ATA DE REGISTRO DE PREÇOS Nº 031/2021

Ata nº 031/2021
Processo nº. 00002865
Pregão nº. 029/2021

Pelo presente instrumento, a **DEFENSORIA PÚBLICA DO ESTADO DO ESPÍRITO SANTO**, inscrita no CNPJ/MF sob o nº 00.671.513/0001-24, com sede na Praça Manoel Silvino Monjardim, 54, Centro, Vitória/ES, CEP 29.010-520, representada legalmente pelo seu Defensor Público-Geral Dr. Gilmar Alves Batista, brasileiro, com endereço profissional na Praça Manoel Monjardim, 54, Centro, Vitória/ES, CEP 29.010-520, considerando o julgamento da licitação **PARA REGISTRO DE PREÇOS PARA CONTRATAÇÃO DE SOLUÇÕES DE ANTIVÍRUS E ANTISPAM PARA PROTEÇÃO DE ENDPOINTS E SERVIDORES,** na modalidade de **PREGÃO ELETRÔNICO,** registrado sob nº 029/2021, publicada no DIOES do dia 14 de julho de 2021, bem como, a classificação das propostas publicada no DIOES de 24 de agosto de 2021, e a respectiva homologação exarada na fl. 311 do processo 00002865, RESOLVE registrar os preços da empresa **BRINFOR SOLUÇÕES EM TI LTDA**, pessoa jurídica de direito privado, inscrito no CNPJ sob nº 07.716.261/0001-51, com endereço na Avenida Professor Mario Werneck, nº 280, Loja 01, Bairro Buritis – Belo Horizonte/MG, CEP: 30.455/610, neste ato representado por Bruno Vieira Rodrigues, com endereço em Belo Horizonte/MG, nas quantidades estimadas, de acordo com a classificação alcançada por item, atendendo as condições previstas no Instrumento Convocatório e as constantes desta Ata de Registro de Preços, e regido pela Lei Federal nº 10.520/2002, pelo Decreto Estadual nº 2.458-R, publicado em 5 de fevereiro de 2010, pelo Decreto Estadual nº 1.790/-R/2007, de 24 de janeiro de 2007, pela Lei Federal nº 8.666/93 e suas alterações e em conformidade com as disposições a seguir.

CLÁUSULA PRIMEIRA – DO OBJETO

1.1. A presente Ata tem por objeto o registro de preços para contratação de soluções de antivírus e antispam para proteção de endpoints e servidores, para atender a esta Defensoria.

CLÁUSULA SEGUNDA – DO PREÇO

2.1. Os preços a serem pagos coincidem com os preços definidos no ANEXO I desta Ata, e nele estão inclusos todas as espécies de tributos, diretos e indiretos, encargos sociais, seguros, fretes, material, mão-de-obra e quaisquer despesas inerentes à compra.

2.2. Os preços contratados serão fixos e irreajustáveis, ressalvado o disposto na cláusula terceira deste instrumento.

2.3. A existência de preços registrados não obrigará a Administração a firmar contratações que deles poderão advir, facultada a realização de licitação específica ou a contratação direta para a aquisição pretendida nas hipóteses previstas na Lei Federal nº 8.666/93, mediante fundamentação, assegurando-se ao beneficiário do registro a preferência de fornecimento em igualdade de condições.

CLÁUSULA TERCEIRA – DA ALTERAÇÃO DO PREÇO PRATICADO NO MERCADO E DO REEQUILÍBRIO DA EQUAÇÃO ECONÔMICO-FINANCEIRA

3.1. Quando, por motivo superveniente, o preço registrado tornar-se superior ao preço praticado pelo mercado, o órgão gerenciador deverá:

- Convocar o fornecedor visando à negociação para redução de preços e sua adequação ao praticado pelo mercado;
- Frustrada a negociação, liberar o fornecedor do compromisso assumido;
- Convocar os demais fornecedores para conceder igual oportunidade de negociação.

3.2. Quando o preço de mercado tornar-se superior aos preços registrados e o fornecedor, mediante oferta de justificativas comprovadas, não puder cumprir o compromisso, o órgão gerenciador poderá:

- Liberar o fornecedor do compromisso assumido, sem aplicação de sanção administrativa, desde que as justificativas sejam motivadamente aceitas e o requerimento ocorra antes da emissão de ordem de fornecimento;
- Convocar os demais fornecedores para conceder igual oportunidade de negociação.

3.3. Não logrando êxito nas negociações, o órgão gerenciador deve proceder à revogação da Ata de Registro de Preços e à adoção de medidas cabíveis para obtenção de contratação mais vantajosa.

3.4. Em caso de desequilíbrio da equação econômico-financeira, será adotado o critério de revisão, como forma de restabelecer as condições originalmente pactuadas.

3.5. A revisão poderá ocorrer a qualquer tempo da vigência da Ata, desde que a parte interessada comprove a ocorrência de fato imprevisível, superveniente à formalização da proposta, que importe, diretamente, em majoração ou minoração de seus encargos.

3.5.1. Em caso de revisão, a alteração do preço ajustado, além de obedecer aos requisitos referidos no item anterior, deverá ocorrer de forma proporcional à modificação dos encargos, comprovada minuciosamente por meio de memória de cálculo a ser apresentada pela parte interessada.

3.5.2. Dentre os fatos ensejadores da revisão, não se incluem aqueles eventos dotados de previsibilidade, cujo caráter possibilite à parte interessada a sua aferição ao tempo da formulação/aceitação da proposta, bem como aqueles decorrentes exclusivamente da variação inflacionária, uma vez que inseridos, estes últimos, na hipótese de reajustamento, modalidade que não será admitida neste registro de preços, posto que a sua vigência não supere o prazo de um ano.

3.5.3. Não será concedida a revisão quando:

- Ausente a elevação de encargos alegada pela parte interessada;
- O evento imputado como causa de desequilíbrio houver ocorrido antes da formulação da proposta definitiva ou após a finalização da vigência da Ata;

- Ausente o nexo de causalidade entre o evento ocorrido e a majoração dos encargos atribuídos à parte interessada;
- A parte interessada houver incorrido em culpa pela majoração de seus próprios encargos, incluindo-se, nesse âmbito, a previsibilidade da ocorrência do evento.

3.5.4. Em todo o caso, a revisão será efetuada por meio de aditamento contratual, precedida de análise pela Assessoria Jurídica da Defensoria Pública do Estado do Espírito Santo, e não poderá exceder o preço praticado no mercado.

CLÁUSULA QUARTA – DO CANCELAMENTO DO REGISTRO DE PREÇOS

4.1. O preço registrado poderá ser cancelado nas seguintes hipóteses:

4.1.1. Pela Administração, quando houver comprovado interesse público, ou quando o fornecedor:

- não cumprir as exigências da Ata de Registro de Preços;
- não formalizar contrato decorrente do Registro de Preços ou não retirar o instrumento equivalente no prazo estabelecido, sem justificativa aceitável;
- não aceitar reduzir o preço registrado, na hipótese de se tornar este superior aos praticados no mercado;
- incorrer em inexecução total ou parcial do contrato decorrente do registro de preços;

4.1.2. Pelo fornecedor, quando, mediante solicitação formal e expressa, comprovar a impossibilidade, por caso fortuito ou força maior, de dar cumprimento às exigências do instrumento convocatório e da Ata de Registro de Preços.

4.2. O cancelamento do registro de preços por parte da Administração, assegurados a ampla defesa e o contraditório, será formalizado por decisão da autoridade competente.

4.2.1. O cancelamento do registro não prejudica a possibilidade de aplicação de sanção administrativa, quando motivada pela ocorrência de infração cometida pelo particular, observados os critérios estabelecidos na cláusula décima primeira deste instrumento.

4.3. Da decisão da autoridade competente se dará conhecimento aos fornecedores, mediante o envio de correspondência, com aviso de recebimento.

4.4. No caso de ser ignorado, incerto ou inacessível o endereço do fornecedor, a comunicação será efetivada através de publicação na imprensa oficial, considerando-se cancelado o preço registrado, a contar do terceiro dia subsequente ao da publicação.

4.5. A solicitação, pelo fornecedor, de cancelamento do preço registrado deverá ser formulada com antecedência mínima de 30 (trinta) dias, instruída com a comprovação dos fatos que justificam o pedido, para apreciação, avaliação e decisão da Administração.

CLÁUSULA QUINTA – DAS CONDIÇÕES DE PAGAMENTO

5.1. A Contratante pagará à Contratada pelos materiais adquiridos até o 10° (décimo) dia útil após a apresentação da Nota Fiscal/Fatura correspondente, devidamente atestada pelo fiscal, vedada antecipação.

5.2. Decorrido o prazo indicado no item anterior, incidirá multa financeira nos seguintes termos:

$$V.M = V.F \times \frac{12}{100} \times \frac{ND}{360}$$

Onde:

V.M. = Valor da Multa Financeira.
V.F. = Valor da Nota Fiscal referente ao mês em atraso.
ND = Número de dias em atraso.

5.3. O pagamento far-se-á por meio de uma única fatura.

5.4. Incumbirão à Contratada a iniciativa e o encargo do cálculo minucioso da fatura devida, a ser revisto e aprovado pela Contratante, juntando-se o cálculo da fatura.

5.5. A liquidação das despesas obedecerá rigorosamente o estabelecido na Lei nº 4.320/64, assim como na Lei Estadual nº 2.583/71 e alterações posteriores.

5.6. Se houver alguma incorreção na Nota Fiscal/Fatura, a mesma será devolvida à Contratada para correção, ficando estabelecido que o prazo para pagamento será contado a partir da data de apresentação na nova Nota Fiscal/Fatura, sem qualquer ônus ou correção a ser paga pela Contratante.

5.7. A eventual inadimplência de um dos órgãos participantes desta Ata não produzirá efeitos quanto aos demais.

CLÁUSULA SEXTA – DO PRAZO DE VIGÊNCIA DA ATA

6.1. O prazo de vigência dessa Ata de Registro de Preços é de 12 (doze) meses, contado do dia posterior à data de sua publicação no Diário Oficial, vedada a sua prorrogação.

6.2. O prazo de vigência das contratações decorrentes desse registro de preços apresentará como termo inicial o recebimento da ordem de fornecimento e como termo final o recebimento definitivo dos materiais pela Administração, observados os limites de prazo de entrega fixados na (Anexo I) Ordem de Fornecimento, e sem prejuízo para o prazo mínimo de validade dos produtos adquiridos.

CLÁUSULA SÉTIMA – DA DOTAÇÃO ORÇAMENTÁRIA

7.1. As despesas inerentes a esta Ata correrão à conta da respectiva dotação orçamentária desta Defensoria Pública e serão especificadas ao tempo da ordem de emissão de fornecimento.

CLÁUSULA OITAVA – DA CONVOCAÇÃO PARA RECEBER A ORDEM DE FORNECIMENTO

8.1. A emissão da ordem de fornecimento constitui o instrumento de formalização da aquisição com os fornecedores, devendo o seu resumo ser publicado na Imprensa Oficial, em conformidade com os prazos estabelecidos na Lei Federal nº 8.666/93.

8.2. Se o licitante classificado em primeiro lugar se recusar a receber a ordem de fornecimento ou se não dispuser de condições de atender integralmente à necessidade da Administração, poderá a ordem de fornecimento ser expedida para os demais proponentes cadastrados que concordarem em fornecer os materiais ao preço e nas mesmas condições do primeiro colocado, observada a ordem de classificação.

CLÁUSULA NONA – DAS CONDIÇÕES DE ENTREGA

9.1. As soluções deverão ser entregues na Diretoria de Tecnologia da Informação (DTI) da *DPES.*

9.2. A licitante terá o prazo máximo de 30 (trinta) dias úteis, para o fornecimento da solução, a contar da data de recebimento da ordem de compra, emitida por esta Instituição.

CLÁUSULA DÉCIMA – DAS RESPONSABILIDADES DAS PARTES

Compete à Contratada:

a) entregar os produtos de acordo com as condições e prazos propostos e mantê-los em pleno funcionamento dentro do período da garantia;
b) providenciar a imediata correção das deficiências apontadas pelo setor competente do Contratante;
c) manter, durante toda a execução da garantia, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação, conforme dispõe o inciso XIII, do artigo 55, da Lei Nº 8.666/93 e alterações;

Compete à Contratante:
a) Efetuar os pagamentos nas condições pactuadas;
b) definir o local para entrega dos materiais adquiridos;
c) designar servidor (ou comissão de, no mínimo, 3 três membros, na hipótese do parágrafo 8º do art. 15 da Lei nº 8.666/93) responsável pelo acompanhamento e fiscalização na entrega dos produtos adquiridos.

CLÁUSULA DÉCIMA PRIMEIRA – DAS SANÇÕES ADMINISTRATIVAS

11.1. Comete infração administrativa nos termos da Lei nº 10.520, de 2002, a Contratada que:

- Inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

- Ensejar o retardamento da execução do objeto;
- Falhar ou fraudar na execução do contrato;
- Comportar-se de modo inidôneo;
- Cometer fraude fiscal;

11.2. Pela inexecução total ou parcial do objeto deste contrato, a Administração pode aplicar à CONTRATADA as seguintes sanções:

- **Advertência,** por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a Contratante;
- Multa moratória de 0,3% (zero virgula três por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 20 (vinte) dias úteis de atraso, caracterizando inexecução parcial;
- Multa compensatória de 10% (dez por cento) sobre o valor total do contrato, no caso de inexecução total do objeto;
- Em caso de inexecução parcial, a multa compensatória, no mesmo percentual do subitem acima, será aplicada de forma proporcional à obrigação inadimplida;
- Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;
- Impedimento de licitar e contratar com órgãos e entidades da União com o consequente descredenciamento no SICAF pelo prazo de até cinco anos;
  11.2.6.1 A Sanção de impedimento de licitar e contratar prevista neste subitem também é aplicável em quaisquer das hipóteses previstas como infração administrativa no subitem 11.1 deste termo.

11.2.7. Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados;

11.3. A aplicação da multa de mora não impede que a Administração rescinda unilateralmente o contrato e aplique as outras sanções previstas no item 11.2 desta Ata e na Lei Federal nº 8.666/93.

11.4. As sanções previstas nos subitens 11.2.1, 11.2.5, 11.2.6 e 11.2.7 poderão ser aplicadas à CONTRATADA juntamente com as de multa, descontando-a dos pagamentos a serem efetuados.

11.5. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

11.5.1. tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;
11.5.2. tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;
11.5.3. demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

11.6. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à Contratada, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

11.7. As multas devidas e/ou prejuízos causados à Contratante serão deduzidos dos valores a serem pagos, ou recolhidos em favor da União, ou deduzidos da garantia, ou ainda, quando for o caso, serão inscritos na Dívida Ativa da União e cobrados judicialmente.

11.8. Caso a Contratante determine, a multa deverá ser recolhida no prazo máximo de 15 (quinze) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

11.9. Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a União ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

11.10. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

CLÁUSULA DÉCIMA SEGUNDA – DA RESCISÃO

12.1. A rescisão da Ata poderá ocorrer nas hipóteses e condições previstas nos artigos 78 e 79 da Lei nº 8.666/93, no que couberem, com aplicação do art. 80 da mesma Lei, se for o caso.

CLÁUSULA DÉCIMA TERCEIRA – DOS ADITAMENTOS

13.1. A presente Ata poderá ser aditada, estritamente, nos termos previstos na Lei nº 8.666/93, após manifestação formal da Defensoria Pública do Estado.

CLÁUSULA DÉCIMA QUARTA – DOS RECURSOS

14.1. Os recursos, representação e pedido de reconsideração, somente serão acolhidos nos termos do art. 109, da Lei nº 8.666/93 e alterações posteriores.

CLÁUSULA DÉCIMA QUINTA – DO ACOMPANHAMENTO E DA FISCALIZAÇÃO

15.1. Nos termos do art. 67 Lei nº 8.666, de 1993, será designado representante para acompanhar e fiscalizar a entrega dos bens, anotando em registro próprio todas as ocorrências relacionadas com a execução e determinando o que for necessário à regularização de falhas ou defeitos observados.

15.2. A fiscalização de que trata este item não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios, e, na ocorrência desta, não implica em corresponsabilidade da Administração ou de seus agentes e prepostos, de conformidade com o art. 70 da Lei nº 8.666, de 1993.

15.3. O representante da Administração anotará em registro próprio todas as ocorrências relacionadas com a execução do contrato, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das falhas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

CLAUSULA DECIMA SEXTA – DA GARANTIA E ATUALIZAÇÕES

16.1. O licitante vencedor prestará garantia, suporte técnico e direito a atualizações e novas versões do produto, quando necessário aos sistemas fornecidos, pelo período de 36 (trinta e seis) meses, contado a partir da data de instalação dos softwares.

16.2. O licitante vencedor deverá fornecer serviço de suporte técnico on-site ou remotamente via ferramenta apropriada previamente analisada e autorizada pela Diretoria de Tecnologia da Informação – DTI, sempre que for necessário à *DPES* para instalar, desinstalar, reinstalar, solucionar problemas, reconfigurar, corrigir defeitos, ajustes e reparos ou tão somente dirimir dúvidas técnicas.
Assistência técnica do tipo corretiva, compreendendo procedimentos destinados a recolocar em perfeito estado de operação os serviços e softwares. Caso não seja possível a solução pelo fornecedor, este deverá acionar o fabricante da solução para a criação de patch corretivo.

16.3. O serviço deverá ser prestado por técnicos devidamente qualificados e certificados pelo fabricante dos produtos para executar as atividades compatíveis com as exigidas no edital.

16.4. O licitante vencedor deverá garantir atualizações pertinentes aos softwares. Entende-se como "atualização" o provimento de toda e qualquer evolução de software, incluindo correções, "patches", "fixes", "updates", "service packs", novas "releases", "versions", "builds", "upgrades", englobando inclusive versões não sucessivas, nos casos em que a liberação de tais versões ocorra durante o período de manutenção e suporte técnico especificado.
A CONTRATADA prestará, sem qualquer custo adicional, os serviços de suporte técnico que abrangem todas as atividades acordadas pela garantia do software ou pelo suporte técnico do fornecedor/fabricante, que garante a solução de problemas referentes a falhas e defeitos de software.

16.5. O regime de suporte deverá ser de 8x5 (8 horas para os 5 dias úteis da semana), com atendimento remoto ou on-site na sede da *DPES*. Os serviços de suporte técnico poderão ser solicitados à contratada mediante apresentação da solicitação de suporte técnico via e-mail, sistema informatizado e linha telefônica 0800 ou gratuita.

16.6. A assistência técnica em garantia deve garantir o fornecimento de acesso irrestrito 24x7 (24 horas por dia x 7 dias da semana), ao endereço eletrônico (web site), a toda a documentação técnica pertinente (guias de instalação/configuração atualizados, FAQ's, bases de conhecimento e bases de soluções, com pesquisa efetuada através de ferramentas de busca).

16.7. Todas as solicitações feitas pela *DPES* deverão ser registradas em sistema informatizado de chamados via WEB que possibilite, no mínimo:

A) Abertura, acompanhamento, listagem e fechamento de chamados. Os chamados devem estar sempre atualizados ao final do dia.
B) Geração automatizada do número do protocolo no momento da abertura do chamado, pelo qual se referenciará cada atendimento/chamado.
C) Possibilidade de mostrar os tempos de atendimentos dos chamados atendidos, bem como os tempos excedidos com base nos SLA's contratados.
D) Envio automatizado de informações via e-mail para a *DPES* sobre todas as alterações nos status dos chamados, desde sua abertura até seu fechamento, referenciando o chamado através de seu número do protocolo.
E) Envio automático mensal dos chamados abertos, detalhando todo o escopo do chamado, desde sua abertura à sua finalização, constando tempo de atendimento e ressaltando, se houver tempo excedido de SLA.
F) Armazenar, e quando solicitado gerar os relatórios das atividades executadas associadas ao chamado.
G) Manter o mais absoluto sigilo sobre todas as informações nele imputadas, segregando-as inclusive de outros clientes que também mantenham contratos com a CONTRATADA e que por ventura também acessem o mesmo sistema.
H) Deverão ser fornecidas ao Gestor do Contrato da *DPES* e a um servidor responsável da GETEC, credenciais individuais para acesso ao sistema Web para abertura e acompanhamento dos chamados.
I) O sistema WEB será o método preferencial para abertura de chamados, porém, não eximindo a sua obrigatoriedade, para os casos de indisponibilidade deste, a CONTRATADA também deverá disponibilizar método alternativo para abertura de chamados, através de endereço de correio eletrônico e número telefônico.
    i. Para abertura de chamados via correio eletrônico deverá ser definido um remetente e destinatário para troca de mensagens.
    ii. O número telefônico designado pela CONTRATADA deverá permanecer disponível no regime de 8x5 (8 horas para os 5 dias úteis da semana), no qual um atendente deverá proceder à abertura do chamado e ativação da equipe técnica competente.
    iii. Este número telefônico deverá ser local ou equivalente à chamada gratuita do tipo 0800.
    iv. Opcionalmente a CONTRATADA poderá disponibilizar mais de um número telefônico.

Durante o período de suporte, a contratada deverá atender as solicitações da *DPES*, feitas por meio da Diretoria de Tecnologia da informação (DTI) respeitando as condições e níveis de serviço (SLA) especificados a seguir.

A) Severidade **ALTA**: Este nível é aplicado quando há falha crítica no ambiente da solução, deixando os componentes indisponíveis.

DIAS ÚTEIS		
Prazo de atendimento	Prazo de solução de contorno	Prazo de solução definitiva
04 horas	08 horas	10 dias úteis

B) Severidade **MÉDIA**: Este nível é aplicado quando há falha no uso do software, estando ainda disponível, porém apresentando problemas ou instabilidade.

DIAS ÚTEIS		
Prazo de atendimento	Prazo de solução de contorno	Prazo de solução definitiva
12 horas	24 horas	20 dias úteis

C) Severidade **BAIXA**: Este nível de severidade é aplicado para elaboração de diagnóstico, avaliação e tunning de ambiente, customização de funcionalidades, documentação de procedimentos, esclarecimento técnico, implementação de procedimentos de evolução de versão de softwares e aplicação de melhorias e correções.

DIAS ÚTEIS		
Prazo de atendimento	Prazo de solução de contorno	Prazo de solução definitiva
24 horas	36 horas	25 dias úteis

Serão considerados para efeitos dos níveis exigidos:

A) Prazo de atendimento: Tempo em horas úteis decorridos entre a solicitação efetuada pela equipe técnica da *DPES* à contratada e o efetivo início dos trabalhos de manutenção.
B) Prazo de solução de contorno: Tempo em horas úteis decorridos entre a solicitação efetuada pela equipe técnica da *DPES* à contratada e a recolocação do sistema em funcionamento de forma paliativa.
C) Prazo de solução definitiva: Tempo em horas úteis decorridos entra a solicitação efetuada pela equipe técnica da *DPES* à contratada e a efetiva recolocação do sistema em seu pleno estado de funcionamento e operações normais.

16.8. Depois de concluído o suporte técnico, a contratada comunicará o fato à *DPES* e solicitará autorização para o fechamento do chamado. Caso a *DPES* não confirme a solução definitiva do problema, o chamado permanecerá aberto até que seja efetivamente solucionado pela contratada. Nesse caso, a *DPES* fornecerá as pendências relativas ao chamado aberto.

16.9. Os serviços de garantia e suporte técnico iniciarão a partir da data de aceite do recebimento definitivo da solução de Auditoria de Acesso Remoto.

CLAUSULA DECIMA SÉTIMA – DA PROPRIEDADE, SIGILO E RESTRIÇÕES

17.1 Todas as informações, imagens, aplicativos, dados e/ou Metadados trafegados e documentos que forem manuseados e utilizados, são de propriedade da *DPES*, não podendo ser repassadas, copiadas, alteradas ou absorvidas na relação de bens da empresa contratada, bem como de seus executores, sem expressa autorização do Gestor do Contrato;

17.2. A empresa CONTRATADA obriga-se a dar ciência à *DPES*, imediatamente e por escrito, sobre qualquer anormalidade que verificar na prestação dos serviços;

17.3. Os executores da empresa CONTRATADA que atuarão na implantação e nos demais serviços previstos receberão acesso privativo e individualizado, não podendo repassá-los a terceiros, sob pena de responder, criminal e judicialmente, pelos atos e fatos que venham a ocorrer, em decorrência deste ilícito;

17.4. Todas as informações obtidas ou extraídas pela empresa CONTRATADA quando da execução dos serviços deverão ser tratadas como confidenciais, sendo vedada qualquer reprodução, utilização ou divulgação a terceiros, zelando pela manutenção do sigilo absoluto sobre os dados, informações, documentos, especificações técnicas e comerciais de que eventualmente tenham conhecimento ou acesso em razão dos serviços executados;

17.5. Cada profissional a serviço da empresa CONTRATADA deverá estar ciente de que a estrutura da *DPES* não poderá ser utilizada para fins particulares;

17.6. A empresa CONTRATADA deverá entregar à *DPES* toda e qualquer documentação produzida decorrente da prestação de serviços, objeto desta licitação, bem como, cederá à *DPES*, em caráter definitivo e irrevogável, o direito patrimonial e a propriedade dos hardwares, softwares e insumos instalados para o atendimento deste objeto durante a vigência do contrato e eventuais aditivos.

CLÁUSULA DÉCIMA SEXTA – DO FORO

18.1. Fica eleito o foro de Vitória, Comarca da Capital do Estado do Espírito Santo, para dirimir qualquer dúvida ou contestação oriunda direta ou indiretamente deste instrumento, renunciando-se expressamente a qualquer outro, por mais privilegiado que seja.

18.9. E, por estarem justos e contratados, assinam o presente em três vias de igual teor e forma, para igual distribuição, para que produza seus efeitos legais.

Vitória, 25 de agosto de 2021.

DEFENSORIA PÚBLICA DO ESTADO DO ESPIRITO SANTO
GILMAR ALVES BATISTA

BRINFOR SOLUÇÕES EM TI LTDA
representada por seu responsável legal **Bruno Vieira Rodrigues – CPF 046.557.606-05**

PODER JUDICIÁRIO - TJMG - CORREGEDORIA GERAL DE JUSTIÇA
º TABELIONATO DE NOTAS DE NOVA LIMA MG
teconheço, por semelhança, a(s) assinatura(s) de
RUNO VIEIRA RODRIGUES
m testemunho da verdade.
lova Lima, 26/08/2021 10:21:52 6180
ELO DE CONSULTA: EVZ53416
ÓDIGO DE SEGURANÇA: 5776.5384.2090.7993
uantidade de atos praticados: 01
to(s) praticado(s) por:
LIANE PAOLA CARDOSO SIQUEIRA - Escrevente
nol:R$5,82 TFJ:R$1,81 Total:R$7,63 ISS:R$0,27
onsulte a validade deste selo no site https://selos.tjmg.jus.br
Nº DA ETIQUETA ABK285625
TABELIONATO DE NOTAS DE NOVA LIMA - MG

ANEXO I

Este documento é parte integrante da Ata de Registro de Preços nº 031/2021, celebrada entre a **DEFENSORIA PÚBLICA DO ESTADO DO ESPÍRITO SANTO** e a empresa **BRINFOR SOLUÇÕES EM TI LTDA,** cujos preços estão a seguir registrados por item, em face à realização do Pregão nº 029/2021.

1. DO OBJETO

1.1. Registro de Preço para contratação de soluções de antivírus e antispam para proteção de endpoints e servidores, para atender esta Defensoria Pública do Estado do Espírito Santo.

- **ESPECIFICAÇÕES DO OBJETO**

LOTE 01

ITEM	DESCRIÇÃO	UN. DE FORNECIMENTO	QUANT. MÍNIMA	QUANT. MÁXIMA	VALOR UNITÁRIO	VALOR TOTAL
01	Aquisição de solução de Antivírus Next Generation (NGAV) Endpoints (estações de trabalho / mobile) e servidores por no mínimo 36 meses com instalação, configuração, suporte técnico, atualizações e treinamento (repasse tecnológico)	UN	950	1200	R$ 170,00	R$ 204.000,00

VALOR TOTAL DO LOTE 01: R$ 204.000,00 (DUZENTOS E QUATRO MIL REAIS).

OBS 1: <u>Aquisição de solução de Antivírus Next Generation – NGAV</u>

A solução de antivírus é comum de mercado e não há necessidade de se impor a CONTRATANTE uma única solução de antivírus. Contudo, considerando que as especificações técnicas das soluções de antivírus de mercado convergem a padrões de qualidade comuns e passíveis de especificação objetiva, serão listadas os benefícios e vantagens para a aquisição desta nova solução.

Consideremos também que a aquisição de nova solução apesar de implicar em custos adicionais de instalação e de deployment da aplicação nos Endpoints das redes é de suma importância à adequação aos novos padrões de mercado.

A aquisição de nova solução implica na seguinte composição de custos estimada para 36 meses.

2.1. Aquisição de Solução de Segurança Next Generation para Endpoints e Servidores com a contratação de empresa especializada para fornecimento, instalação e treinamento da solução para a *DPES*, permitindo que tanto o suporte a solução quanto as funcionalidades sejam inteiramente interligadas e gerenciadas através de uma única console de gerenciamento.

2.2. O fabricante/fornecedor vencedor deverá prover treinamento (repasse de conhecimento) para operacionalização do software, bem como execução de serviços de planejamento, implantação e testes, com garantia de atualizações de segurança e novas versões do produto, além de suporte técnico pelo prazo mínimo de 36 (trinta e seis) meses e demais licenciamentos necessários ao funcionamento da Solução a contar do aceite de entrega dos softwares e licenças.

2.3. A solução ofertada pelo licitante vencedor em relação ao LOTE 01 deve possuir as seguintes características:

2.3.1. Das especificações técnicas mínimas

A) A solução deve ser do tipo cliente/servidor, onde a parte servidora mantém todas as configurações definidas pelo administrador e a parte cliente busca ou recebe essas configurações do servidor. O software cliente é instalado em estações de trabalho e outros clientes, como servidores e computadores portáteis.

B) O software de gerenciamento (parte servidora) é instalado em um ou mais servidores dedicados e dimensionados para esse fim, denominado, neste documento, de Servidores de Gerenciamento.

C) O servidor de Gerenciamento poderá também atuar de forma híbrida, ou seja, parte na rede *DPES* e outro módulo online por meio de armazenamento em nuvem.

D) A gestão online por meio de armazenamento em Nuvem completa para o Servidor de Gerenciamento também é permitida

E) Os Servidores de Gerenciamento devem atuar de forma redundante onde, no caso de falha de um dos servidores, o outro assume todas as funções da solução, sem provocar indisponibilidade para os Endpoints.

i. A solução deverá permitir a sincronização das configurações e dados entre os Servidores de Gerenciamento.

F) Na impossibilidade de operação redundante fail-safe dos servidores de gerenciamento, é permitida a salvaguarda em backup das configurações de forma agendada, onde os dados deverão ser mantidos fora dos servidores, em banco de dados SQL ou similar.

G) Permitir o gerenciamento de clientes com no mínimo os seguintes sistemas operacionais:

i. Windows Server 2008 R2 e superior, 32 e 64 bits;
ii. Windows 7, 32 e 64 bits;
iii. Windows 10 e superior, 32 e 64 bits;
iv. Android versão 6.0 e superior.

H) Deve suportar os seguintes requisitos mínimos:

i. Reputação de Arquivos, tanto locais como no acesso web;
ii. IPS de Próxima Geração (*Next Generation IPS*);
iii. Proteção de Navegadores (*Browser Protection*);
iv. Aprendizado de Máquinas (*Machine Learning*);
v. Análise Comportamental (*Behavioral Analysis*);

vi. Mitigação da Exploração de Memória (*Memory Exploit Mitigation*);
vii. Controle de Aplicações (*Application Control*);
viii. Controle de Dispositivos (*Device Control*);
ix. Emulação para Malware (*Emulation for Malware – Sandbox*);
x. Mitigação de Exploração de Vulnerabilidades em aplicações conhecidas (*Exploit Mitigation*).

I) Deve ter a capacidade de implementar a funcionalidade de "*Web Reputation*" utilizando como fonte de aprendizado a rede de inteligência do fabricante, correlacionando no mínimo as seguintes técnicas de proteção com os vetores de ataques, identificando não somente os aspectos maliciosos, como também as características de boa pontuação:

i. Exploração de navegadores com reputação de URL;
ii. Websites infectados com reputação de URL;
iii. Download de arquivos com reputação de arquivos.

J) A funcionalidade de "Machine Learning" deve trabalhar baseado no mínimo nas seguintes premissas:

i. Atualização da base de reputação das URL's com a periodicidade máxima de 2,0 horas;
ii. Bloqueio de URL's de má reputação;
iii. Bloqueio das instruções de "*Command & Control*";
iv. Atualização da base de reputação de Arquivos com a periodicidade máxima de 2,0 horas;
v. Bloqueio das ameaças polimorfas mesmo que arquivos desconhecidos;
vi. Prevenção de Falso Positivo;
vii. Bloqueio de Malwares desconhecidos e suas variantes.

K) A funcionalidade de emulação para Malware deve ter suporte para as plataformas Windows (32 e 64 bits), no caso de On–Premisses, sendo também permitido que o ambiente virtual (Sandboxing) opere em armazenamento em nuvem, possibilitando detectar e impedir as técnicas de evasão de detecção, mesmo que utilizando polimorfismo no seu empacotamento.

L) A solução de proteção dos Endpoints deve ter a funcionalidade específica de impedir as técnicas de manipulação e randomização de memória impossibilitando a exploração de vulnerabilidades em aplicações, para no mínimo:

i. Adobe PDF;
ii. Flash;
iii. Java;
iv. Navegadores (Internet Explorer, Microsoft Edge, Chrome e Firefox).

M) A solução deve ter a capacidade de impedir os ataques direcionados mesmo que utilizando as vulnerabilidades de dia zero, mitigando no mínimo os conhecidos comportamentos de exploração de vulnerabilidades:

i. Heap Spray Allocation (Exploits que iniciam através do HEAP);
ii. DLL Hijacking;
iii. Java Exploit Protection.

N) A solução deve ter a capacidade de implementar integração entre a gerência central com plataformas de terceiros, possibilitando no mínimo:

i. Capturas de Login e Logout na Gerência Central;
ii. Captura dos detalhes das máquinas protegidas;

iii. Captura dos detalhes de Domínios implementados pelo software;
iv. Captura dos detalhes de Grupos implementados pelo software;
v. Captura dos detalhes das políticas aplicadas;
vi. Captura das atualizações dos detalhes das políticas aplicadas;
vii. Captura da lista dos usuários administradores da solução;
viii. Criação de novos administradores da solução;
ix. Capacidade de mover clientes de Endpoints entre grupos lógicos.

O) A solução de proteção de Endpoints deve ter a capacidade de receber instruções de comando e ações diretamente do servidor contra aos ataques de APT (*Advanced Persistent Threats*), possibilitando ações mais rápidas, assertivas e minimizando falsos positivos.

P) A solução deve ter capacidade de implementar técnicas de EDR (*Endpoint Detection and Response*), possibilitando detecção e investigação nos Endpoints com atividades suspeitas.

Q) Exibir ícone na barra de ferramentas do sistema operacional do Endpoint, devendo ser possível configurá-la para que nenhum ícone seja exibido.

R) O software deve utilizar banco de dados MS SQL Server 2016 ou superior disponibilizado pela CONTRATADA. Será aceito software que utilize outro banco de dados relacional proprietário, desde que o licitante vencedor forneça a licença de banco de dados sem custo adicional e sem limite de armazenamento de dados.

S) Deverá prover funcionalidade de envio de logs para servidores do tipo Syslog.

T) Deverá permitir o gerenciamento de clientes que não estejam na rede interna da *DPES*, por meio de conectividade via Internet.

2.3.2. Console de Gerenciamento

A) Possuir administração centralizada por meio de console única de gerenciamento acessível através de tecnologia Web HTTPS.

B) Permitir a exportação de dados exibidos na console.

C) As configurações do Antivírus, AntiSpyware, Firewall, Proteção Contra Intrusos, Controle de Dispositivos e Controle de Aplicações deverão ser realizadas para máquinas físicas e virtuais através da mesma console.

D) A solução que será implantada para prestar os serviços deverá funcionar com agente único a ser instalado em estação de trabalho, servidores físicos e virtuais a fim de diminuir o impacto ao usuário final.

E) Deve possuir mecanismo de comunicação (via *push*) em tempo real entre servidor e clientes, para entrega de configurações e assinaturas.

F) Deve possuir mecanismo de comunicação randômico (via *pull*) em tempo determinado pelo administrador entre o cliente e servidor, para consulta de novas configurações e assinaturas evitando sobrecarga de rede e servidor.

G) Permitir a divisão lógica dos computadores, dentro da estrutura de gerenciamento, em sites, domínios e grupos, com administração individualizada por domínio.

H) O servidor de gerenciamento deverá possuir compatibilidade para instalação no sistema operacional Microsoft Windows Server 2016 ou superior.

I) O servidor de gerenciamento deverá possuir compatibilidade para instalação em Sistemas Operacionais 64 bits suportando, no mínimo, ambiente virtual VMware e Microsoft Hyper-V.

J) Possuir integração com LDAP, inclusive com o serviço de diretório Microsoft Active Directory, para importação da estrutura organizacional e autenticação dos Administradores.

K) Possibilidade de aplicar regras diferenciadas baseando-se na localidade lógica da rede.

L) Permitir que a localidade lógica da rede seja definida pelo conjunto dos seguintes itens:

i. IP e range de IP;
ii. Endereço de Servidores de DNS, DHCP e WINS;
iii. Conexão com o servidor de gerência.

M) Possibilidade de aplicar regras diferenciadas por grupos de máquinas.

N) Possuir a funcionalidade e recursos para a criação e agendamento periódicos de backups da base de dados ou fornecer uma ferramenta para tal finalidade.

O) Permitir a instalação remota pela console Web e via console de gerenciamento ou permitir a geração de um executável para instalação via Política de Grupo – GPO.

P) Descobrir automaticamente as estações da rede que não possuem o cliente instalado.

Q) Fornecer ferramenta de pesquisa de estações e servidores da rede que não possuem o cliente instalado com opção de instalação remota.

R) Fornecer atualizações do produto e das definições de vírus e proteção contra intrusos.

S) O console de gerenciamento deve permitir travar as configurações por senha nos clientes, definindo permissões para que somente o administrador possa alterar as configurações, desinstalar ou parar o serviço do cliente.

T) Capacidade de criação de contas de usuário com diferentes níveis de acesso de administração e operação.

U) Instalação e atualização do software sem a intervenção do usuário.

V) Possibilidade de configurar o bloqueio da desinstalação, desabilitar o serviço do cliente, importar e exportar configurações e abrir a console do cliente, por senha.

W) Utilizar comunicação segura (criptografada) entre o servidor de gerenciamento e o cliente gerenciado.

X) Deverá fornecer acesso gráfico aos problemas, eventos e alertas detectados, com opção de salvaguardar os logs ou direcioná-los para um servidor Syslog, além de oferecer mecanismos de emissão de alarmes via correio eletrônico, Syslog.

Y) Todos os eventos gerados pela solução devem ser armazenados por período configurável de até 12 meses.

Z) Deverá possuir integração com sistemas SIEM, para possibilitar coleta de logs de gerenciamento e correlação em "real-time".

AA) Permitir acesso a todos os logs, com interface para consultas com filtros.

2.3.3. Atualização de vacinas

A) Atualização incremental, remota e em tempo real das vacinas do Antivírus e mecanismo de verificação (Engine) dos clientes da rede.
B) Permitir criar planos de distribuição das atualizações via comunicação segura entre cliente e Servidores de Gerenciamento, Site do fabricante, Via Servidor de atualização interno e podendo eleger qualquer cliente gerenciado para distribuição das atualizações.
C) Atualização remota e incremental da versão do software cliente instalado.
D) Nas atualizações das configurações e das definições de vírus não poderá utilizar scripts de login, agendamentos ou tarefas manuais ou outros módulos adicionais que não sejam parte integrante da solução e sem requerer reinicialização do computador ou serviço para aplicá-la.
E) Atualização automática das assinaturas dos servidores de gerenciamento e clientes via Internet, com periodicidade mínima diária.
F) Capacidade de voltar qualquer vacina e assinatura anterior armazenadas no servidor, utilizando opção e comando do console podendo utilizar a arquitetura de grupos lógicos do console.
G) Capacidade de gerenciar vacinas aplicadas em clientes gerenciados que não estejam na rede interna da organização.
H) Possuir um único e mesmo arquivo de vacina de vírus para todas as plataformas Windows e versões do antivírus.

2.3.4. Quarentena

A) Possuir funcionalidades que permitam o isolamento (área de quarentena) de arquivos contaminados por códigos maliciosos que não sejam conhecidos ou que não possam ser reparados em um servidor central da rede.
B) Envio automático dos Metadados dos arquivos da área de isolamento para o fabricante, via protocolo seguro, onde este será responsável por gerar a vacina, automaticamente, sem qualquer tipo de intervenção do administrador. O recebimento da vacina deverá ocorrer da mesma forma que foi enviada e logo em seguida deverá ser aplicada nas estações de trabalho.

2.3.5. Cliente gerenciado

A) Suportar máquinas com arquitetura 32-bit e 64-bit.
B) Deve possuir funcionalidade de Firewall e de Detecção e Proteção de Intrusão (IDS/IPS) com as funcionalidades:
i. Suporte aos protocolos TCP, UDP e ICMP;
ii. Possuir proteção contra exploração de buffer overflow;
iii. Possuir proteção contra aos ataques de Denial of Service (DOS), Port-Scan e MAC Spoofing;
iv. Possibilidade de criar regras diferenciadas por aplicações;
v. Possibilidade de reconhecer automaticamente as aplicações utilizadas via rede baseado no fingerprint do arquivo;

vi. Proteger o computador identificando a impressão digital de cada executável existente no sistema, para que somente as aplicações que possuam essa impressão digital executem no computador;
vii. Funcionalidade de Whitelist e Blacklist para o recurso de Impressão digital para os executáveis, possibilitando bloquear todos os executáveis da lista ou só liberar os executáveis da lista;
viii. Permitir criação de zona confiável, permitindo que determinados IPs, protocolos ou aplicações se comuniquem na rede;
ix. Bloqueio de ataques baseado na exploração da vulnerabilidade;
x. Gerenciamento integrado a console de gerência da solução.

2.3.6. Funcionalidade de Antivírus e AntiSpyware

A) Proteção em tempo real contra vírus, trojans, worms, cavalos-de-tróia, spyware, adwares e outros tipos de códigos maliciosos.
B) Proteção anti-spyware deverá ser nativa do próprio antivírus, ou seja, não dependente de plug-in ou módulo adicional.
C) As configurações do anti-spyware deverão ser realizadas através da mesma console de todos os itens da solução.
D) Permitir a configuração de duas ações, primária e secundária, executadas automaticamente para cada ameaça, com as opções de: alertar, limpar automaticamente, apagar automaticamente ou colocar em quarentena.
E) Permitir configurar a verificação contra ameaças para ser executada de maneira manual, agendada e em Tempo Real detectando ameaças no nível do Kernel do Sistema Operacional e excluindo os Rootkits.
F) Permitir configurar a verificação contra ameaças com a possibilidade de selecionar uma máquina ou grupo de máquinas para rastrear com periodicidade mínima diária.
G) Permitir configurar a verificação contra ameaças com a possibilidade de selecionar uma máquina ou grupo de máquinas para rastrear.
H) Implementar intervalos de tempo para início de verificações agendadas de forma a reduzir impacto em ambientes virtuais.
I) Verificação de vírus nas mensagens de correio eletrônico, pelo antivírus da estação de trabalho, suportando clientes Outlook e POP3/SMTP.
J) Capacidade de detecção em tempo real de vírus novos, desconhecidos pela vacina com opção da sensibilidade da detecção (baixo, médio e alto).
K) Capacidade de identificação da origem da infecção, para vírus que utilizam compartilhamento de arquivos como forma de propagação informando nome ou IP da origem com opção de bloqueio da comunicação via rede.
L) Proteção com funcionalidades de otimização de verificação (escaneamento) aplicáveis para no mínimo:

i. Proteção de Antivírus e AntiSpyware;
ii. Proteção de heurística e reputação de arquivos em tempo real (real-time);
iii. Proteção IPS de Host;
iv. Controle de dispositivos e aplicações;

v. Cache local na reputação de arquivos, possibilitando não varrer arquivos categorizados como não maliciosos e já escaneados anteriormente;
vi. Capacidade de implementar varreduras otimizadas em máquinas físicas e virtuais, onde o arquivo verificado pela varredura uma vez, não será verificado novamente, até que ocorra alguma alteração no mesmo;
vii. Capacidade de realizar monitoramento em tempo real (*real-time*) por heurística correlacionando com a reputação de arquivos.

M) Possuir funcionalidades que permitam o isolamento (área de quarentena) de arquivos contaminados por códigos maliciosos que não sejam conhecidos ou que não possam ser reparados no cliente.

N) Permitir configurar ações a serem tomadas na ocorrência de ameaças, incluindo Reparar, Deletar, Mover para a Área de Isolamento e Ignorar.

O) Possuir funcionalidades que permitam a detecção, exclusão ou desinfecção de arquivos contaminados por códigos maliciosos mesmo que sejam compactados nos formatos ZIP, ARJ e RAR, tendo como abrangência até o 7º (sétimo) nível de compactação.

P) Capacidade de remoção automática total dos danos causados por spywares, adwares e worms, como limpeza do registro e pontos de carregamento, com opção de terminar o processo e terminar o serviço da ameaça no momento de detecção.

Q) Criar uma cópia backup do arquivo suspeito antes de limpá-lo.

R) Gerenciamento integrado à console de gerência da solução.

S) Capacidade de executar varreduras em tempo real (real time) contra aos ataques dirigidos às vulnerabilidades do navegador (browser).

T) Detecção e remoção de vírus de macro em tempo real.

2.3.7. Detecção Proativa de reconhecimento de novas ameaças

A) Funcionalidade de detecção de ameaças desconhecidas que estão em memória por comportamento dos processos e arquivos das aplicações.

B) Não utilizar a assinatura de vírus para esta funcionalidade e fornecer assinatura periódicas da técnica de detecção.

C) Capacidade de detecção de Keyloggers, Trojans, Spywares e Worms por comportamento dos processos em memória, com opção da sensibilidade distintas da detecção.

D) Reconhecimento comportamento malicioso de modificação da configuração de DNS e arquivo Host.

E) Possuir a funcionalidade de exclusão de detecção diferenciada do recurso de Antivírus.

F) Possibilidade de habilitar o recurso de correlacionamento da funcionalidade de detecção Proativa com a base de reputação do fabricante.

2.3.8. Funcionalidade de Controle de Dispositivos e Aplicações

A) Gerenciar o uso de dispositivos USB e CD/DVD, através de controles de leitura/escrita/execução do conteúdo desses dispositivos e também sobre o tipo de dispositivo permitido (Ex.: permitir mouse USB e bloquear disco USB).
B) Gerenciamento integrado a console de gerência da solução.
C) Permitir o bloqueio do uso de aplicações baseado em nome, diretório e hash da aplicação.
D) O software de proteção do Endpoint deve ter a capacidade de implementar controle de dispositivos para leitura, escrita e execução em Windows 7 e superiores, para no mínimo:

i. USB;
ii. CD/DVD;
iii. SD Card.

2.3.9. Funcionalidade de emissão de Relatórios e Monitoramento da solução

A) Pelo menos 25 tipos de relatórios diferentes, permitindo a exportação para os formatos PDF e HTML.
B) Recursos do relatório e monitoramento deverão ser nativos da própria console central de gerenciamento.
C) A capacidade de exibir a lista de servidores e estações que possuam a solução instalada, contendo informações como nome da máquina, usuário logado, versão do engine, data da vacina, data da última verificação e status.
D) A capacidade de Geração de relatórios, estatísticos e gráficos contendo no mínimo os seguintes tipos pré-definidos:

i. As 10 máquinas com maior ocorrência de códigos maliciosos;
ii. Os 10 usuários com maior ocorrência de códigos maliciosos;
iii. Localização dos códigos maliciosos;
iv. Número de infecções detectadas diário, semanal e mensal;
v. Códigos maliciosos detectados.

2.3.10. Console avançada de distribuição e Relatórios

A) Console de gerenciamento via tecnologia Web segura (HTTPS) independente da console central da solução.
B) Possibilidade de recuperar instalação em clientes em caso de falha.
C) Exportar os relatórios criados nos formatos PDF e HTML.

2.3.11. Funcionalidades do Controle de Acesso à Rede

A) Deve possibilitar a colocação dos equipamentos em quarentena, bloqueando o acesso à rede para aqueles computadores que não estiverem em conformidade com as políticas, para no mínimo as seguintes premissas:

i. Computador deve possuir antivírus, atualizado e ativo;
ii. Computador deve possuir firewall ativo;
iii. Computador deve possuir AntiSpyware, atualizado e ativo.

B) Deve ter a capacidade de alterar automaticamente as regras de firewall nos clientes que falharam na política restringindo o acesso à rede;

C) Deve ter a possibilidade de notificação customizada para o usuário com diferentes ícones e como erro, informação e notificação no idioma Português Brasil.