.;
3.2.2.44. Capacidade de configurar novos dispositivos por Class ID/Hardware ID;
3.2.2.45. Capacidade de limitar a execução de aplicativos por hash MD5, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc.);
3.2.2.46. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
3.2.2.47. Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo;
3.2.2.48. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web;
3.2.2.49. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web;
3.2.2.50. Capacidade de voltar ao estado anterior após um ataque de malware, incluindo recuperação de arquivos criptografados;
3.2.2.51. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros;
3.2.2.52. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

3.3. Estações de trabalho Linux

3.3.1. Compatibilidade:

3.3.1.1. Plataforma 32-bits/64-bits:
3.3.1.1.1. Ubuntu Versão LTS (suporte de no mínimo 12 meses) ou superior
3.3.1.1.2. Red Hat® Enterprise Linux® 6.10 ou superior
3.3.1.1.3. CentOS-7.9 ou superior
3.3.1.1.4. Debian GNU/Linux LTS (suporte de no mínimo 12 meses) ou superior
3.3.1.1.5. ALT Linux 8.2 ou superior
3.3.1.1.6. openSUSE Leap (suporte de no mínimo 12 meses) ou superior
3.3.1.1.7. Oracle Linux 7 ou superior
3.3.1.1.8. SUSE® Linux Enterprise Server LTSS (suporte de no mínimo 12 meses) ou superior

3.3.2. Características:

3.3.2.1. Deve prover as seguintes proteções:

3.3.2.2. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

3.3.2.3. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

3.3.2.4. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

3.3.2.5. Capacidade de criar exclusões por local, máscara e nome da ameaça;

3.3.2.6. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

3.3.2.7. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

3.3.2.8. Detectar aplicações que possam ser utilizadas como vetor de ataque por hackers;

3.3.2.9. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:

- Alta;
- Média;
- Baixa;
- Recomendado.

3.3.2.10. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;

3.3.2.11. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados;

3.3.2.12. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;

3.3.2.13. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

3.3.2.14. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

3.3.2.15. Capacidade de verificar objetos usando heurística;

3.3.2.16. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

3.3.2.17. Deve possuir módulo escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

3.3.2.18. Possibilidade de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

3.4. Servidores Windows

3.4.1. Compatibilidade:

3.4.1.1. Plataforma 64-bits

3.4.1.1.1. Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter;

3.4.1.1.2. Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter;

3.4.1.1.3. Windows Server 2016 Essentials/Standard/Datacenter/MultiPoint Premium Server;

3.4.1.1.4. Windows Server 2016 Core Standard/Datacenter;
3.4.1.1.5. Windows Storage Server 2016;
3.4.1.1.6. Windows Hyper-V Server 2016;
3.4.1.1.7. Windows Servers Superiores.

3.4.2. Características:

3.4.2.1. Deve prover as seguintes proteções:
3.4.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
3.4.2.1.2. Auto-proteção contra-ataques aos serviços/processos do antivírus;
3.4.2.1.3. Firewall com IDS;
3.4.2.1.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados.

3.4.2.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
3.4.2.3. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
3.4.2.4. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
3.4.2.4.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
3.4.2.4.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
3.4.2.4.3. Leitura de configurações;
3.4.2.4.4. Modificação de configurações;
3.4.2.4.5. Gerenciamento de Backup e Quarentena;
3.4.2.4.6. Visualização de relatórios;
3.4.2.4.7. Gerenciamento de relatórios;
3.4.2.4.8. Gerenciamento de chaves de licença;
3.4.2.4.9. Gerenciamento de permissões (adicionar/excluir permissões acima).

3.4.2.5. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
3.4.2.5.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
3.4.2.5.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

3.4.2.6. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total;
3.4.2.7. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede;
3.4.2.8. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc);
3.4.2.9. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS);

3.4.2.10. Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;
3.4.2.11. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;
3.4.2.12. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;
3.4.2.13. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;
3.4.2.14. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
3.4.2.15. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
3.4.2.16. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
3.4.2.17. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
3.4.2.18. Capacidade de verificar somente arquivos novos e alterados;
3.4.2.19. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.);
3.4.2.20. Capacidade de verificar objetos usando heurística;
3.4.2.21. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;
3.4.2.22. Capacidade de agendar uma pausa na verificação;
3.4.2.23. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
3.4.2.24. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
3.4.2.24.1. Perguntar o que fazer, ou;
3.4.2.24.2. Bloquear acesso ao objeto:
3.4.2.24.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
3.4.2.24.2.2. Caso positivo de desinfecção:

- Restaurar o objeto para uso;

3.4.2.24.2.3. Caso negativo de desinfecção:

- Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).

3.4.2.25. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
3.4.2.26. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
3.4.2.27. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

3.4.2.28. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa;
3.4.2.29. Capacidade de voltar ao estado anterior após um ataque de malware, incluindo recuperação de arquivos criptografados;
3.4.2.30. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros;
3.4.2.31. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

3.5. Servidores Linux

3.5.1. Compatibilidade:

3.5.1.1. Plataforma 32-bits/64-bits:
3.5.1.1.1. Ubuntu Versão LTS (suporte de no mínimo 12 meses) ou superior
3.5.1.1.2. Red Hat® Enterprise Linux® 6.10 ou superior
3.5.1.1.3. CentOS-7.9 ou superior
3.5.1.1.4. Debian GNU/Linux LTS (suporte de no mínimo 12 meses) ou superior
3.5.1.1.5. ALT Linux 8.2 ou superior
3.5.1.1.6. openSUSE Leap (suporte de no mínimo 12 meses) ou superior
3.5.1.1.7. Oracle Linux 7 ou superior
3.5.1.1.8. SUSE® Linux Enterprise Server LTSS (suporte de no mínimo 12 meses) ou superior

3.5.2. Características:

3.5.2.1. Deve prover as seguintes proteções:
3.5.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
3.5.2.1.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

3.5.2.2. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
3.5.2.2.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
3.5.2.2.2. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;
3.5.2.2.3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
3.5.2.2.4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

3.5.2.3. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;
3.5.2.4. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

3.5.2.5. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
3.5.2.6. Capacidade de verificar objetos usando heurística;
3.5.2.7. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
3.5.2.8. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
3.5.2.9. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

3.6. Smartphones e tablets

3.6.1. Compatibilidade:

3.6.1.1. Dispositivos com os sistemas operacionais:
3.6.1.1.1. Android com suporte e atualizações de segurança (mínimo de 12 meses à frente) ou superior;
3.6.1.1.2. iOS com suporte e atualizações de segurança (mínimo de 12 meses à frente) ou superior.

3.6.2. Características:

3.6.2.1. Deve prover as seguintes proteções:
3.6.2.1.1. Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:
3.6.2.1.2. Proteção contra adware e autodialers;
3.6.2.1.3. Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser;
3.6.2.1.4. Arquivos abertos no smartphone;
3.6.2.1.5. Programas instalados usando a interface do smartphone;
3.6.2.1.6. Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento.

3.6.2.2. Deverá isolar em área de quarentena os arquivos infectados;
3.6.2.3. Deverá atualizar as bases de vacinas de modo agendado;
3.6.2.4. Deverá bloquear spams de SMS através de Black lists;
3.6.2.5. Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado com mensagem de aviso ao utilizador do dispositivo;
3.6.2.6. Capacidade de desativar por política:

- Wi-fi;
- Câmera;
- Bluetooth.

3.6.2.7. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;
3.6.2.8. Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha;
3.6.2.9. Deverá ter firewall pessoal (Android);
3.6.2.10. Capacidade de tirar fotos quando a senha for inserida incorretamente;

3.6.2.11. Possibilidade de instalação remota utilizando o Microsoft System Center Mobile Device Manager 2012 ou superior;

3.6.2.12. Capacidade de enviar comandos remotamente de:

- Localizar;
- Bloquear.

3.6.2.13. Capacidade de detectar Jailbreak em dispositivos iOS;

3.6.2.14. Capacidade de bloquear o acesso a site por categoria em dispositivos;

3.6.2.15. Capacidade de bloquear o acesso a sites phishing ou malicioso;

3.6.2.16. Capacidade de bloquear o dispositivo quando o cartão "SIM" for substituído;

3.6.2.17. Capacidade de configurar White e blacklist de aplicativos;

3.6.2.18. Capacidade de localizar o dispositivo quando necessário;

3.6.2.19. Permitir atualização das definições quando estiver em "roaming";

3.6.2.20. Capacidade de selecionar endereço do servidor para buscar a definição de vírus;

3.6.2.21. Deve permitir verificar somente arquivos executáveis;

3.6.2.22. Deve ter a capacidade de desinfectar o arquivo se possível;

3.6.2.23. Capacidade de agendar uma verificação;

3.6.2.24. Capacidade de enviar URL de instalação por e-mail;

3.6.2.25. Capacidade de fazer a instalação através de um link QRCode;

3.6.2.26. Capacidade de executar as seguintes ações caso a desinfecção falhe:

- Deletar;
- Ignorar;
- Quarentenar;
- Perguntar ao usuário.

3.7. Gerenciamento de dispositivos móveis (MDM)

3.7.1. Compatibilidade:

3.7.1.1. Dispositivos com os sistemas operacionais:

3.7.1.1.1. Android com suporte e atualizações de segurança (mínimo de 12 meses à frente) ou superior;

3.7.1.1.2. iOS com suporte e atualizações de segurança (mínimo de 12 meses à frente) ou superior.

3.7.1.2. Softwares de gerência de dispositivos:

3.7.1.2.1. Kaspersky Security Center 12 e superior;

3.7.1.2.2. Kaspersky Endpoint Security Cloud 3.0 e superior;

3.7.1.2.3. VMWare AirWatch 9.2 e superior;

3.7.1.2.4. MobileIron 9.6 e superior;

3.7.1.2.5. IBM Maas360 10.66 e superior;

3.7.1.2.6. SOTI MobiControl 14.1.0 (1152) e superior.

3.7.2. Características:

3.7.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;

3.7.2.2. Capacidade de ajustar as configurações de:

3.7.2.2.1. Sincronização de e-mail;
3.7.2.2.2. Uso de aplicativos;
3.7.2.2.3. Senha do usuário;
3.7.2.2.4. Criptografia de dados;
3.7.2.2.5. Conexão de mídia removível.

3.7.2.3. Capacidade de instalar certificados digitais em dispositivos móveis;
3.7.2.4. Capacidade de, remotamente, resetar a senha de dispositivos iOS;
3.7.2.5. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;
3.7.2.6. Capacidade de, remotamente, bloquear um dispositivo iOS;
3.7.2.7. Deve permitir configurar horário para sincronização do dispositivo com a console de gerenciamento;
3.7.2.8. Permitir sincronização com perfil do "Touch Down";
3.7.2.9. Capacidade de desinstalar remotamente o antivírus do dispositivo;
3.7.2.10. Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual;
3.7.2.11. Capacidade de sincronizar com Samsung Knox;
3.7.2.12. Deve permitir criar perfis de políticas para out-of-office no caso de BYOD.

3.8. Informações gerais

3.8.1. Serão necessárias 60 (sessenta) licenças, entre Estações Windows e Linux e Servidores Windows Server Virtualizados em VMware vSphere 5.5;
3.8.2. Solução com tecnologias do EDR automatizado que se associam com abordagem em camadas visando equilíbrio entre desempenho e eficiência da proteção;
3.8.3. O presente T.R. descreve a estrutura mínima a ser fornecida para a implantação da solução de antivírus. A EMPRESA CONTRATADA também deverá assumir os custos com serviços, suporte, licenciamento e treinamento, sem ônus para o IPS;
3.8.4. A solução de antivírus deverá ser fornecida pronta para a utilização imediata do IPS, não será permitido qualquer procedimento que configure o desenvolvimento da solução após a contratação. Caso seja identificado tal procedimento, configurando desenvolvimento de solução, a solução não será aceita sendo aplicadas as penalidades cabíveis ao caso;
3.8.5. A solução deverá contemplar ferramentas que façam varreduras periódicas na rede a fim de localizar máquinas que, possivelmente, não estejam com o cliente do antivírus instalado no equipamento;
3.8.6. Configurar hora, semana, dia do mês e ainda em horários definidos pelo administrador da rede através de parâmetros de configuração das atualizações automáticas do antivírus;
3.8.7. Deverá ser possível, a critério do administrador da solução de antivírus, retornar a configuração anterior do Pacote de Vacinas e das Políticas de Segurança;
3.8.8. Deverá permitir a instalação dos softwares sem a necessidade de forçar a reinicialização da máquina;
3.8.9. Deverá possibilitar a atualização do Pacote de Vacinas definidas pelo administrador do sistema de forma automática através de um ou mais sites locais pré-definidos e também pela Internet;
3.8.10. A solução deverá rastrear em tempo real arquivos durante entrada e saída (gravação e leitura) no equipamento. Durante o rastreamento deverá limpar, apagar ou isolar o arquivo infectado conforme a política definida pelo administrador da Solução de Antivírus;

3.8.11. A solução deverá rastrear arquivos compactados para, no mínimo, os seguintes formatos:

- ZIP;
- ARJ;
- RAR;
- Microsoft Compress;
- Novos padrões de mercado.

3.8.12. Deverá ser possível, a critério do administrador da solução, a seleção de exclusão de pastas e arquivos que não devem ser rastreados;

3.8.13. Deverá permitir ao administrador bloquear os serviços de compartilhamento quando alvo de códigos maliciosos, no momento de uma epidemia, e, após o término desta, restaurar as configurações originais;

3.8.14. Deverá gerar notificações para o administrador de rede quando ocorrer uma epidemia de vírus através de e-mail;

3.8.15. Deverá ser possível a instalação e a desinstalação dos softwares da Solução de Antivírus, de forma automática, remota silenciosa, ou seja, de maneira que o usuário não perceba ou necessite interagir com o processo de instalação ou desinstalação do produto. Não será considerado como instalação remota, acesso a máquina do usuário usando recursos de terceiros como: teamviewer, vnc, terminal servisse, remote desktop, etc.;

3.8.16. Deverá ser possível instalar, também de forma silenciosa, a Solução de Antivírus nas estações de trabalho através de scripts durante o Login na rede;

3.8.17. Deverá ser possível instalar o agente de forma remota através de credenciais de administrador local ou do domínio.

3.9. Compatibilidade

3.9.1. Todos os componentes da Solução de antivírus deverão ser compatíveis entre si, com o conjunto da solução e com suas funcionalidades, sem a utilização de quaisquer procedimentos que visem adaptar forçadamente os componentes da solução ou seus módulos que sejam incompatíveis;

3.9.2. Todos os componentes da solução deverão ser totalmente compatíveis com a estrutura de TI presente no IPS, que poderá, a critério da empresa, ser verificada durante visita técnica previamente agendada junto à TI;

3.9.3. Para se atingir a compatibilidade citada no item anterior, o IPS não deverá acrescentar qualquer item de hardware ou software a sua estrutura atual. Caso tal acréscimo seja necessário, este deverá ser de responsabilidade da EMPRESA CONTRATADA sem ônus para o IPS (custos, procedimentos e treinamento).

4. DA INSTALAÇÃO E CONFIGURAÇÃO

4.1. A instalação e configuração da Solução de Antivírus deverá ser realizada preferencialmente presencialmente na atual sede do IPS;

4.2. Para os procedimentos de instalação e configuração a EMPRESA CONTRATADA deverá se utilizar de sua própria mão-de-obra, de seus materiais e equipamentos. A TI somente fará a supervisão dos trabalhos e auxiliará a EMPRESA CONTRATADA no fornecimento de dados essenciais para o cumprimento do objeto;

4.3. A EMPRESA CONTRATADA deverá instalar os softwares em todos os equipamentos do IPS, conforme definição e acompanhamento técnico da TI, considerando todos os setores do IPS;

4.4. É de responsabilidade da EMPRESA CONTRATADA a remoção da solução antiga de antivírus, atualmente instalada nos servidores e estações de trabalho do IPS, de todos os equipamentos localizados em sua Sede:

4.4.1. Havendo quaisquer impossibilidades técnicas de remover o produto antigo ou instalar produto novo de forma remota ou automatizada caberá à EMPRESA CONTRATADA encaminhar técnicos especializados ao local para proceder a migração;

4.4.2. A EMPRESA CONTRATADA deverá deixar todos os softwares (patches, service packs, etc.) atualizados em todas as máquinas do IPS.

4.5. A integração dos componentes da solução, entre si e com a estrutura de TI do IPS, é responsabilidade da EMPRESA CONTRATADA;

4.6. Deverão ser configuradas todas as características solicitadas pela TI do IPS, disponíveis na solução fornecida;

4.7. Após a instalação da Solução de Antivírus a EMPRESA CONTRATADA deverá efetuar todos os testes de funcionalidade da solução fornecida incluindo testes de desempenho nos servidores, estações de trabalho e linhas de comunicação;

4.8. Os trabalhos deverão ser realizados no período compreendido entre 9 (nove) e 16 (dezesseis) horas, de segunda a sexta-feira, excluídos os feriados. Caso a EMPRESA CONTRATADA queira realizar atendimentos fora desse horário, deve previamente agendar o horário com o IPS, sob pena de não ser atendida. Esse agendamento estará condicionado à disponibilidade dos técnicos da TI;

4.9. A EMPRESA CONTRATADA deverá garantir atendimento fora do horário mencionado no item anterior, inclusive sábados, domingos e feriados, quando solicitado pelo IPS;

4.10. A data de início dos serviços será agendada pela TI do IPS após a entrega oficial do produto pela EMPRESA CONTRATADA, sendo comunicada à EMPRESA CONTRATADA através de ordem de serviço;

4.11. Os serviços de instalação e configuração deverão ser concluídos pela EMPRESA CONTRATADA dentro do prazo máximo de 10 (dez) dias uteis, a contar da data da ordem de serviço. O descumprimento ao prazo citado sujeitará a EMPRESA CONTRATADA a penalidade de multa;

4.12. Concomitante aos serviços a EMPRESA CONTRATADA deverá repassar conhecimento aos técnicos do IPS e gerar documentação de todos os procedimentos realizados, assim como roteiro de instalação e configuração da solução no ambiente do IPS;

4.13. A EMPRESA CONTRATADA deverá realizar os trabalhos citados anteriormente através de técnico certificados na solução fornecida;

4.14. A EMPRESA CONTRATADA deverá apresentar, após a assinatura do contrato, a relação dos técnicos que farão a instalação do produto e que prestarão atendimento no IPS. Será considerado apto o técnico que possuir as certificações exigidas pelo fabricante de acordo com a tarefa a ser realizada. Na ocasião do cadastro, junto a TI, a EMPRESA CONTRATADA deverá apresentada cópia autenticada do(s) certificado(s) do(s) técnico(s) relacionado(s). O IPS irá permitir a intervenção técnica apenas aos profissionais previamente cadastrados e certificados.

5. DA GARANTIA

5.1. Os produtos fornecidos deverão estar cobertos por garantia, compreendendo os defeitos decorrentes de projeto, confecção e desenvolvimento do software, pelo período de, no mínimo, igual período à expiração da licença;

5.2. Durante o período de garantia a EMPRESA CONTRATADA deverá, sem ônus adicional para o IPS, fornecer, instalar e configurar as atualizações ("patches") corretivas do software fornecido, bem como o recebimento de novas versões dos produtos que integram a solução de antivírus;

5.3. Durante todo o período de garantia a assistência técnica poderá ser prestada com atendimento "on-site" ou remotamente por mão-de-obra treinada, para os serviços solicitados conforme descrito em cada item quando couber;

5.4. O diagnóstico dos problemas ou defeitos que a solução apresentar durante a garantia ou a vigência do Contrato deve ser realizado por técnicos do fabricante ou da CONTRATADA "on-site" ou remotamente;

5.5. O chamado técnico será feito pela CONTRATANTE junto à CONTRATADA, que será a responsável pela abertura do suporte técnico junto ao fabricante quando couber.

6. DO LOCAL DE ENTREGA E RECEBIMENTO

6.1. DA ENTREGA

6.1.1. Deverão ser entregues junto com a solução de antivírus:

6.1.1.1. Todos os manuais necessários à instalação do software de antivírus e seus componentes;

6.1.1.2. Todas as licenças de utilização definitivas para os softwares fornecidos, em suas últimas versões disponíveis considerando a data de entrega do software, em nome do IPS. As licenças do software deverão ser ofertadas na modalidade de licenciamento por tempo determinado.

6.1.2. Os softwares deverão ser entregues na sede do IPS, no TI (2º andar), sito à Rua Maestro Antônio Cícero, 269, Centro - Serra/ES - CEP 29176-100, de segunda à sexta no horário de 09:00h às 16:00h, em sua totalidade, condicionada à conferência;

6.1.3. Havendo a possibilidade de obter a solução de antivírus pela internet, caberá à EMPRESA CONTRATADA realizar os procedimentos de download com acompanhamento da TI;

6.1.4. Em caso de entrega de mídia física, o transporte dos componentes do software de antivírus até o local especificado pela TI no dia da entrega deverá ser realizado pela EMPRESA CONTRATADA (inclusive os procedimentos de seguro, embalagem e transporte até o local especificado);

6.1.4.1. A entrega deve ser agendada com antecedência mínima de 24 horas, sob o risco de não ser autorizada;

6.1.5. No ato da entrega, caso seja detectado que as licenças não atendem às especificações contidas do objeto licitado, poderá o IPS rejeitá-lo, obrigando-se a Licitante a providenciar a sua substituição no prazo máximo de até 48 horas.

6.1.6. Por se tratar de um ativo digital/eletrônico, os bens poderão ser entregues no seguinte e-mail **dti@ips.es.gov.br**;

6.1.7. No ato da entrega, caso seja detectado que o objeto não atende às especificações contidas no objeto licitado, poderá o IPS rejeitá-lo, obrigando-se a LICITANTE a providenciar a sua substituição no prazo máximo de até 10 (dez) dias.

6.2. DO RECEBIMENTO

6.2.1. No ato de entrega do software, a TI do IPS fornecerá à empresa vencedora termo de recebimento provisório;

6.2.2. Para o recebimento definitivo da solução de antivírus, após homologado pela TI, será feita uma análise detalhada da procedência do software, considerando os seguintes procedimentos:

6.2.2.1. Verificação da origem do software, junto ao fabricante: A TI analisará se o software fornecido foi adquirido pela empresa através do fabricante ou distribuidor autorizado pelo fabricante.

6.2.3. A TI recusará o software caso os requisitos acima descritos não sejam atendidos.

7. DAS RESPONSABILIDADES DAS PARTES

7.1. DO CONTRATANTE

7.1.1. Cumprir o que está descrito no instrumento de convocação, em especial no TR, na proposta de preços adjudicada da Contratada e no contrato;

7.1.2. Autorizar o início da execução do objeto, mediante a expedição de Autorização de Fornecimento ou outro documento equivalente, em nome da Contratada;

7.1.3. Solicitar junto à Contratada, ao seu exclusivo critério na Autorização de Fornecimento, os quantitativos relativos à execução do objeto;

7.1.4. Cumprir os compromissos financeiros assumidos com a Contratada;

7.1.5. Fornecer à Contratada todos os elementos e informações, de qualquer natureza, que se fizerem necessários à execução do objeto;

7.1.6. Notificar, formal e tempestivamente, a Contratada sobre quaisquer irregularidades observadas na execução do objeto;

7.1.7. Notificar a Contratada, por escrito e com antecedência mínima de 72 h, sobre multas, penalidades e quaisquer débitos de sua responsabilidade;

7.1.8. Acompanhar e fiscalizar a execução do objeto por meio de Gestores e Fiscais do contrato, composta por profissionais nomeados ao exclusivo critério do Contratante, cuja ratificação da referida nomeação dar-se-á pela edição de Portaria, também pelo Contratante;

7.1.9. Pagar a importância correspondente aos serviços corretamente prestados pela Contratada, no prazo pactuado, mediante as notas fiscais/faturas, devidamente atestadas pelos Gestores e Fiscais;

7.1.10. Permitir o livre acesso dos colaboradores da Contratada às dependências do Contratante, quando necessário e por intermédio de solicitação formal, a fim de que o objeto possa ser corretamente executado;

7.1.11. Promover, caso necessário, auditoria técnica e operacional no ambiente e demais recursos utilizados pela Contratada, por meio de pessoal próprio ou equipe de terceiros, relacionados à execução do objeto;

7.1.12. Certificar toda a documentação e demais produtos gerados em decorrência da execução do objeto, efetuando o seu atesto através de seus Gestores e Fiscais, assim que seja constatada a sua conformidade.

7.2. DA CONTRATADA

7.2.1. Será obrigatório, cumprir todas as especificações estabelecidas no contrato, caso contrário o produto/serviço não será aceito;

7.2.2. Executar o objeto em conformidade com o instrumento de convocação, em especial com o TR, com a proposta de preços adjudicada da Contratada e com o contrato;

7.2.3. Iniciar a execução do objeto em até 10 dias corridos, exclusivamente mediante o conhecimento da Autorização de Fornecimento ou outro documento equivalente, expedido pelo Contratante;

7.2.4. Manter durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas;

7.2.5. Assumir a responsabilidade pelos encargos fiscais e comerciais resultantes da execução do objeto;

7.2.6. Responsabilizar-se por todos os ônus, diretos e indiretos, referentes a execução do objeto;

7.2.7. Responsabilizar-se por todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho, quando, em ocorrência da espécie, forem vítimas os seus colaboradores no desempenho dos serviços desta contratação ou em conexão com eles, ainda que acontecido nas dependências do Contratante;

7.2.8. Responsabilizar-se por qualquer prejuízo causado ao Contratante, a seus prepostos ou a terceiros, provocados por ação ou omissão da Contratada, em decorrência de falhas ou imperfeições na execução do objeto;

7.2.9. Responsabilizar-se pelos eventuais danos ou desvios causados aos bens que lhe forem confiados, devendo efetuar o ressarcimento correspondente, imediatamente após o recebimento da notificação expressa do Contratante, sob pena de glosa de qualquer importância que tenha direito a receber;

7.2.10. Garantir absoluto sigilo sobre todos os processos, informações e quaisquer outros dados ou produtos disponibilizados pelo Contratante, em função das peculiaridades inerentes à execução do objeto;

7.2.11. Abster-se, qualquer que seja a hipótese, de veicular publicidade ou qualquer outra informação acerca das atividades, objeto desta contratação, sem a prévia autorização do Contratante;

7.2.12. Indicar profissional preposto para tratar das questões administrativas e daquelas inerentes a execução do objeto junto ao Contratante;

7.2.13. Esclarecer, em tempo hábil, eventuais dúvidas e indagações, de qualquer natureza, do Contratante;

7.2.14. Comunicar à Gestão e Fiscalização do contrato qualquer fato extraordinário ou anormal que ocorra durante a execução do objeto;

7.2.15. Executar o objeto, ajustando os serviços às particularidades e às especificidades do Contratante, personalizando-os em razão da obtenção de melhores resultados e da melhor eficiência;

7.2.16. Produzir, disponibilizar ao Contratante e manter toda a documentação e demais produtos advindos da execução do objeto;

7.2.17. Disponibilizar em meio digital e com acesso integral e irrestrito, a qualquer momento quando solicitado e ao exclusivo critério do Contratante, todos os bancos de dados e demais informações, de qualquer natureza, que tenham sido produzidos e encontrem-se no âmbito da execução do objeto, de propriedade do Contratante, até o momento da referida solicitação, devidamente acompanhados das instruções que proporcionem a sua correta identificação e operacionalização autônoma pelo Contratante;

7.2.18. Exigir dos seus colaboradores, quando em serviço nas dependências do Contratante, o uso obrigatório de uniformes e crachás de identificação;

7.2.19. Por se tratar de serviço que estão em constante evolução, seja técnica ou legal, deverá a CONTRATADA manter o mesmo, sempre atualizado e em perfeitas condições de uso durante toda a execução do contrato, sem qualquer custo adicional para a CONTRATANTE, adequando todos os "módulos" contratados à legislação vigente, bem como atualizando o sistema para versões superiores, todas sem qualquer ônus.

7.2.20. A CONTRATADA deverá zelar para que seus profissionais mantenham conduta compatível com os princípios de decência e boa educação, obedecendo rigorosamente às determinações do GESTOR ou FISCAIS.

7.2.21. Prestar o serviço objeto do contrato durante todo o período de vigência do contrato, salvaguardados os casos de interrupções programadas.

8. DO PAGAMENTO E REAJUSTE

8.1. O pagamento somente será autorizado depois de efetuado o "atesto" pela Fiscalização designada pela autoridade máxima da unidade para esta finalidade, condicionado este ato à verificação da conformidade da Nota Fiscal/Fatura apresentada em relação ao objeto efetivamente prestado;

8.2. O pagamento será realizado mediante o fornecimento ao IPS de nota fiscal, juntamente com a comprovação da regularidade fiscal exigidos em conformidade com o Art. 68, incisos I, III, IV, V, §1º e §2º da Lei nº 14.133/2021. Estes documentos depois de conferidos serão encaminhados para processamento e pagamento, após a respectiva apresentação;

8.3. A contagem do prazo de pagamento será iniciada com a conclusão dos itens 9.3.4 e 9.4.4;

8.4. O pagamento será realizado em até 15 (quinze) dias úteis após a data do ato de "aceite" definitivo de recebimento do objeto, fundamentado no processo principal, considerando as condições deste instrumento;

8.5. O cronograma de pagamento será fixo, ocorrendo nos dias 05, 15 ou 25 de cada mês. Caso uma dessas datas não seja dia útil, o pagamento poderá ser antecipado para o dia útil anterior;

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

9. DO ACOMPANHAMENTO DO CONTRATO E DOS PROCEDIMENTOS DE FISCALIZAÇÃO

9.1. Os serviços serão acompanhados pelo GESTOR e FISCAIS, nos termos da Lei 14.133/2021.

9.1.1. O GESTOR ou FISCAIS registrarão as falhas detectadas e comunicarão as ocorrências de quaisquer fatos que, a seu critério, requeiram medidas corretivas por parte da CONTRATADA;

9.1.2. O GESTOR ou FISCAIS poderão, a qualquer tempo, exigir a paralisação dos serviços ou o imediato afastamento de profissionais cuja atuação, permanência ou comportamento sejam considerados prejudiciais, inconvenientes ou insatisfatórios à disciplina do CONTRATANTE ou ao interesse dos serviços, sem que seja necessário declarar os motivos de tal exigência.

9.2. **A CONTRATADA** deverá designar, antes do início dos serviços, um SUPERVISOR com qualificações técnicas necessárias para garantir a boa execução do contrato, nos termos do art. 67, inciso III da Lei 14.133/2021.

9.2.1. O SUPERVISOR atenderá ao GESTOR ou FISCAIS sempre que solicitado, devendo informar por escrito um número de telefone celular para contato emergencial.

9.2.1.1. Esta comunicação poderá ser enviada ao GESTOR e FISCAIS por intermédio de correio eletrônico (e-mail: administrativo@ips.es.gov.br e daf@ips.es.gov.br ou outro a ser informado oportunamente);

9.2.1.2. Durante a vigência do contrato, a CONTRATADA deverá manter permanentemente atualizado os endereços físico, eletrônico e os números de telefone para contatos;

9.2.1.3. Qualquer mudança no responsável deve ser comunicada formalmente à administração pública, preferencialmente com antecedência.

9.3. **Cabe ao Gestor do Contrato:**

9.3.1. Notificar, sempre que solicitado pelo Fiscal Técnico ou Administrativo à CONTRATADA quanto ao não cumprimento dos prazos, custos, falta de certidões, solicitação de visitas e etc.;

9.3.2. Prestar as informações e esclarecimentos gerenciais que venham a ser solicitados pelos servidores do IPS;

9.3.3. Atentar para vigência do contrato, tomando as medidas cabíveis para que os serviços continuem a serem prestados sem intercorrências;

9.3.4. Atestar a nota fiscal em conjunto com o Fiscal Administrativo.

9.4. Cabe ao Fiscal Administrativo do Contrato:

9.4.1. Emitir a Solicitação de Serviço com todas as informações necessárias e acompanha-la até a sua conclusão, junto à Contratada;

9.4.1.1. Informar ao Fiscal Técnico quanto ao contato realizado com a Contratada e a previsão para visita, atendimento ou conclusão da Solicitação de Serviço.

9.4.2. Prestar as informações administrativas e os esclarecimentos que venham a ser solicitados pela Contratada;

9.4.3. Acompanhar e fiscalizar a execução do objeto desta contratação, sob os aspectos quantitativos e de custos;

9.4.4. Atestar a nota fiscal quanto à cobrança dos serviços e situação das certidões da Contratada.

9.4.4.1. Encaminhar a nota fiscal para o ateste do Fiscal Técnico, exclusivamente quando registrada falha no fornecimento do serviço no período para ateste.

9.5. Cabe ao Fiscal Técnico do Contrato:

9.5.1. Relatar e solicitar ao Fiscal Administrativo a emissão de Solicitação de Serviço à Contratada, com todas as informações técnicas necessárias;

9.5.1.1. Prestar diretamente as demais informações e esclarecimentos técnicos que venham a ser solicitados pela Contratada;

9.5.1.2. Informar ao Fiscal Administrativo quanto a homologação da conclusão da Solicitação de Serviço.

9.5.2. Acompanhar e fiscalizar a execução do objeto desta contratação, sob os aspectos técnicos;

9.5.3. Acompanhar o acesso do pessoal técnico da Contratada de modo a viabilizar a prestação dos serviços;

9.5.4. Atestar a nota fiscal solidariamente ao Fiscal Administrativo quanto à entrega dos serviços contratados, quando registrada falha no fornecimento do objeto do período para ateste.

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

9.7. Ficam designados os representantes da administração para acompanhamento, Gestão e Fiscalização do Contrato:

GESTOR:			
Nome:	CHEFE DEPARTAMENTO DE ADMINISTRATIVO	**Matricula:**	
E-mail:		**Telefone:**	
Atribuições:	Servidor(a) com atribuições gerenciais, técnicas e operacionais, relacionadas ao processo de gestão do contrato.		
FISCAL ADMINISTRATIVO:			
Nome:	SERVIDOR DEPARTAMENTO DE ADMINISTRATIVO	**Matricula:**	
E-mail:		**Telefone:**	
Atribuições:	Servidor(a) indicado para fiscalizar o contrato quanto aos aspectos administrativos, documentais e de custos.		
FISCAL TÉCNICO:			
Nome:	SERVIDOR DO SETOR DE TI	**Matricula:**	
E-mail:		**Telefone:**	
Atribuições:	Servidor(a) indicado para fiscalizar tecnicamente o contrato do ponto de vista funcional da Solução de Tecnologia da Informação.		

10. DOS RECURSOS ORÇAMENTÁRIOS

10.1. As despesas decorrentes da presente contratação onerarão a dotação orçamentária própria do Instituto de Previdência dos Servidores Públicos do Município da Serra (IPS), identificada conforme segue:

- **Projeto / Atividade:**

9.122.0018.2.120 - Promover a gestão administrativa do IPS.

- **Elemento / Subelemento:**

3.3.90.40.06 – LOCACAO DE SOFTWARE

11. DA ESTIMATIVA DE VALOR DA CONTRATAÇÃO E DA ACEITABILIDADE DA PROPOSTA

11.1. O custo médio estimado total da contratação para o prazo de licenças de vigência de 36 (trinta e seis) meses é de R$ 141,66 (Cento e Quarenta e Um reais e Sessenta e Seis Centavos), sendo o valor total de R$ 8.499,60 (Oito Mil Quatrocentos e Noventa e Nove Reais e Sessenta Centavos).

* Fonte: Relatório extraído do site Compras.gov.br

12. DO PRAZO

12.1. O prazo de entrega dos bens é de 20 (vinte) dias corridos a contar da emissão da ordem de fornecimento, em remessa única;

12.2. Caso não seja possível a entrega na data assinalada, a empresa deverá comunicar as razões respectivas com pelo menos 5 (cinco) dias de antecedência para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior;

12.3. A garantia legal ou contratual do objeto tem prazo de vigência próprio e desvinculado daquele fixado no contrato, permitindo eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual;

12.4. Reparar, corrigir, remover ou substituir, no prazo que lhe for determinado, sem ônus para o CONTRATANTE sem prejuízo das sanções cabíveis, no todo ou em parte, o objeto do instrumento contratual ou equivalente, que se verificarem pela equipe de fiscalização, vícios, defeitos ou incorreções resultantes da fabricação ou da execução do serviço de suporte técnico;

12.5. Os bens poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 10 (dez) dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades;

12.6. O recebimento definitivo ocorrerá no prazo de 10 (dez) dias úteis, a contar do recebimento da nota fiscal ou instrumento de cobrança equivalente pela Administração, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo detalhado;

12.7. Para as contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021, o prazo máximo para o recebimento definitivo será de até 10 (dez) dias úteis;

12.8. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais;

12.9. O prazo para a solução, pelo contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.

13. DA VIGÊNCIA

13.1. O prazo de vigência do contrato será de 12 (doze) meses, contados a partir da assinatura do contrato, estabelecida conforme as disposições da Lei nº 14.133/2021 e não está sujeita a prorrogação. O contrato poderá ser rescindido ou alterado conforme as condições previstas nos artigos 106 e 107 da referida lei.

14. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

14.1. Dispensa eletrônica através do menor preço.

15. DOS RESPONSÁVEIS PELA ELABORAÇÃO DO TERMO DE REFERÊNCIA

15.1. O Termo de Referência foi elaborado por Felipe Mendonça Carvalho, com base em análise detalhada das necessidades institucionais, observando rigorosamente as diretrizes da Lei nº 14.133/2021, combinado com a lei municipal nº 5.875/2023 e com o decreto municipal nº 5.619/2023 e das melhores práticas de gestão pública, cujos esclarecimentos e informações poderão ser prestados através do e-mail **dti@ips.es.gov.br**.

RESPONSÁVEL(IS) PELA ELABORAÇÃO DO T.R.:
Felipe Mendonça Carvalho
Chefe do Departamento de TI

Aprovado por:
Welligton Costa Freitas
Diretor Presidente

Helder Catarino da Silva Tavares
Diretor Administrativo e Financeiro