CONTRATO	Nº 216/2018	DATA 12/12/2018

CONTRATADO (A)
VTECH COMÉRCIO SERVIÇOS E EQUIPAMENTOS DE INFORMÁTICA EIRELI

OBJETO

Aquisição de licenças de uso de software antivírus corporativo com console de administração, etc.

DESO
COMPANHIA DE SANEAMENTO DE SERGIPE

CONTRATO Nº 216/2018

Contrato de **Prestação de Serviços**, que entre si fazem a **COMPANHIA DE SANEAMENTO DE SERGIPE – DESO** e a empresa **VTECH COMÉRCIO SERVIÇOS E EQUIPAMENTOS DE INFORMÁTICA EIRELI**, na forma abaixo:

PREÂMBULO

1. DAS PARTES E SEUS REPRESENTANTES

Pelo presente instrumento particular a **COMPANHIA DE SANEAMENTO DE SERGIPE – DESO**, pessoa jurídica de direito privado organizada sob a forma de Sociedade de Economia Mista, nos termos do Decreto-Lei nº 109 de 25 de agosto de 1969, com as alterações e acréscimos do Decreto-Lei nº 268 de 16 de janeiro de 1970 e da Lei Estadual nº 4.898 de 10 de julho de 2003, inscrita no CNPJ/MF sob o nº 13.018.171/0001-90 e no Cadastro Estadual sob o nº 27.051.036-2, com sede à Rua Campo do Brito, nº 331 – Bairro Praia 13 de Julho – Aracaju/SE, doravante denominada **CONTRATANTE**, representada neste ato por seu Diretor-Presidente **Jethro Duarte Moreira**, brasileiro, casado, engenheiro, inscrito no CNPF sob o nº 111.044.495-87 e seu Diretor de Gestão Corporativa **Haroldo Anderson Déda Filho**, brasileiro, casado, economista, inscrito o CNPF sob o nº 138.179.815-20 e a empresa **VTECH COMÉRCIO, SERVIÇOS E EQUIPAMENTOS DE INFORMÁTICA EIRELI** com sede na Avenida Santos Dumont, nº 4487, km 3,5, loja 157, Shopping Passeio Norte, Estrada do Coco, Lauro de Freitas/BA, CEP 42.702-400, inscrita no CNPJ/MF sob o nº 22.122.370/0001-34, por sua Representante Legal a Sra. **Luciana Santos da Silva**, inscrito no CNPF sob nº 790.641.595-72, resolvem celebrar o presente **CONTRATO** que se regerá pelas seguintes **CLÁUSULAS E CONDIÇÕES**:

2. DA FINALIDADE – O presente Contrato tem por finalidade formalizar e disciplinar o relacionamento contratual com vistas a prestação dos serviços definidos e especificados na **CLÁUSULA PRIMEIRA – OBJETO**, sendo que sua lavratura foi regularmente autorizada em despacho datado de 01/10/2018 do Senhor Presidente da DESO, em Processo Administrativo nº 94190/2018.

3. DO FUNDAMENTO LEGAL – Esta adjudicação decorre de licitação sob modalidade de **Pregão Eletrônico**, nos termos e condições do Edital nº **103/2018**, cujo resultado foi homologado em data de **03.12.2018** pelo Presidente, conforme consta do Processo Administrativo acima mencionado, submetendo-se as partes às disposições constantes da Lei nº 10.520/2002 e sua legislação suplementar, e à Lei nº 13.303/2016, às cláusulas e condições aqui estabelecidas pela Contratante.

CLÁUSULA I – DO OBJETO

1.1 – AQUISIÇÃO DE LICENÇAS DE USO DE SOFTWARE ANTIVÍRUS CORPORATIVO COM CONSOLE DE ADMINISTRAÇÃO, SERVIÇOS DE TREINAMENTO, CONFIGURAÇÕES E SUPORTE TÉCNICO REMOTO ON-SITE.

CLÁUSULA II – DO PREÇO

2.1 – A DESO pagará à Contratada pelo fornecimento objeto deste Contrato, a importância de **R$ 57.896,80 (cinquenta e sete mil oitocentos e noventa e seis reais e oitenta centavos).**

CLÁUSULA III – DOS PRAZOS

3.1 – O prazo de vigência deste Contrato será de **30 (trinta) dias**, contando-se a partir da emissão da Ordem de Serviço.

3.2 – O prazo de execução será de **30 (trinta) dias,** contados a partir da emissão da Ordem de Serviço.

3.3 – A Contratada, com domicílio no Estado de Sergipe, será convocada, para a assinatura das 02 (duas) vias do Contrato, devendo fazê-lo em 05 (cinco) dias úteis, sob pena de decair o seu direito à contratação, além de sujeitá-la às penalidades previstas no Pregão Eletrônico originante deste Instrumento.

a) Para a Contratada com domicílio fora do Estado de Sergipe, será enviada ao endereço de email fornecido pela mesma, a mídia digitalizada do Contrato no formato PDF, que deverá ser assinada em 02 (duas) vias, cuja devolução de ambas, deverá ocorrer em até 10 (dez) dias úteis.

CLÁUSULA IV – DO RECURSO FINANCEIRO

4.1 – Para os pagamentos decorrentes deste Contrato, serão utilizados recursos financeiros provenientes da **Receita Própria da DESO – Rubrica 10.**

CLÁUSULA V – DA DOCUMENTAÇÃO

5.1 – Quando da assinatura do presente instrumento, a Contratada, deverá apresentar a Certidão Conjunta Negativa de Débitos Relativos aos Tributos Federais e à Dívida Ativa da União, abrangendo as Contribuições Previdenciárias e às de Terceiros (INSS), o Certificado de Regularidade do FGTS (CRF), a Certidão de Regularidade de Tributos Estaduais (ICMS), Certidão Trabalhista(CNDT) dentro do prazo de validade, sob pena de decair o seu direito à contratação.

CLÁUSULA VI – DA SUBCONTRATAÇÃO E ALTERAÇÃO SUBJETIVA

6.1 - Não será admitida a subcontratação do objeto licitatório.

CLÁUSULA VII – DA FORMA DE PAGAMENTO

7.1 – O objeto deste Contrato será pago mediante apresentação à DESO dos documentos abaixo transcritos e exigidos na R.D.E. nº 12 de 13/07/04 e na R.D.E nº 21/2015 de 22/10/2015 desta Companhia, que depois de conferidos e visados serão encaminhados para processamento e posterior pagamento em **30 (trinta) dias** consecutivos, contados a partir da data de entrada da fatura no Protocolo da DESO;

- As faturas só serão liberadas para pagamento após aprovadas pela Fiscalização da DESO.

- Qualquer erro detectado no documento de cobrança acarretará a devolução do mesmo à Contratada para correções e acertos, iniciando-se, após nova apresentação, a contagem de novos prazos para pagamento.

7.1.1 – Nota Fiscal e Fatura/Recibo com o mesmo CNPJ constante do processo licitatório e do preâmbulo deste instrumento, constando nos seus anversos, o número do Contrato e da Ordem de Serviço;

a) Quando houver emissão de nota fiscal eletrônica, informamos que a DESO disponibiliza o seguinte endereço eletrônico: **nfse@deso-se.com.br**, para recepcionar as notas fiscais eletrônicas emitidas pela empresa contratada.

7.1.2 – Certidão Conjunta Negativa ou Positiva com efeito Negativo, de Débitos Relativos aos Tributos Federais e à Dívida Ativa da União, emitida pela Secretaria da Receita Federal do Ministério da Fazenda comprovando sua regularidade para com a Fazenda Federal, abrangendo as Contribuições Previdenciárias e às de Terceiros (INSS);

7.1.3 – Certidão Negativa ou Positiva com efeito Negativo, de Débitos Trabalhistas (CNDT), comprovando a inexistência de débitos inadimplidos perante a Justiça do Trabalho, 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, em conformidade com a Lei nº 12.440, de 07/07/2011;

7.1.4 – Certidão de Regularidade do FGTS – CRF, emitida pela Caixa Econômica Federal – CAIXA, comprovando sua regularidade perante o Fundo de Garantia por Tempo de Serviço.

7.1.5 – Prova de regularidade para com a Fazenda Estadual (ISS) do domicílio ou sede da Contratada;

7.1.6- Prova de regularidade para com a Fazenda Estadual (ICMS) do domicílio ou sede da CONTRATADA;

7.1.7 – Apresentar DARF da retenção de 1,5% IRPJ e DARF da retenção de 4,65% (CSII, COFINS, PIS/PASEP);

7.1.8 – Certidão Negativa de Débitos, emitida pela DESO, referente aos serviços prestados pela Companhia, conforme R.D.E. nº 21/2015, de 22/10/2015;

7.2 – É de inteira responsabilidade da Contratada a entrega a DESO, dos documentos de cobrança acompanhado dos seus respectivos anexos, de forma, clara, objetiva e orde-nada, que se não atendido, implica em desconsideração pela DESO dos prazos estabelecidos para conferência e pagamento.

7.3 – A Nota fiscal/Fatura deverá destacar o valor dos impostos ou informar a isenção, não incidência ou alíquota zero, e respectivo enquadramento legal, sob pena de retenção do imposto de renda e das contribuições sobre o valor total do documento fiscal, no percentual correspondente à natureza do bem ou serviço.

7.4 – Caso a Contratada seja optante do SIMPLES, deverá apresentar, acompanhado da Nota Fiscal, a devida comprovação, a fim de evitar a retenção na fonte dos tributos e contribuições, conforme legislação em vigor.

7.5 – Nenhum pagamento será efetuado à empresa, enquanto houver pendência de liquidação de obrigação financeira, em virtude de penalidade ou inadimplência contratual.

7.6 – Somente poderá ser acatada junto ao faturamento, Nota Fiscal dentro do seu período de validade de emissão, cujo CNPJ – Cadastro Nacional de Pessoas Jurídicas corresponda àquele do Contrato e da respectiva Ordem de Serviço.

7.7 – Todo e qualquer pagamento será efetuado através da Rede Bancária de Aracaju, sob pena da incidência das taxas de serviços para pagamentos por Ordem Bancária para outras Praças.

7.8 – A DESO incorrerá em mora caso não efetue o pagamento das faturas no 30º (trigésimo) dia de sua apresentação no protocolo da DESO, conforme disposto no item ***7.1*** acima, desde que a Contratada não tenha concorrido de alguma forma para tanto. Passado este prazo, estará obrigada a efetuar a compensação financeira, ou seja, correção monetária por atraso de pagamento, calculada com base no INPC ou outro índice substitutivo, calculando-se o período compreendido entre o 31º (trigésimo primeiro) dia até a data do seu efetivo pagamento.

7.8.1- Caso o trigésimo dia ocorra em data não útil na administração da DESO, o vencimento será prorrogado para o primeiro dia útil subsequente;

7.8.2 – A administração da DESO poderá realizar pagamento antes do 30º (trigésimo) dia da apresentação das faturas no protocolo da DESO, sendo que no caso da DESO efetuar o pagamento após o 30º(trigésimo) dia e havendo requerimento do contratado pela mora, a DESO deverá promover a compensação financeira quando ocorrer pagamentos antecipados, calculado com base no INPC ou outro índice substitutivo, entre a data do efetivo pagamento e a data de vencimento.

7.9 – A DESO fica autorizada a promover a retenção de créditos devidos em decorrência da execução do presente contrato quando se fizer necessário para evitar prejuízo decorrente do inadimplemento do contrato.

7.10 – Fica estabelecido que a contratada não procederá ao desconto de título, não fará cessão de crédito, nem fará apresentação para cobrança pela rede bancaria e a DESO não endossará nem dará aceite a eventuais títulos que forem apresentados por terceiros.

7.11- Nenhum pagamento será efetuado, a qualquer título, à empresa que tenha em seu quadro societário servidor público da ativa, ou empregado de empresa pública ou de sociedade de economia mista, por serviços prestados, inclusive consultoria, assistência técnica ou assemelhados.

CLÁUSULA VIII – SUSTAÇÃO DO PAGAMENTO

8.1 – Os pagamentos poderão ser sustados nos seguintes casos:

a) Irregularidade, avaria ou defeito no serviço prestado, ou realizado fora dos padrões exigidos, de responsabilidade da Contratada;
b) Não cumprimento dos prazos, em desobediência as condições estabelecidas no Contrato;
c) Não apresentação dos documentos exigidos no item anterior;
d) Erro ou vício da Fatura;

e) Apresentação de Fatura/Nota Fiscal/Recibo, com CNPJ diferente do constante no preâmbulo deste instrumento.

8.2 – Na ocorrência da hipótese prevista na alínea **"d"** acima mencionada, as faturas serão devolvidas para respectiva correção, contando-se o prazo de seu vencimento a partir da data da sua reapresentação

CLÁUSULA IX – DAS OBRIGAÇÕES DA CONTRATADA

9.1- Além dos encargos resultantes da observância da Lei nº 13.303/2016, da Lei nº 10.520/02 e do Regulamento Interno de Licitações, Contratos e Convênios da DESO, compete à Contratada:

9.1.1 – Executar os serviços conforme especificações deste Termo de Referência e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, além de fornecer e utilizar os materiais e equipamentos, ferramentas e utensílios necessários, na qualidade e quantidade mínimas especificadas neste instrumento e em sua proposta;

9.1.2 – Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução;

9.1.3 – Manter os empregados nos horários predeterminados pela Contratante;

9.1.4 – Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com os artigos 14 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990), ficando a Contratante autorizada a descontar da garantia prestada, caso exigida no edital, ou dos pagamentos devidos à Contratada, o valor correspondente aos danos sofridos;

9.1.5 – Utilizar empregados habilitados e com conhecimentos básicos dos serviços a serem executados, em conformidade com as normas e determinações em vigor;

9.1.6 – Apresentar os empregados devidamente identificados por meio de crachá, além de provê-los com os Equipamentos de Proteção Individual – EPI;

9.1.7 – Apresentar à Contratante, quando for o caso, a relação nominal dos empregados que adentrarão no órgão para a execução do serviço;

9.1.8 – Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas na legislação específica, cuja inadimplência não transfere responsabilidade à Contratante;

9.1.9 – Atender às solicitações da Contratante quanto à substituição dos empregados alocados, no prazo fixado pela fiscalização do contrato, nos casos em que ficar constatado descumprimento das obrigações relativas à execução do serviço, conforme descrito neste Projeto Básico;

9.1.10 – Instruir seus empregados quanto à necessidade de acatar as Normas Internas da Contratante;

9.1.11 – Instruir seus empregados a respeito das atividades a serem desempenhadas, alertando-os a não executarem atividades não abrangidas pelo contrato, devendo a Contratada relatar à Contratante toda e qualquer ocorrência neste sentido, a fim de evitar desvio de função;

9.1.12 – Relatar à Contratante toda e qualquer irregularidade verificada no decorrer da prestação dos serviços;

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

9.1.14 – Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

9.1.15 – Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

9.1.16 – Manter preposto aceito pela Contratante nos horários e locais de prestação de serviço para representá-la na execução do contrato com capacidade para tomar decisões compatíveis com os compromissos assumidos;

9.1.17 – Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança da Contratante;

9.1.18 – Instruir os seus empregados, quanto à prevenção de incêndios nas áreas da Contratante;

9.1.19 – Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, fornecendo todos os materiais, equipamentos e utensílios em quantidade, qualidade e tecnologia adequadas, com a observância às recomendações aceitas pela boa técnica, normas e legislação;

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

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

9.1.22 – Manter sigilo, sob pena de responsabilidades civil, pena e administrativa, sobre qualquer assunto de interesse da DESO ou de terceiros de que tomar conhecimento em razão da execução do objeto do contrato;

9.1.23 – Manter em caráter confidencial as informações relativas ao processo de instalação, configuração e adaptações de produtos, ferramentas e equipamentos, mesmo após o término do prazo de vigência ou rescisão contratual.

CLÁUSULA X – DAS OBRIGAÇÕES DA CONTRATANTE

10.1- Além dos encargos resultantes da observância da Lei nº 13.306/2016 e da Lei nº 10. 520/02, são obrigações da DESO:

10.1.1 – Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta;

10.1.2 – Exercer o acompanhamento e a fiscalização dos serviços, por servidor ou comissão especialmente designada, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, encaminhando os apontamentos à autoridade competente para as providências cabíveis;

10.1.3 – Notificar a Contratada por escrito da ocorrência de eventuais imperfeições, falhas ou irregularidades constatadas no curso da execução dos serviços, fixando prazo para a sua correção, certificando-se de que as soluções por ela propostas sejam as mais adequadas;

10.1.4 – Pagar à Contratada o valor resultante da prestação do serviço, conforme cronograma físico-financeiro;

10.1.5 – Efetuar as retenções tributárias devidas sobre o valor da fatura de serviços da Contratada consoante previsão na legislação;

10.1.6 – Fornecer por escrito as informações necessárias para o desenvolvimento dos serviços objeto do contrato;

10.1.7 – Realizar avaliações periódicas da qualidade dos serviços, após seu recebimento;

10.1.8 – Cientificar a Assessoria Jurídica de Licitações e Contratos para adoção das medidas cabíveis quando do descumprimento das obrigações pela Contratada;

10.1.9 – Aplicar as sanções administrativas, quando se fizerem necessária.

10.1.10 – A Administração não responderá por quaisquer compromissos assumidos pela Contratada com terceiros, ainda que vinculados à execução do Contrato a ser firmado, bem como por qualquer dano causado a terceiros em decorrência de ato da Contratada, de seus empregados, prepostos ou subordinados.

CLÁUSULA XI – DAS SANÇÕES ADMINISTRATIVAS

11.1 - A Contratada, pelo inadimplemento de suas obrigações, garantida a sua prévia defesa no prazo de 10 (dias) dias úteis, ficará sujeita as seguintes sanções previstas no RILC e na Lei 13.303/2016:

11.1.1 - Advertência;
11.1.2 - Multa moratória;
11.1.3 - Multa compensatória;
11.1.4 - Suspensão do direito de participar de licitação e impedimento de contatar com a DESO, pelo prazo de até 02 (dois) anos;
11.1.5 - Declaração de inidoneidade para licitar ou contratar com a Administração Pública.

11.2 - As sanções constantes no subitem 11.1 poderão ser aplicadas de forma cumulativa.

11.3 - Ficará suspenso de licitar e de contratar com a DESO, pelo prazo de até 02 (dois) anos, garantido o direito prévio de defesa, o fornecedor que:

11.3.1 - Ensejar o retardamento da execução do objeto desta licitação;
11.3.2 - Não mantiver proposta, injustificadamente;
11.3.3 - Comportar-se de modo inidôneo;
11.3.4 - Fizer declaração falsa;
11.3.5 - Cometer fraude fiscal;
11.3.6 - Falhar ou fraudar no fornecimento do objeto.

11.4 - São consideradas condutas reprováveis e passíveis de sanções, dentre outras, as previstas no art. 186 do RILC.

11.5 - As multas estabelecidas serão entendidas como independentes e cumulativas e serão compensadas pela DESO com as importâncias em dinheiro, relativas às prestações a que corresponderem, ou da garantia do contrato, quando for o caso, cobradas judicialmente.

11.6 - A aplicação de sanção de advertência se efetiva com o registro da mesma junto ao cadastro de fornecedores e no sistema de gerenciamento de contatos da DESO, independentemente de tratar-se de pessoa cadastrada ao não.

11.7 - A multa poderá ser aplicada nos seguintes casos:

I – Em decorrência da interposição de recursos meramente procrastinatórios, poderá ser aplicada multa correspondente 3% do valor máximo estabelecido para a licitação em questão.

II – Em decorrência da não regularização da documentação de habilitação, nos termos do artigo 43, § 1º da Lei Complementar nº 123/2006, poderá ser aplicada multa correspondente 3% do valor máximo estabelecido para a licitação em questão.

III – Pela recusa em assinar o contrato, aceitar ou retirar o instrumento equivalente, dentro do prazo estabelecido por este edital, poderá ser aplicada multa correspondente a 5% do valor máximo estabelecido para a licitação em questão.

IV – No caso de atraso na entrega da garantia contratual, quando exigida, o instrumento convocatório deverá prever, mediante competente justificativa, a incidência de multa correspondente 3% do valor total do contrato;

V – No caso de inexecução parcial, incidirá multa na razão de 10% sobre o valor da parcela não executada;

VI – No caso de inexecução total, incidirá multa na razão de 25% sobre o saldo remanescente do contrato;

VII – Nos demais casos de atraso, incidirá multa na razão de 5% sobre o valor da parcela em atraso.

11.8 - Caso não haja o recolhimento da multa no prazo estipulado, a DESO descontará a referida importância de eventuais créditos a vencer da empresa contratada. Na ausência de créditos disponíveis para quitação da importância da multa, a DESO executará a garantia quando exigida, e quando for o caso, será cobrada judicialmente.

11.9 - A DESO poderá quando do não pagamento da multa pela Contratada, aplicar a sanção de suspensão do direito de participar de licitação e impedimento de contratar com a DESO, por até 02 (dois) anos;

11.10 - Cabe a sanção de suspensão em razão de ação ou omissão capaz de causar, ou que tenha causado dano à DESO, suas instalações, pessoas, imagem, meio ambiente ou a terceiros, aplicando a disposição do art. 189 e 190 do RILC em face da legislação fiscal, previdenciária, social ou trabalhista.

CLÁUSULA XII - DA FISCALIZAÇÃO DO CONTRATO

12.1 – O acompanhamento e a fiscalização da execução deste Contrato consistem na verificação da conformidade da prestação dos serviços, dos materiais, técnicas e equipamentos empregados, de forma a assegurar o perfeito cumprimento do ajuste, que serão exercidos por um ou mais representantes da Contratante, especialmente designados, na forma dos *arts. 174* a *177* do RILC.

12.2 - Para a execução do objeto deste Contrato, será designada a comissão de fiscalização, sendo o gestor do Contrato, seu Presidente.

12.3 - A comissão de fiscalização terá plenos poderes para decidir sobre questões técnicas e burocráticas relativa aos serviços, sem que implique a transferência de responsabilidade sobre sua execução, a qual será única e exclusivamente da contratada.

Quando as decisões ou as providências ultrapassarem a competência do gestor de contrato, deverá solicitar aos seus superiores hierárquicos, em tempo hábil, a adoção das medidas cabíveis, sob pena de responsabilidade solidária pelos danos causados por sua omissão.

12.4 - A fiscalização, o acompanhamento, a orientação e o recebimento dos serviços ficará a cargo da comissão de fiscalização.

12.5 - As relações entre a DESO e a Contratada serão mantidas por intermédio dos membros da comissão de fiscalização.

12.6 - A comissão de fiscalização rejeitará, no todo ou em parte, o objeto em desconformidade com as especificações.

12.7 - Os esclarecimentos solicitados pelo gestor do contrato deverão ser prestados imediatamente, ou em prazo fixado, levando em consideração a complexidade do caso.

12.8 - A comissão de fiscalização anotará, em registro próprio, as eventuais falhas detectadas em 2 (duas) vias, uma das quais será encaminhada e visada pela Contratada para, a partir de então, produzir seus efeitos.

12.9 - A fiscalização será exercida no interesse da DESO, não excluindo ou reduzindo esta atividade a responsabilidade da Contratada pela adequada prestação dos serviços contratados e pelos danos ou prejuízos por ele causados, por culpa ou dolo, a DESO ou a terceiros.

CLÁUSULA XIII – DA DESCRIÇÃO DOS SERVIÇOS

13.1- Os serviços estão em um **LOTE ÚNICO** e descritos no **Item 03** do **TERMO DE REFERENCIA**, abaixo transcritos:

13.1.1 - O software para estações de trabalho e máquinas servidores deverá atender as seguintes especificações:

13.1.1.1 - Licenciamento de uso do software para 1000 estações de trabalho e 40 servidores;
13.1.1.2 - Upgrade de versões e atualizações do software de antivírus por 03 (três) anos, sem custos adicionais;
13.1.1.3 - Atualizações das definições de malware por 03 (três) anos, sem custos adicionais;
13.1.1.4 - Suporte em português do Brasil, oferecido pelo próprio fabricante, representante ou parceiro certificado do software de antivírus, por telefone 08x05 e, quando necessário, presencialmente nas instalações da CONTRATANTE, conforme as especificações de níveis de serviço deste Termo por 03 (três) anos;
13.1.1.5 - Ser compatível para instalação em estações de trabalho e servidores com os seguintes sistemas operacionais: Microsoft Windows 7 (32 e 64 bits); Microsoft Windows 7 SP1 (32 e 64 bits) ou mais recente; Microsoft Windows 8 e 8.1 (32 e 64 bits); Microsoft Windows 10 (32 e 64 bits); Microsoft Windows Server 2008 e 2008 R2, Microsoft Windows Server 2012 e 2012 R2; Microsoft Windows Server 2016; Microsoft Small Business Server 2008 e 2011; Ubuntu 14.x, 16.x, 18.x ou mais recente, SUSE Linux Enterprise Server 11 SP3 ou mais recente; GNU/Linux 64 bits; Hyper-V, Vmware, Vsphere Essential Plus;
13.1.1.6 - Servidor de gerenciamento instalável em Microsoft Windows Server 2008 e 2008 R2, Microsoft Windows Server 2012 e 2012 R2; Microsoft Windows Server 2016; Microsoft Small Business Server 2008 e 2011; Ubuntu 14.x, 16.x, 18.x ou

mais recente, SUSE Linux Enterprise Server 11 SP3 ou mais recente; GNU/Linux 64 bits; Hyper-V, Vmware, Vsphere Essential Plus;
13.1.1.7 - Console de Gerenciamento instalável em todas as plataformas do servidor de gerenciamento, além das seguintes plataformas: Microsoft Windows 7 (32 e 64 bits); Microsoft Windows 7 SP1 (32 e 64 bits) ou mais recente; Microsoft Windows 8 e 8.1 (32 e 64 bits); Microsoft Windows 10 (32 e 64 bits);
13.1.1.8 - Todas as funcionalidades devem ser ativadas por agente de modo a facilitar a instalação, a configuração e o gerenciamento;
13.1.1.9 - Ser composto de software dedicado à proteção contra diversos tipos de malware, tais como vírus, spyware, adware, worm, rootkit e vulnerabilidades zero-hour para estações de trabalho e servidores;
13.1.1.10 - Detectar e remover malwares localizados em drives locais, diretórios e subdiretórios, mídias removíveis, programas executáveis, setores de BOOT e vírus de macro;
13.1.1.11 - Permitir a instalação remota do software via console, por script de login ou Política de Grupo (GPO), e impedir a interrupção do processo de instalação ou a sua desinstalação pelo usuário;
13.1.1.12 Toda a solução de segurança proposta deverá ser fornecida por um único fabricante, de modo que tanto o suporte à solução quanto as suas funcionalidades sejam inteiramente integradas e gerenciadas através de um único console de gerenciamento;
13.1.1.13 - O software antivírus para estações e servidores deverá ser baseado em três níveis: console de gerenciamento, servidores de gerenciamento e agente de comunicação entre cliente antivírus e servidor antivírus;
13.1.1.14 - A conexão entre o cliente e o servidor antivírus deverá suportar configurações sobre os protocolos TCP/IP;
13.1.1.15 - A proteção anti-spyware deverá ser nativa da própria solução, isto é, não poderá depender de plugin ou módulo adicional;

13.1.2 Solução para servidores Windows:

13.1.2.1 - Possuir a capacidade de atualizar remotamente e em tempo real, as listas de definições de malware, sem a necessidade de utilização de login-scripts, agendamentos ou intervenções do usuário;
13.1.2.2 - Possuir capacidade de programação de atualizações das listas de definições de malware, a partir de local predefinido da rede ou site da Internet;
13.1.2.3 - Possuir capacidade de atualização das listas de definições de malware por meio de um servidor proxy, fornecido pelo fabricante da solução, para redução do consumo de banda em sites remotos;
13.1.2.4 - Possuir atualização incremental das assinaturas nas estações de trabalho;
13.1.2.5 - Realizar, no mínimo, 03 (três) atualizações diárias das listas de definições de malware;
13.1.2.6 - O sistema de antivírus ofertado deve permitir a programação de, no mínimo, duas ações automáticas (primária e secundária), para o caso de detecção de malware, com as seguintes opções:
13.1.2.6.1 - Somente alertar;
13.1.2.6.2 - Limpar automaticamente;
13.1.2.6.3 - Apagar automaticamente;
13.1.2.6.4 - Colocar em quarentena (isolar);
13.1.2.7 Possibilitar a tomada de ações independentes para casos de detecção de malware;
13.1.2.8 - Relatar para o console de gerenciamento todos os tipos de programas potencialmente perigosos (ex: spyware) para que sua utilização possa ser definida (liberada ou bloqueada) pelo administrador;
13.1.2.9 Possuir controle de aplicativos que acessam a rede, reportando todos eles

para o console de gerenciamento, de forma que o administrador possa controlar sua utilização pelos usuários (liberar ou bloquear a abertura e o recebimento de conexões);

13.1.2.10 Possibilitar acionamento de função de verificação do sistema de forma manual, pré-agendada ou em tempo real contra vírus, worms, cavalos de troia e demais tipos de códigos maliciosos;

13.1.2.11 Possuir proteção em tempo real contra vírus, worms, cavalos de troia, spywares, adwares, e demais tipos de códigos maliciosos, integrada em uma única solução independente de plugin ou módulo adicional;

13.1.2.12 - Possuir proteção contra rootkits;

13.1.2.13 - Detectar e remover cookies potencialmente indesejáveis no sistema (ex: cookies de rastreamento);

13.1.2.14 - Permitir a verificação em tempo real e a verificação manual de todos os tipos de arquivos, bem como a definição dos tipos de arquivos a serem verificados contra malware;

13.1.2.15 - Permitir a criação de listas de exclusões de objetos da varredura (diretórios, arquivos e extensões de arquivos);

13.1.2.16 - Realizar verificação e proteção do sistema de registro (registry) contra modificações não autorizadas;

13.1.2.17 - Reconhecer e impedir, através de análise heurística, a ação de software malicioso ao tentar executar funções que possam causar dano ao sistema, tais como alterar o registro do sistema operacional e associações críticas a arquivos, com capacidade de finalizar processos perigosos que possam causar instabilidade ou risco ao sistema;

13.1.2.18 - Possuir rastreamento manual, disparado pelo usuário, com interface gráfica e opções de seleção de arquivos, diretórios ou discos a serem analisados, ou de varredura completa da estação, inclusive com verificação de rootkits;

13.1.2.19 - Detectar novos tipos de ameaças, ainda desconhecidas, como spyware, adware, jokes, dialers, remote access, trackware e ferramentas de hack através de análise heurística de comportamento;

13.1.2.20 - Possuir sistema de proteção proativo que realize análise na nuvem (in-the-cloud) através da Internet, utilizando base de dados mundial de reputação de aplicações disponibilizada pelo fabricante;

13.1.2.21 - Permitir o envio de amostras de arquivos suspeitos para análise do fabricante;

13.1.2.22 - Deve possuir a capacidade de detectar a origem de ameaças na rede, fornecendo informações como endereço IP e nome DNS / NetBios;

13.1.2.23 - Realizar o rastreamento em tempo real, para arquivos criados, copiados, renomeados, movidos ou modificados;

13.1.2.24 - Realizar a verificação de malware em arquivos compactados em pelo menos 05 (cinco) níveis de profundidade;

13.1.2.25 - Possuir, no mínimo, 02 (dois) mecanismos (engines) anti-malware trabalhando simultaneamente e gerenciados através do mesmo console de gerenciamento;

13.1.2.26 - Gerar registro (log) dos eventos de detecção de malware em arquivo em local definido pelo usuário;

13.1.2.27 - Possuir geração e exibição de alertas em caso de detecção de malware, através de mensagem na tela, no console de administração e no sistema de registro de eventos da estação, via SNMP e e-mail SMTP;

13.1.3 - Solução para estações de trabalho Windows:

13.1.3.1 - Possuir a capacidade de atualizar remotamente e em tempo real, as listas de definições de malware, sem a necessidade de utilização de login-scripts, agendamentos ou intervenções do usuário;

13.1.3.2 - Possuir capacidade de programação de atualizações das listas de definições de malware, a partir de local predefinido da rede ou site da Internet;
13.1.3.3 - Possuir capacidade de atualização das listas de definições de malware por meio de um servidor proxy, fornecido pelo fabricante da solução, para redução do consumo de banda em sites remotos;
13.1.3.4 - Possuir atualização incremental das assinaturas nas estações de trabalho;
13.1.3.5 - Possuir solução de reputação WEB, integrada e gerenciada através da solução de antivírus, cancelando conexões prejudiciais de forma automática, com base na resposta à consulta da base do fabricante;
13.1.3.6 - Possuir recurso de proteção contra exploits inseridos em páginas e scripts WEB.
13.1.3.7 - Possuir solução de reputação de arquivos, integrada e gerenciada através da solução de antivírus, cancelando a execução do arquivo, de forma automática, com base na resposta à consulta da base do fabricante;
13.1.3.8 - O sistema de antivírus ofertado deve possuir a possibilidade de programar no mínimo duas ações automáticas (primária e secundária), para o caso de detecção de malware, com as seguintes opções:
13.1.3.8.1 - Somente alertar;
13.1.3.8.2 - Limpar automaticamente;
13.1.3.8.3 - Apagar automaticamente;
13.1.3.8.4 - Colocar em quarentena (isolar).
13.1.3.9 - Possibilitar a tomada de ações independentes para casos de detecção de malware;
13.1.3.10 - Relatar para o console de gerenciamento todos os tipos de programas potencialmente perigosos (ex: spyware) para que sua utilização possa ser definida (liberada ou bloqueada) pelo administrador;
13.1.3.11 - Possuir controle de aplicativos que acessam a rede, reportando todos eles para o console de gerenciamento, de forma que o administrador possa controlar sua utilização pelos usuários (liberar ou bloquear a abertura e o recebimento de conexões);
13.1.3.12 - Possibilitar acionamento de função de verificação do sistema de forma manual, pré-agendada ou em tempo real contra vírus, worms, cavalos de troia e demais tipos de códigos maliciosos;
13.1.3.13 - Possuir proteção em tempo real contra vírus, worms, cavalos de troia, spywares, adwares, e demais tipos de códigos maliciosos, integrada em uma única solução independente de plugin ou módulo adicional;
13.1.3.14 - Possuir proteção contra rootkits;
13.1.3.15 - Detectar e remover cookies potencialmente indesejáveis no sistema (ex: cookies de rastreamento);
13.1.3.16 - Permitir a verificação em tempo real e a verificação manual de todos os tipos de arquivos, bem como a definição dos tipos de arquivos a serem verificados contra malware;
13.1.3.17 - Permitir a criação de listas de exclusões de objetos da varredura (diretórios, arquivos e extensões de arquivos);
13.1.3.18 - Realizar verificação e proteção do sistema de registro (registry) contra modificações não autorizadas;
13.1.3.19 - Reconhecer e impedir, através de análise heurística, a ação de software malicioso ao tentar executar funções que possam causar dano ao sistema, tais como alterar o registro do sistema operacional e associações críticas a arquivos, com capacidade de finalizar processos perigosos que possam causar instabilidade ou risco ao sistema;
13.1.3.20 - Possuir rastreamento manual, disparado pelo usuário, com interface gráfica e opções de seleção de arquivos, diretórios ou discos a serem analisados, ou de varredura completa da estação, inclusive com verificação de rootkits;

13.1.3.21 - Detectar novos tipos de ameaças, ainda desconhecidas, como spyware, adware, jokes, dialers, remote access, trackware e ferramentas de hack através de análise heurística de comportamento;
13.1.3.22 - Possuir sistema de proteção proativo que realize análise na nuvem (in-the-cloud) através da Internet, utilizando base de dados mundial de reputação de aplicações disponibilizada pelo fabricante;
13.1.3.23 - Permitir o envio de amostras de arquivos suspeitos para análise do fabricante;
13.1.3.24 - Fazer a análise de malware dentro de mensagens de correio eletrônico que utilizam os protocolos POP, IMAP e SMTP, através do antivírus da estação de trabalho;
13.1.3.25 - Possuir IDS (intrusion detection system), integrado com firewall pessoal e gerenciado pelo mesmo console do mesmo fabricante da solução de antivírus, com atualização automática;
13.1.3.26 - Permitir a definição de novos serviços baseados nos protocolos e portas utilizados;
13.1.3.27 - Permitir a definição de regras para permissão/negação de acesso baseadas nos serviços, origem e destino das conexões;
13.1.3.28 Possibilitar a definição de múltiplas políticas, utilizando as regras definidas;
13.1.3.29 Possibilitar a aplicação de diferentes políticas para grupos de estações ou estações específicas;
13.1.3.30 - Possibilitar a aplicação automática de diferentes políticas de firewall nas estações de trabalho e notebooks, através de regras definidas pelo administrador (ex: notebooks em uso na rede local e em uso remoto);
13.1.3.31 - Viabilizar o controle de aplicativos nas estações de trabalho, listando os softwares confiáveis que trafegam pela rede, desta forma bloqueando o tráfego desnecessário gerado por softwares não autorizados;
13.1.3.32 - Deve possuir a capacidade de detectar a origem de ameaças na rede, fornecendo informações como endereço IP e nome DNS / NetBios;
13.1.3.33 - Realizar o rastreamento em tempo real, para arquivos criados, copiados, renomeados, movidos ou modificados;
13.1.3.34 - Possibilitar acionamento de função de verificação de ocorrência de malware de forma manual, pré-agendada ou em tempo real;
13.1.3.35 - Realizar a verificação de malware em arquivos compactados em pelo menos 05 (cinco) níveis de profundidade;
13.1.3.36 - Possuir, no mínimo, 02 (dois) mecanismos (engines) anti-malware trabalhando simultaneamente e gerenciados através do mesmo console de gerenciamento;
13.1.3.37 - Gerar registro (log) dos eventos de detecção de malware em arquivo em local definido pelo usuário;
13.1.3.38 - Possuir geração e exibição de alertas em caso de detecção de malware, através de mensagem na tela, no console de administração e no sistema de registro de eventos da estação, via SNMP e e-mail SMTP;
13.1.3.39 - Possuir interface do usuário no idioma Português (Brasil) ou Inglês;
13.1.3.40 - Ser capaz de detectar malwares durante a navegação web de forma independente do navegador web, interceptando e verificando o tráfego do protocolo HTTP;
13.1.3.41 - Impedir a execução de componentes ActiveX;
13.1.3.42 - Agregar proteção integrada aos browsers Internet Explorer e Mozilla Firefox contra sites maliciosos, com sistema de reputação. A proteção deve conectar-se à nuvem onde deverá haver lista atualizada de websites maliciosos;
13.1.3.43 - Classificar resultados de pesquisas em sites de busca como Google, Yahoo, etc., de acordo com a reputação do site, indicando para o usuário a classificação de cada resultado através de informações na tela;

13.1.3.44 - Bloquear sites (páginas) que contenham vulnerabilidades detectadas pelo módulo de proteção a navegação;
13.1.3.45 - Mostrar a classificação de links em serviços de e-mail via web (web-mails);
13.1.3.46 - Permitir ao administrador liberar o acesso a páginas bloqueadas automaticamente pela solução, caso entenda que as mesmas não oferecem risco aos usuários;
13.1.3.47 - Permitir a atualização de um determinado segmento de rede através de estações de trabalho eleitas para serem os repositórios deste segmento, sem a necessidade de instalação de um módulo adicional nas estações ou servidores para realizar esta tarefa;
13.1.3.48 - Permitir a definição de um adaptador de rede confiável, onde o tráfego de e/ou para este adaptador não será bloqueado pelo firewall;
13.1.3.49 - Possuir módulo de controle de aplicativos, bloqueando-os mesmo se os seus nomes forem alterados pelo usuário, e viabilizando seu gerenciamento através do mesmo console de gerenciamento dos módulos antivírus, anti-spyware, firewall e IDS/IPS;
13.1.3.50 - Possuir controle de todos os aplicativos que acessam recursos de rede em cada uma das estações de trabalho, informando a sua existência ao console de administração e permitindo ao administrador definir quais destes aplicativos podem ou não ser executados. Permitir ao administrador definir mensagens a serem apresentadas para os usuários nos casos de bloqueio de aplicações;
13.1.3.51 - Permitir habilitar/desabilitar dispositivos de hardware externo (USB) por tipo específico, classe e subclasse de dispositivo nas estações de trabalho.

13.1.4 - Solução para servidores e estações de trabalho GNU/Linux:

13.1.4.1 - O sistema de antivírus, anti-spyware, anti-rootkit e firewall integrado para servidores de arquivos Linux deve ser fornecido em um único pacote de instalação para ambientes de servidores e de estações de trabalho para S.O local e em máquina virtual;
13.1.4.2 - Deverá possibilitar varredura em tempo real para arquivos durante a sua leitura e escrita, com, no mínimo, as seguintes opções:
13.1.4.2.1 - Renomear o arquivo infectado;
13.1.4.2.2 - Desinfetar o arquivo infectado;
13.1.4.2.3 - Apagar o arquivo infectado;
13.1.4.2.4 - Colocar o arquivo infectado em quarentena.
13.1.4.3 - Rastreamento manual através da interface gráfica e de linha de comando (CLI) local, personalizável;
13.1.4.4 - Rastreamento em tempo real dos processos em memória;
13.1.4.5 - Possuir capacidade de programação de atualizações das listas de definições de malware, a partir de local predefinido da rede ou site da Internet;
13.1.4.6 - Possuir atualização incremental das assinaturas nas estações de trabalho;
13.1.4.7 - Salvar automaticamente as listas de definições de malware no repositório central da rede;
13.1.4.8 - Programação de rastreamento automático do sistema:
13.1.4.8.1 - Ação: Somente alertar, limpar automaticamente, apagar automaticamente ou renomear automaticamente;
13.1.4.8.2 - Frequência: Horária, diária, semanal, mensal;
13.1.4.8.3 - Exclusões: Pastas ou arquivos que não devem ser rastreados.
13.1.4.9 - Gerar registro (log) dos eventos de detecção de malware em arquivo;
13.1.4.10 - Gerar notificações de eventos de malware através de alerta na rede;
13.1.4.11 - Capacidade de finalizar processos perigosos que possam causar instabilidade ou risco ao sistema através de análise heurística;
13.1.4.12 - Possuir ferramenta de segurança que assine e verifique a integridade dos

módulos do kernel, possibilitando alteração mediante autorização do administrador;
13.1.4.13 - Rastreamento em tempo real de discos contra spyware, com pelo menos as seguintes opções:

13.1.4.13.1 - Apagar o spyware;

13.1.4.13.2 - Mover o spyware para a quarentena.

13.1.4.14 Detecção de cookies potencialmente indesejáveis no sistema (ex: cookies de rastreamento);
13.1.4.15 - Rastreamento em tempo real dos processos em memória contra spywares;
13.1.4.16 - Programação de rastreamento manual do sistema:

13.1.4.16.1 - Escopo: Todos os drives locais, drives específicos, ou pastas específicas;

13.1.4.16.2 - Ação: Somente alertar, limpar automaticamente, apagar automaticamente;

13.1.4.16.3 - Exclusões: Pastas ou arquivos que não devem ser rastreados.

13.1.4.17 - Atualização incremental da lista de ameaças;
13.1.4.18 - Operar tanto no ambiente corporativo como em ambiente de VPN;
13.1.4.19 - Possuir gerenciamento centralizado, permitindo a configuração de recursos antivírus e anti-spyware através da mesma interface de gerenciamento utilizada para as soluções Windows;
13.1.4.20 - Possuir IDS (intrusion detection system), integrado com firewall pessoal e gerenciado pelo mesmo console da solução de antivírus;
13.1.4.21 - Permitir a utilização de interface de linha de comando (CLI) para as ações de proteção;
13.1.4.22 - Possuir capacidade de criar baseline de assinatura para arquivos de sistema (kernel, etc.) impedindo a modificação e a atualização indevidas do sistema operacional. As modificações e atualizações do sistema devem ser permitidas pelo administrador através do console de gerenciamento.

13.1.5 - Módulo para gerenciamento da solução antivírus – gerência centralizada de todos os módulos da suíte:

13.1.5.1 - Deve permitir a instalação do servidor de gerenciamento em todas as plataformas indicadas na seção inicial deste Termo;
13.1.5.2 - Deve permitir a instalação do console de gerenciamento em todas as plataformas indicadas na seção inicial deste Termo;
13.1.5.3 - Deve administrar toda a solução ofertada no S.O local e em máquina virtual, inclusive estações de trabalho e servidores Linux;
13.1.5.4 - Deve possuir interface única para configuração de políticas para antivírus, anti-spyware, firewall e IDS;
13.1.5.5 - Utilizar chave de criptografia para garantir segurança de comunicação entre o servidor de gerenciamento, o console de gerenciamento e as estações de trabalho. Toda a troca de informação entre qualquer dos componentes da solução deve ser assinada digitalmente para garantir a origem da informação;
13.1.5.6 - Executar a comunicação com estações de trabalho, servidores e servidor de gerenciamento através do protocolo HTTP, em portas definidas pelo administrador;
13.1.5.7 - Permitir a criação de grupos de estações, definidos pelo administrador;
13.1.5.8 - Permitir o gerenciamento dos produtos antivírus como uma árvore de diretórios, personalizada pelo administrador;
13.1.5.9 - Exibir a lista de servidores e estações que possuam o antivírus instalado, contendo informações como nome da estação, versão do antivírus, data das definições de malware, data da última verificação e status (infectada por malware, desatualizada etc.);
13.1.5.10 - Permitir a visualização das características das estações como: nome de

rede, IP e sistema operacional;
13.1.5.11 - Bloquear o acesso às configurações e remoção do software antivírus pelo usuário final, através de políticas definidas pelo administrador;
13.1.5.12 - Aplicar mudanças nas configurações do antivírus, para todos os computadores, por grupo de computadores ou individualmente por computador;
13.1.5.13 - Forçar a configuração determinada no servidor para as estações clientes;
13.1.5.14 - Permitir a instalação e atualização do software sem a intervenção do usuário;
13.1.5.15 - Possibilitar a identificação de estações de trabalho que ainda não possuem o software de proteção ativo;
13.1.5.16 - Possibilitar a programação e execução de rastreamento remoto contra malware, com a opção de selecionar uma estação ou um grupo de estações para rastreamento;
13.1.5.17 - Realizar o gerenciamento centralizado da área de quarentena;
13.1.5.18 - Emitir relatórios sobre o status de toda a solução instalada;
13.1.5.19 - Gerar relatórios gráficos através de interface WEB;
13.1.5.20 - Permitir a exportação dos relatórios para, pelo menos, um dos formatos a seguir: HTML, XML e CSV;
13.1.5.21 - O sistema de antivírus ofertado deve permitir a geração de relatórios que contenham as seguintes informações:
13.1.5.21.1 - Lista de estações com as definições de malware desatualizadas;
13.1.5.21.2 - Versão do software de antivírus instalado em cada estação;
13.1.5.21.3 - Lista de malwares com maior número de detecções;
13.1.5.21.4 - Lista de estações que mais sofreram infecções, em determinado período de tempo;
13.1.5.21.5 - Estado da comunicação entre as estações clientes e o servidor de gerência;
13.1.5.21.6 - Distribuição das listas de definições e mecanismo de varredura nas estações clientes;
13.1.5.21.7 - Sumário dos produtos antivírus instalados;
13.1.5.21.8 - Versão do software de gerenciamento instalado;
13.1.5.21.9 - Ações tomadas pelo software antivírus;
13.1.5.21.10 - Histórico das infecções;
13.1.5.21.11 - Número de arquivos infectados detectados;
13.1.5.21.12 - Contagem de infecções por tipo de malware e período;
13.1.5.21.13 - Ranking das estações que mais sofreram ataque.
13.1.5.22 - Permitir o armazenamento das informações coletadas nas estações clientes em um banco de dados centralizado, sem a necessidade de aquisição de solução de banco de dados de terceiros, devendo este ser fornecido de forma integrada à solução antivírus, ofertada sem qualquer custo adicional;
13.1.5.23 - Suportar o gerenciamento de pelo menos 5.000 (cinco mil) estações a partir de um único servidor;
13.1.5.24 - Permitir o acesso ao servidor de gerenciamento a partir de console instalado em outra estação;
13.1.5.25 - Permitir a instalação do antivírus nas estações clientes a partir de um único servidor, sem a necessidade de instalação prévia de um agente ou módulo;
13.1.5.26 - Permitir a alteração das configurações e políticas do antivírus nas estações clientes, de maneira remota;
13.1.5.27 - Permitir a execução de tarefas remotas de atualização, verificação de malware e upgrades, através do console de gerenciamento;
13.1.5.28 - Possibilitar a criação de grupos de estações baseadas em regras definidas pelo administrador;
13.1.5.29 - Forçar que as estações clientes recebam a configuração determinada através do servidor;
13.1.5.30 - Forçar a instalação do software antivírus nas estações clientes;

13.1.5.31 - Gerenciar a atualização do antivírus em computadores portáteis (notebooks), automaticamente, mediante conexão em rede local ou dial-up;
13.1.5.32 - Possuir a capacidade de gerar registros/logs para auditoria;
13.1.5.33 - Atualizar e implementar políticas de segurança proativas para toda a solução;
13.1.5.34 - Permitir a utilização de repositórios remotos para atualização, sem limite de instalação;
13.1.5.35 - Possibilitar o cadastro de vários administradores com permissão para acesso e configuração simultâneos;
13.1.5.36 - Permitir a importação da estrutura do Active Directory da Microsoft, de forma automática;
13.1.5.37 - Realizar a importação automática de novas estações com a instalação do produto baseado em regras, colocando-as no segmento da árvore de políticas definida pelo administrador;
13.1.5.38 - Remover automaticamente da árvore de políticas as estações que não estiverem mais presentes na rede
13.1.5.38.1 - Bloquear automaticamente máquina na rede se não for atualizada por pelo menos 4 dias;
13.1.5.39 - Todas as configurações dos softwares de antivírus deverão ser efetuadas no software de gerenciamento, e a sua aplicação nas estações deverá ser feita de forma automática, sem a necessidade de intervenção do usuário;
13.1.5.40 - Serviços de Instalação, Configuração e Treinamento Hands-On deverão ser executados localmente na sede da DESO, na rua Campo do Brito, 331, Praia 13 de Julho, Centro, Aracaju/SE com duração mínima de 24 horas.

CLÁUSULA XIV – DOS CASOS FORTUITOS E FORÇA MAIOR

14.1 – Os casos fortuitos e de força maior, conforme disposto no Artigo nº 393 e seu Parágrafo Único, do Código Civil, eximem as partes de responsabilidade pelo não cumprimento das obrigações assumidas no presente Contrato.

CLÁUSULA XV – DAS DESPESAS DE CONTRATO

15.1 – Todas as despesas para elaboração, validade e eficácia jurídica do Contrato, correrão por conta exclusiva da DESO.

CLÁUSULA XVI – DOS ELEMENTOS INTEGRANTES

16.1 – Integram este Contrato:

- Pregão Eletrônico nº 103/2018 – 01/11/2018;
- Documentação da Contratada (Certidões);
- Homologação do Presidente de 03/12/2018;
- Publicação.

CLÁUSULA XVII – DA RESCISÃO

17.1 – O Contrato poderá ser rescindido a qualquer tempo, na ocorrência de quaisquer das hipóteses previstas nos arts. 181 a 183 do RILC e pelo descumprimento das obrigações da contratada, conforme edital e termo de referência.

CLÁUSULA XVIII – DO FORO

18.1 – Fica eleito o Foro da cidade de Aracaju, capital do Estado de Sergipe, para dirimir quaisquer questões decorrentes deste Contrato, com renúncia a qualquer outro, por mais

especial que o seja.

18.2 – E assim, por estarem justos e contratados, assinam o presente em 02 (duas) vias de igual teor e para um só fim legal.

Aracaju/SE, 12 de dezembro de 2018.

"LUCIANA SANTOS DA SILVA"
VTECH COM. SERV. E EQUIP. DE INFORMÁTICA EIRELI

"JETHRO DUARTE MOREIRA"
PRESIDENTE – DESO

"VINÍCIUS ARAGÃO SANTIAGO COSTA"
ADVOGADO/ASLC – DESO

Emerson Dantas de Menezes
Advogado DESO / AJU
OAB/SE n.º 3172

"HAROLDO ANDERSON DÉDA FILHO"
DIRETOR DE GESTÃO CORPORATIVA