EDITAL COTAÇÃO ELETRÔNICA CDSA N° 002/2021-CPL/CDSA.

PROCESSOS N° 042/2021

A Companhia Docas de Santana (CDSA), por intermédio deste Pregoeiro, designado pela Portaria nº 33/2019-CDSA, torna público, para conhecimento dos interessados, que na data e horário abaixo indicados, fará COTAÇÃO, NA FORMA ELETRÔNICA, tendo como critério de julgamento o MENOR PREÇO, que será regido pelo regulamento de licitação da CDSA, disponível no site da Companhia Docas de Santana, www.docasdesanatana.com.br, Lei Complementar nº 123/06, Lei nº 13.303/2016 e, subsidiariamente, pela Lei nº 8.666/93 e suas alterações posteriores, para suprir as necessidades da Companhia Docas de Santana (CDSA), mediante as condições estabelecidas neste edital e seus anexos.

Início do Acolhimento das Propostas:	10/06/2021 às 12h (Horário de Brasília)
Abertura das Propostas: (SEM DISPUTA)	18/06/2021 às 09h (Horário de Brasília)
N° da Licitação no Licitações-e:	**877410**

Não havendo expediente na data marcada, a licitação ficará adiada para o primeiro dia útil subsequente, mantidos o mesmo horário, salvo disposições em contrário.

I. DO OBJETO

O objeto da presente licitação é a escolha da proposta mais vantajosa para a Aquisição de licença de software de proteção antivírus, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos:

Lote 1: Aquisição de antivírus (Anexo I, Termo de Referência 1);

1.1 Em caso de divergência entre as especificações do objeto descritas no site www.licitacoes-e.com.br do Banco do Brasil S/A e as especificações técnicas constantes nos Termos de Referência (Anexo I), prevalecerá sempre a descrição deste edital.

1.2 Cópia do Edital e seus anexos poderão ser obtidos somente no endereço eletrônico: www.licitacoes-e.com.br.

1.3 FAZEM PARTE INTEGRANTE DESTE EDITAL OS SEGUINTES ANEXOS:

ANEXO I – Termos de Referência 1 respectivos anexos;

ANEXO II – Modelos de Proposta Comercial 1

ANEXO III – Modelo de Declaração ME/EPP;

ANEXO IV – Modelo de Declaração de Requisitos Constitucionais;

ANEXO V – Modelo de Declaração de Inexistência de Fato Impeditivo;

II. DA REFERÊNCIA DE TEMPO

2.1. Todas as referências de tempo no Edital, no Aviso e durante a Sessão Pública observarão, obrigatoriamente, o horário de Brasília-DF e, dessa forma, serão registradas no Sistema Eletrônico e na documentação relativa ao certame.

2.2. Os interessados deverão observar rigorosamente as datas e os horários limites para o recebimento e abertura das propostas.

2.3. Ocorrendo decretação de feriado, ponto facultativo ou qualquer outro fato superveniente que impeça a realização da licitação na data pré-estabelecida, será reiniciada no primeiro dia útil seguinte, com a informação aos participantes no local "Mensagens" do sistema eletrônico do licitações-e.

III. DA PARTICIPAÇÃO

3.1 A presente Aquisição, em observância ao disposto no Decreto nº 8.538/2015 e na Lei Complementar nº 123/2006, destina-se, a participação de interessadas que atendam todas as exigências deste Edital e cuja atividade empresarial abranja o objeto desta aquisição e estejam credenciados no sistema "LICITACOES-E", provido pelo Banco do Brasil S/A, constante da página eletrônica www.licitacoes-e.com.br.

3.2 Não poderão participar desta licitação:

3.3.1. Empresa suspensa de participar de licitação e impedida de contratar com a COMPANHIA DOCAS DE SANTANA, durante o prazo da sanção aplicada;

3.3.2. Empresa declarada inidônea para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou ate que seja promovida sua reabilitação;

3.3.3. Empresa impedida de licitar e contratar com a PREFEITURA MUNICIPAL DE SANTANA, durante o prazo da sanção aplicada;

3.3.4. Empresa que se encontre em processo de dissolução, recuperação judicial, recuperação extrajudicial, falência, concordata, fusão, cisão ou incorporação;

3.3.5. Empresa que esteja com o direito de licitar e contratar com a Administração suspenso ou que tenha sido declarada inidônea por órgão da Administração Pública, Direta ou Indireta, Federal, Estadual, Municipal ou do Distrito Federal.

IV. DA DOTAÇÃO ORÇAMENTÁRIA E DO VALOR

4.1 As despesas decorrentes da presente licitação correrão às rubricas abaixo descritas previstas no Orçamento 2021 da COMPANHIA DOCAS DE SANTANA.

a. Lote 1: 02.03.14 – Aquisição de licença de Software de base;

4.2 Os valores estimados para a contratação estão previstos no Painel de Preços do Governo Federal.

V. DA APRESENTAÇÃO DA PROPOSTA

5.1. O licitante deverá encaminhar a proposta por meio do sistema eletrônico www.licitacoes-e.com.br, até a data e horários marcados para abertura das propostas, quando então, encerrar-se-á automaticamente a fase de recebimento de propostas e, posteriormente, enviar a proposta detalhada conforme modelo em anexo via email: cpl@docasdesantana.com.br.

5.2. O encaminhamento da proposta de preços pressupõe o pleno conhecimento e atendimento às exigências de habilitação previstas neste Edital e seus anexos. O licitante será responsável por todas as

transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras as propostas e lances.

5.3. O licitante deverá, na forma expressa no sistema eletrônico, encaminhar preços propostos indicando o MENOR PREÇO, computando todos os custos necessários à aquisição dos objetos da presente licitação, bem como todos os impostos, fretes, seguros, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, e quaisquer outras despesas que incidam ou venham a incidir sobre o objeto desta licitação.

5.4. As propostas cujos valores sejam exorbitantes ao previsto no item 4.2 (pesquisa de preço) deste Edital, estarão sujeitas à desclassificação.

5.5. As propostas terão validade mínima de 60 (sessenta) dias, contados da data de abertura da sessão pública.

5.6. Antes da abertura das propostas especificadas neste edital, o licitante poderá retirar ou substituir a proposta anteriormente encaminhada.

5.7. A declaração falsa relativa ao cumprimento dos requisitos de habilitação e proposta sujeitará o licitante às sanções previstas neste Edital.

5.8. Serão desclassificadas as propostas que não atendam às exigências do presente Edital e seus Anexos, sejam omissas ou apresentem irregularidades ou defeitos capazes de dificultar o julgamento.

5.9. Havendo recusa na aceitação, o pregoeiro poderá convocar o licitante cuja proposta ou lance esteja classificado em segundo lugar, verificando a sua aceitabilidade e procedendo a sua habilitação e assim, sucessivamente, na ordem de classificação, até que uma das propostas preencha os requisitos para aceitação dispostos no Edital.

VI. DO CRITÉRIO DE JULGAMENTO DAS PROPOSTAS

6.1 O julgamento das propostas obedecerá ao critério do MENOR PREÇO.

6.2 O pregoeiro efetuará o julgamento das Propostas, decidindo sobre a aceitação dos preços obtidos.

6.3 O Pregoeiro verificará as propostas apresentadas e desclassificará, motivadamente, aquelas que não estejam em conformidade com os requisitos exigidos e estabelecidos no instrumento convocatório (Edital).

VII. DA NEGOCIAÇÃO

7.1 O Pregoeiro poderá encaminhar a contraproposta diretamente ao licitante que tenha apresentado a proposta mais vantajosa, observado o critério de julgamento para a contratação, não se admitindo negociar condições diferentes daquelas previstas neste Edital.

VIII. DA HABILITAÇÃO

8.1 O licitante classificado provisoriamente em primeiro lugar deverá encaminhar no prazo de até 01 (um) dia após a abertura de proposta no sistema, para envio da proposta ou email cpl@docasdesantana.com.br, a proposta de preço.

8.2 A habilitação dar-se-á:

a) Habilitação jurídica (quando houver necessidade de assinatura de contrato);

b) Regularidade fiscal e trabalhista;

c) Declarações.

8.2.1 Relativos à Habilitação Jurídica:

a) Cédula de identidade do representante legal da empresa;

b) Registro comercial, no caso de empresa individual;

c) Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, para as sociedades comerciais e, no caso de sociedades por ações, acompanhado dos documentos comprobatórios de eleição de seus administradores.

8.2.2 Relativos à Regularidade Fiscal e Trabalhista:

a) Prova de inscrição no Cadastro Nacional de Pessoa Jurídica (CNPJ);

b) Prova de regularidade perante a Fazenda Federal, mediante apresentação de Certidão Conjunta de Débitos Relativos a Tributos Federais e a Dívida Ativa da União, fornecida pela Secretaria da Receita Federal ou pela Procuradoria-Geral da Fazenda Nacional;

c) Prova de regularidade para com a Fazenda Estadual do domicílio ou sede do licitante, ou outra equivalente, na forma da lei;

d) Prova de regularidade para com a Fazenda Municipal do domicílio ou sede do licitante, ou outra equivalente, na forma da lei;

e) Prova de regularidade relativa ao Fundo de Garantia por Tempo de Serviço (FGTS), emitida pela Caixa Econômica Federal;

f) Certidão Negativa de Débitos Trabalhistas (CNDT), conforme o Titulo VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto Lei nº 5.452/43 e Lei nº 12.440/2011.

9. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

9.1 O objeto desta licitação será adjudicado pelo MENOR PREÇO o licitante vencedor. Após a adjudicação, sendo constatada a regularidade dos atos procedimentais, a autoridade competente homologará a licitação e formalizará a contratação por intermédio de Nota de Empenho e Contrato.

IX. DO CONTRATO

10.1 A Companhia Docas de Santana firmará Contrato com o Licitante Vencedor, conforme consoante as minutas que constituem o Anexo VII desta licitação, quando necessário.

X. DA FISCALIZAÇÃO E ACOMPANHAMENTO DOS SERVIÇOS

11.1 O fornecimento será acompanhado e fiscalizado por empregado da COMPANHIA DOCAS DE SANTANA (CDSA) designado através de Portaria, na condição de representante da Contratante.

11.2 A existência da fiscalização de nenhum modo diminui ou altera a responsabilidade da contratada na prestação dos serviços a serem executados.

XI. DA FORMA DE PAGAMENTO

12.1 O pagamento será efetuado mensalmente, conforme a necessidade, pela Companhia Docas de Santana (CDSA), em Real (R$), até 30 (trinta) dias após a apresentação da Nota Fiscal eletrônica devidamente atestada pelo fiscal do Contrato, acompanhada da Nota de Empenho e Ordem de Fornecimento, por meio de ordem de pagamento emitida em nome do proponente vencedor, para crédito na conta corrente da pessoa jurídica por ele indicada, uma vez satisfeitas as condições estabelecidas neste Edital e seus anexos.

12.2 Será considerada, para fins de pagamento, a data do "atesto" certificando o recebimento definitivo do material por esta Companhia Docas de Santana (CDSA).

XII. DAS SANÇÕES ADMINISTRATIVAS

13.1 Sanções relativas à licitação:

13.1.1 A licitante que, convocada dentro do prazo de validade de sua proposta, não assinar o Contrato, deixar de entregar documentação exigida no Edital, apresentar documentação falsa, não mantiver a proposta, comportar-se de modo inidôneo, fizer declaração falsa ou cometer fraude fiscal, ficara impedida de licitar e de contratar com a União, Estados, Distrito Federal ou Municípios, pelo prazo de ate 05 (cinco) anos, garantido o direito a ampla defesa;

13.2 Além da penalidade prevista acima, a licitante ficará sujeita a multas na fase de licitação, sobre o valor estimado do objeto, por infração, a ser recolhida no prazo de 10 (dez) dias após notificação, nos seguintes termos:

a) Multa moratória de 10% (dez por cento) por cada uma das infrações a seguir: aquele que se comportar de modo inidôneo; deixar de entregar a documentação exigida no Edital; não assinar o Contrato ou deixar de retirar o instrumento equivalente; não mantiver a proposta; e atrasos injustificados na execução do Contrato;

b) Multa compensatória de 15% (quinze por cento) por cada uma das infrações a seguir: aquele que fizer declaração falsa; apresentar documentação falsa; ou cometer fraude fiscal.

XIII. DA VIGÊNCIA

14.1 O software terá validade de 36 (trinta e seis) meses (direito de atualização), a partir da data de sua assinatura ou instalação do software, podendo ser prorrogado por mais 24 meses.

XIV. DAS OBRIGAÇÕES DA CONTRATADA

15.1 A CONTRATADA deverá atender às normas do Código de Defesa do Consumidor.

15.2 A CONTRATADA deverá possuir representação local ou, na impossibilidade de tal evento, disponibilizar um agente executivo que atenda exclusivamente às demandas formuladas pelo órgão contratante in loco.

15.3 Deverá emitir e encaminhar à CONTRATANTE a fatura mensal, computada nesse documento a totalização das operações registradas no mês da ocorrência.

15.4 O pagamento será efetuado pela CONTRATANTE mediante a entrega da nota fiscal eletrônica pela CONTRATANTE,.

15.5 A CONTRATADA deverá atender as obrigações constantes no subitens dos Termos de Referência (Anexo I) deste edital.

XV. DAS OBRIGAÇÕES DA CONTRATANTE

16.1 A CONTRATANTE deverá atender as obrigações constantes no itens e subitens dos Termos de Referência (Anexo I) deste edital:

XVI. DAS DISPOSIÇÕES FINAIS

17.1 O julgamento das propostas será com base no MENOR PREÇO, estando computados neste os itens como tributos, seguros, encargos e demais despesas.

17.2 As normas que disciplinam esta licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, atendidos os interesses públicos e o da Administração, sem comprometimento da segurança da contratação.

17.3 As decisões do Pregoeiro somente serão consideradas definitivas depois de homologadas pela Companhia Docas de Santana (CDSA).

17.4 Nenhuma indenização será devida aos licitantes pela elaboração de proposta ou pela apresentação de documentação referente ao presente Edital.

17.5 O Ordenador de Despesas da COMPANHIA DOCAS DE SANTANA (CDSA) poderá revogar o presente certame por considerá-lo inoportuno ou inconveniente, decorrente de fato superveniente, mediante ato escrito e fundamentado, pertinente e suficiente para justificar tal conduta, devendo anulá-lo por ilegalidade, de oficio ou mediante provocação de terceiros, nos termos do art. 49 da Lei nº 8.666/93 e alterações.

17.6 A anulação da licitação induz a anulação também do Contrato e da Nota de Empenho.

17.7 Os licitantes não terão direito a indenização em decorrência da anulação do procedimento licitatório, ressalvado o direito do contratado de boa-fé de ser ressarcido pelos encargos que tiver suportado no cumprimento do Contrato.

17.8 No caso de alteração deste Edital no curso do prazo estabelecido para a realização da licitação, este prazo será reaberto, exceto quando, inquestionavelmente, a alteração não afetar a formulação das propostas.

17.9 Aos casos omissos neste edital, aplicar-se-ão as demais disposições das legislações constantes do preâmbulo deste Edital.

17.10 A CDSA poderá, ainda, prorrogar, a qualquer tempo, os prazos para recebimento das propostas.

17.11 Quaisquer informações a respeito deste pedido de cotação poderão ser obtidas diretamente na

Companhia Docas de Santana (CDSA), sito à Rua Cláudio Lúcio Monteiro, nº 1380, Bairro Novo Horizonte, Santana-AP, através do telefone n° (96) 99129-9510 no horário de 08:00 às 14:00 hs (hora de Brasília) ou, ainda, no e-mail: cpl@docasdesantana.com.

XVII. DO FORO

18.1 Fica eleito, de comum acordo entre as partes, o Foro da Comarca de Santana-AP, para dirimir quaisquer litígios oriundos da licitação e do Contrato decorrente, com expressa renúncia a outro qualquer, por mais privilegiado que seja.

Santana-AP, 10 de junho de 2021.

Uélliton Nogueira da Silva
Presidente da CPL
Portaria nº 32/2019/CDSA

Edival Cabral Tork
Presidente da CDSA
Decreto nº 026/2021/PMS

ANEXO I

TERMO DE REFERÊNCIA 1

APROVO o competente Termo de Referencia e autorizo a abertura de Procedimento Licitatório nos termos da Lei nº 10.520/2002.

Em ____ /_____/_____

EDIVAL TORK
-Diretor Presidente da CDSA-

1. **DO OBJETO**

Contratação de licença de uso para solução corporativa de software de proteção para anti-malware (antivírus), com gerência centralizada e com direito de atualização por 36 (trinta e seis) meses, conforme especificação e condições constantes neste termo de referência.

2. **JUSTIFICATIVA**

Solicitamos aquisição de licenças de antivírus para prevenir contaminação por vírus, malwares e suas variantes nos computadores na instituição pondo em risco o sigilo, a integridade e a disponibilidade das informações. Estas aquisições proporcionarão maior proteção evitando possíveis transtornos e é, portanto, uma questão de segurança, possibilitando um maior desempenho das estações de trabalho e, por conseguinte, disponibilizar aos funcionários uma melhor condição para a realização de suas atividades. Contudo esta aquisição é necessária para manter os altos níveis de proteção frente ao surgimento frequente de novas ameaças. O presente termo de referência tem o propósito de, tão somente, preservar as condições atuais de manutenção da solução de antivírus da CDSA.

3. **DA QUANTIDADE**

40 (quarenta) licenças de uso de solução de antivírus para atender todo o parque computacional da CDSA

4. **COMPATIBILIDADE**

4.1. Microsoft Windows XP Professional SP3 ou superior;
4.2. Microsoft Windows 7 Starter/ Home Basic/Home Premium/Professional/Enterprise e Ultimate;
4.3. .Microsoft Windows 10 Professional
4.4. Microsoft Windows Server 2008 x64 e R2
4.5. Microsoft Windows Server 2012;
4.6. Microsoft Windows Server 2019;

5. **CARACTERÍSTICAS GERAIS:**

5.1. A console deve ser acessada via WEB (HTTPS) ou MMC;
5.2. Console deve ser baseada no modelo cliente/servidor;
5.3. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;
5.4. Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, patch management e MDM;
5.5. As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma, o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;
5.6. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;
5.7. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows,

através de compartilhamento administrativo, login script e/ou GPO de Active Directory;

5.8. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;

5.9. A solução de gerência deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;

5.10. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;

5.11. Deve integrar com Active Directory e ler acessos específicos de usuários por permissões em grupos de gerenciamento;

5.12. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;

5.13. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário;

5.14. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux) protegidos pela solução antivírus;

5.15. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;

5.16. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;

5.17. Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;

5.18. A comunicação entre o cliente e o servidor de administração deve ser criptografada;

5.19. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;

5.20. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

5.20.1. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas (varredura);

5.20.2. Nome do computador;

5.20.3. Nome do domínio;

5.20.4. Range de IP;

5.20.5. Sistema Operacional;

5.20.6. Máquina virtual.

5.20.7. Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional;

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

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

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

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

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

5.21. Deve fornecer as seguintes informações dos computadores:

5.21.1. Se o antivírus está instalado;

5.21.2. Se o antivírus está iniciado;

5.21.3. Se o antivírus está atualizado;
5.21.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo;
5.21.5. Minutos/horas desde a última atualização de vacinas;
5.21.6. Data e horário da última verificação executada na máquina;
5.21.7. Versão do antivírus instalado na máquina;
5.21.8. Se é necessário reiniciar o computador para aplicar mudanças;
5.21.9. Data e horário de quando a máquina foi ligada;
5.21.10. Quantidade de vírus encontrados (contador) na máquina;
5.21.11. Nome do computador;
5.21.12. Domínio ou grupo de trabalho do computador;
5.21.13. Data e horário da última atualização de vacinas;
5.21.14. Sistema operacional com Service Pack.

5.22. Quantidade de processadores;
5.23. Quantidade de memória RAM;
5.24. Usuário(s) logado(s) naquele momento, com informações de contato (caso disponível no Active Directory);
5.25. Endereço IP;
5.26. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;
5.27. Atualizações do Windows Update instaladas;
5.28. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;
5.29. Vulnerabilidades de aplicativos instalados na máquina;
5.30. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
5.31. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:
5.31.1. Alteração de Gateway Padrão;
5.31.2. Alteração de subrede;
5.31.3. Alteração de domínio;
5.31.4. Alteração de servidor DHCP;
5.31.5. Alteração de servidor DNS;
5.31.6. Alteração de servidor WINS;
5.31.7. Alteração de subrede;
5.31.8. Resolução de Nome;
5.31.9. Disponibilidade de endereço de conexão SSL;
5.32. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
5.33. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
5.34. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
5.35. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
5.36. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;
5.37. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;

5.38. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;
5.39. Capacidade de gerar traps SNMP para monitoramento de eventos;
5.40. Capacidade de enviar emails para contas específicas em caso de algum evento;
5.41. Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;
5.42. Deve possuir compatibilidade com Cisco Prime Infrastructure - Version: 3.1 ou superior;
5.43. Deve possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por exemplo);
5.44. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc), inclusive de máquinas que estejam em subnets diferentes do servidor;
5.45. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
5.46. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;
5.47. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:
5.47.1. Nome do vírus;
5.47.2. Nome do arquivo infectado;
5.47.3. Data e hora da detecção;
5.47.4. Nome da máquina ou endereço IP;
5.47.5. Ação realizada.
5.48. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;
5.49. Capacidade de realizar inventário de hardware de todas as máquinas clientes;
5.50. Capacidade de realizar inventário de aplicativos de todas as máquinas clientes;
5.51. Capacidade de diferenciar máquinas virtuais de máquinas físicas

6. CARACTERÍSTICAS PARA ESTAÇÕES WINDOWS

Deve prover as seguintes proteções:

6.1. Antivírus de Arquivos Residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;
6.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
6.3. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
6.3.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
6.3.2. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;
6.3.3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena.
6.4. Verificação por agendamento:
6.4.1. Procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados);
6.4.2. Análise de arquivos; desinfecção ou remoção de objetos infectados.
6.5. Em caso de erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;
6.6. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
6.7. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
6.8. Capacidade de verificar objetos usando heurística;
6.9. Possibilidade de escolha da pasta onde serão guardados os backups e arquivo em quarentena;
6.10. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
6.11. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin

(ferramenta nativa GNULinux).

7. CARACTERÍSTICAS PARA SERVIDORES WINDOWS

Deve prover as seguintes proteções:

7.1. Antivírus de Arquivos Residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;

7.2. Auto-proteção contra-ataques aos serviços/processos do antivírus;

7.3. Firewall com IDS;

7.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados;

7.5. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

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

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

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

7.7.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);

7.7.3. Leitura de configurações;

7.7.4. Modificação de configurações;

7.7.5. Gerenciamento de Backup e Quarentena;

7.7.6. Visualização de relatórios;

7.7.7. Gerenciamento de relatórios;

7.7.8. Gerenciamento de chaves de licença;

7.7.9. Gerenciamento de permissões (adicionar/excluir permissões acima).

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

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

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

7.8.3. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total;

7.8.4. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc.);

7.8.5. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS);

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

7.8.7. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;

7.8.8. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;

7.8.9. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;

7.8.10. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

7.8.11. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação.

7.8.12. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

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

7.8.14. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for

passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

7.8.15. Capacidade de verificar somente arquivos novos e alterados;

7.8.16. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.);

7.8.17. Capacidade de verificar objetos usando heurística;

7.8.18. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;

7.8.19. Capacidade de agendar uma pausa na verificação;

7.8.20. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado.

7.9. O Antivírus de Arquivos, ao encontrar um objeto potencialmente perigoso, deve:

7.9.1. Perguntar o que fazer, ou;

7.9.2. Bloquear acesso ao objeto;

7.9.3. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

7.9.4. Caso positivo de desinfecção: Restaurar o objeto para uso;

7.9.5. Caso negativo de desinfecção: Mover para quarentena ou apagar (de acordo com a configuração préestabelecida pelo administrador);

7.9.6. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

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

7.9.8. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

7.9.9. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

8. CARACTERÍSTICAS DE CRIPTOGRAFIA

8.1. O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso que o usuário tenha esquecido a senha, através de procedimentos de recuperação;

8.2. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;

8.3. Deve ter a capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;

8.4. Deve ter a capacidade de utilizar single sign-on para a autenticação de pré-boot;

8.5. Permitir criar vários usuários de autenticação pré-boot;

8.6. Deve ter a capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;

8.7. Deve ter a capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:

8.7.1. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;

8.7.2. Criptografar todos os arquivos individualmente;

8.7.3. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;

8.7.4. Criptografar o dispositivo removível, em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;

8.8. Deve ter a capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente. Nesta modalidade, os arquivos devem estar acessíveis para todas as máquinas gerenciadas pela mesma console de maneira transparente para os usuários;

8.9. Deve ter a capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;

8.10. Deve ter a capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;

8.11. Verificar compatibilidade de hardware antes de aplicar a criptografia;

8.12. Deve ter a capacidade de estabelecer parâmetros para a senha de criptografia;
8.13. Bloquear o reuso de senhas;
8.14. Bloquear a senha após um número de tentativas pré-estabelecidas;
8.15. Deve ter a capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;
8.16. Permitir criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo;
8.17. Permitir criptografar as seguintes pastas pré-definidas: “meus documentos”, “favoritos”, “desktop”, “arquivos temporários” e “arquivos do outlook”;
8.18. Permitir utilizar variáveis de ambiente para criptografar pastas customizadas;
8.19. Deve ter a capacidade de criptografar arquivos por grupos de extensão, tais como: documentos do office, documentos .txt, arquivos de áudio, etc.;
8.20. Permitir criar um grupo de extensões de arquivos a serem criptografados;
8.21. Deve ter a capacidade de criar regra de criptografia para arquivos gerados por aplicações;
8.22. Permitir criptografia de dispositivos móveis mesmo quando o Endpoint não possuir comunicação com a console de gerenciamento.

9. GERENCIAMENTO DE SISTEMAS

9.1. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;
9.2. Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização, e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários;
9.3. Capacidade de gerenciar licenças de softwares de terceiros;
9.4. Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;
9.5. Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc), informando data de compra, local onde se encontra, servicetag, número de identificação e outros;
9.6. Possibilitar fazer distribuição de software de forma manual e agendada;
9.7. Suportar modo de instalação silenciosa;
9.8. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;
9.9. Possibilitar fazer a distribuição através de agentes de atualização;
9.10. Utilizar tecnologia multicast para evitar tráfego na rede;
9.11. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;
9.12. Suportar modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;
9.13. Capacidade de gerar relatórios de vulnerabilidades e patches;
9.14. Possibilitar criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;
9.15. Permitir iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;
9.16. Permitir baixar atualizações para o computador sem efetuar a instalação;
9.17. Permitir o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;
9.18. Ter capacidade de instalar correções de vulnerabilidades de acordo com a severidade;
9.19. Permitir selecionar produtos a serem atualizados pela console de gerenciamento;
9.20. Permitir selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc.

10. PRAZO DE ENTREGA

10.1. Máximo de 45 (quarenta e cinco) dias, a contar da data da assinatura do contrato;

11. GARANTIA MÍNIMA

11.1. Os objetos deverão possuir garantia técnica mínima de 36 (trinta e seis) meses, sob a responsabilidade da CONTRATADA. A CONTRATADA deverá disponibilizar assistência técnica

no período da garantia técnica;

11.2. No período de vigência, a CDSA não pode ter ônus de nenhuma natureza quando da apresentação de defeito do objeto. É ainda de total responsabilidade do fornecedor qualquer despesa de envio e coleta do mesmo;

11.3. Todas as licenças de software utilizadas para atender o objeto deverão possuir garantia de 36 (trinta e seis) meses;

11.4. A Licitante vencedora deverá prestar suporte técnico e operacional durante o período de vigência da licença, com atendimento através do serviço telefônico (0800), acesso remoto, email ou WEB, para esclarecimento de dúvidas, abertura de chamados, e envio de arquivos para análise (Zero-day). Os prazos relativos aos chamados deverão obedecer ao seguinte nível de serviço: 24 x 7 (vinte e quatro horas por dia, sete dias por semana, dias úteis e horário comercial);

11.5. O serviço de Suporte Técnico garante:

11.6. Reinstalação, reconfiguração e auxilio na utilização de recursos ou solução de problemas relacionados aos sistemas ofertados;

11.7. O direito de receber toda e qualquer atualização de todos os softwares ou patches corretivos de componentes adquiridos após a assinatura do contrato, para a versão mais atual das ferramentas.

11.8. A CONTRATADA deverá prestar atendimento técnico em regime de garantia

12. OBRIGAÇÕES CONTRATUAIS

12.1. DA CONTRATADA

12.1.1. Entregar os bens e serviços discriminados em sua proposta, objeto da contratação, de acordo com as especificações, formas e prazos estipulados neste Termo de Referência, substituindo qualquer item que, a juízo da CDSA, não esteja em conformidade com o ajustado;

12.1.2. Fornecer à CDSA o correspondente termo/certificado de garantia dos objetos adquiridos, emitido pelo respectivo fabricante ou pelo seu representante no Brasil;

12.1.3. Assumir a responsabilidade pelo pagamento dos tributos e encargos resultantes da execução do objeto;

12.1.4. Apresentar se solicitado, documentos que comprovem estarem cumprindo a legislação, em especial, encargos trabalhistas, previdenciários, fiscais e comerciais;

12.1.5. Prestar todos os esclarecimentos que forem solicitados, solucionar de imediato todas as ocorrências relacionadas ao objeto;

12.1.6. Responsabilizar-se pelos danos causados diretamente à Administração ou a terceiros, decorrentes de sua culpa ou dolo na execução do ajuste, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pela CDSA;

12.1.7. Não transferir a outrem, no todo ou em parte, os compromissos avençados;

12.1.8. Prestar assistência técnica, às suas expensas, durante todo o período de garantia do objeto;

12.1.9. Reparar, corrigir, remover, substituir ou ressarcir às suas expensas, no prazo determinado pela fiscalização, os prejuízos causados ao patrimônio da CDSA em decorrência da execução do objeto;

12.1.10. Não divulgar informações a terceiros ou realizar publicidade acerca do objeto, salvo expressa autorização da CDSA;

12.1.11. Customizar todos os softwares pertencentes ao objeto, aos padrões, leis e procedimentos exigidos pela CDSA.

12.1.12. Disponibilizar número de telefone para receber chamados 24 x 7 (vinte e quatro horas por dia, sete dias por semana);

12.1.13. Dar fiel e integral cumprimento ao contido em sua proposta, que passará a integrar o Contrato, independentemente de transcrição;

12.1.14. Não divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto, sem autorização, por escrito, do Contratante, sob pena de aplicação das sanções previstas nos incisos III e IV do artigo 87 da Lei nº. 8.666/93;

12.1.15. Tratar como “segredos comerciais e confidenciais” todos os produtos e subprodutos relativos aos serviços contratados com relação aos dados da administração da CDSA;

12.1.16. Responsabilizar-se por quaisquer ônus, despesas ou obrigações trabalhistas, previdenciárias, fiscais, de acidentes de trabalho, bem como alimentação, viagem, hospedagem e transporte dos seus funcionários ou outros benefícios de qualquer natureza, assim como efetuar o pagamento de seguros, tributos, encargos sociais e de toda e qualquer despesa referente aos serviços contratados e dos documentos a eles relativos, se necessário;

12.1.17. Recrutar em seu nome e sob sua inteira responsabilidade os profissionais necessários à perfeita execução dos serviços, cabendo-lhe efetuar os pagamentos de salários e arcar com as demais obrigações trabalhistas, previdenciárias, fiscais e comerciais, inclusive responsabilidades decorrentes de acidentes, indenizações, substituições, seguros, assistência médica e quaisquer outros, em decorrência da sua condição de empregadora, sem qualquer solidariedade por parte da CONTRATANTE;

12.1.18. Não se valer do Contrato a ser celebrado para assumir obrigações perante terceiros, dando-o como garantia, nem utilizar os direitos de crédito, a serem auferidos em função dos serviços prestados, em quaisquer operações de desconto bancário, sem prévia autorização do Contratante;

12.1.19. Arcar com quaisquer danos ou prejuízos causados à CONTRATANTE;

12.1.20. Nos casos de danos, prejuízos, avarias ou subtração de bens, os valores correspondentes deverão ser descontados do valor a ser pago à CONTRATADA, ou ajuizada, se for ocaso, a dívida, sem prejuízo das demais sanções previstas no Contrato;

12.1.21. Comunicar à CONTRATANTE, de forma detalhada, toda e qualquer ocorrência de acidentes ou incidentes verificada no curso da execução contratual.

12.1.22. Não usar as informações sigilosas ou de uso restrito, quando tais atos forem praticados por quem tenha sido alocado à execução do objeto deste Termo de Referência, sob pena de responsabilidade civil e/ou criminal;

12.1.23. Responsabilizar-se pelo comportamento dos seus empregados e por quaisquer danos que estes ou seus prepostos venham porventura a ocasionar à CONTRATANTE, ou a terceiros, durante a execução dos serviços;

12.1.24. Responder adequadamente a todas as observações, reclamações e exigências efetuadas, no sentido do cumprimento do Contrato e da melhoria dos serviços executados;

12.1.25. Apresentar em até 10 (dez) dias após a data de assinatura do Contrato Cronograma de Execução do serviço;

12.1.26. Informar à CONTRATANTE toda ocorrência que esteja prejudicando a prestação dos serviços e o cumprimento dos níveis de qualidade acordados;

12.1.27. Aceitar que a CONTRATANTE possa rejeitar, no todo ou em parte, os serviços executados em desacordo com as normas estabelecidas no Contrato;

12.1.28. Aceitar que a CONTRATANTE possa solicitar, com justificativa, a substituição de qualquer profissional que considere inadequado para a função, cabendo à CONTRATADA a apresentação de novo profissional, sendo que este profissional deve ter o mesmo perfil exigido na descrição dos serviços deste Termo de Referência;

12.1.29. Manter, em observância às obrigações assumidas, todas as condições de habilitação e qualificação exigidas no processo de licitação

12.2. DA CONTRATANTE

12.2.1. Promover o acompanhamento e a fiscalização do fornecimento dos produtos, sob os aspectos quantitativo e qualitativo, anotando em registro próprio as falhas detectadas;

12.2.2. Prestar informações e esclarecimentos solicitados pelo fornecedor registrado através de seus representantes legais;

12.2.3. Comunicar prontamente à CONTRATADA, qualquer anormalidade no objeto do instrumento contratual ou equivalente, podendo recusar o recebimento, caso não esteja de acordo com as especificações e condições estabelecidas no Termo de Referência;

12.2.4. Deduzir e recolher na fonte os tributos pertinentes sobre os pagamentos efetuados ao fornecedor registrado;

12.2.5. Notificar previamente à CONTRATADA, quando da aplicação de sanções administrativas;

12.2.6. Realizar os atos relativos à cobrança do cumprimento pela CONTRATADA das obrigações contratualmente assumidas e aplicar sanções, garantida a ampla defesa e o contraditório, decorrentes do descumprimento das obrigações contratuais;

12.2.7. Efetuar o pagamento à CONTRATADA, de acordo com o estabelecido no Edital;

12.2.8. Acompanhar, fiscalizar, avaliar o cumprimento das obrigações da CONTRATADA, através de servidor ou de comissão especialmente designada;

12.2.9. Garantir infraestrutura mínima para que a CONTRATADA possa realizar os serviços do objeto contratado;

12.2.10. Colocar à disposição da CONTRATADA os elementos e informações necessários à execução do objeto

13. RESPONSÁVEL PELA ELABORAÇÃO DO TERMO DE REFERÊNCIA

_____

Cláudio Messias Feitosa
CH da Divisão de TI
Portaria 046/2021 PRESI/CDSA

ANEXO II

MODELO DE PROPOSTA

À COMPANHIA DOCAS DE SANTANA CNPJ Nº 04.756.826/0001-36

Rua Cláudio Lúcio Monteiro, nº 1380 – Bairro Novo Horizonte Santana – AP CEP 68.925-974.

Prezados Senhores,

Tendo examinado a relação de itens, nós, abaixo assinados, apresentamos a presente proposta para o objeto em questão, em conformidade com os materiais solicitados, e declaramos que:

1) Os preços cotados incluem todos os custos e despesas necessárias fornecimento dos materiais;

2) Até a formalização da contratação esta proposta constituirá um compromisso de nossa parte, observadas as condições dos materiais apresentados;

Item	Descrição	Marca	Unid.	Quant.	P. Unit.	P. Total
01	LICENÇA DE SOFTWRE ANTIVIRUS CONFORME ESPECIFICACÃO DO TERMO DE REFERENCIA (ANEXO I)		Unid.	40		
GLOBAL					**VALOR TOTAL**	

VALOR TOTAL GLOBAL DA PROPOSTA: R$ XX.XXX,XX (Valor por extenso)

DATA DA PROPOSTA ____/____/_____.

Validade de, no mínimo, 60 (sessenta) dias.

_____

Nome e assinatura do responsável

(carimbo, CNPJ, razão social da empresa)

ANEXO III

MODELO DE DECLARAÇÃO DE CONDIÇÃO DE ME E EPP

A empresa _____, inscrita no CNPJ sob o n.°. _____, por intermédio de seu representante legal,Sr(a). _____, portador do Documento de Identidade n.°. _____, inscrito no CPF/MF sob o n.°. _____, DECLARA,sob as penas da Lei, que cumpre os requisitos legais para qualificação como _____ (incluir a condição da empresa: micro empresa (ME) ou empresade pequeno porte (EPP)), art. 3° da Lei Complementar n.°. 123/2006 e que não está sujeita a qualquer dos impedimentos do §4° deste artigo, estando apta a usufruir do tratamento favorecido estabelecido nos arts. 42 a 49 da citada Lei.

Declaramos possuir restrição fiscal no(s) documento(s) de habilitação e pretendemos utilizar o prazo previsto no art. 43, § 1° da lei Complementar n.°. 123/06, para regularização, estando ciente que, do contrário, decairá o direito à contratação, estando sujeita às sanções previstas no art. 81 da Lei Federal n.°. 8.666/93.

Obs: em caso afirmativo, assinalar a ressalva acima.

(Local)_____ , (Data) ____ de _____ de 2020.

Assinatura e carimbo do representante legal

ANEXO IV

DECLARAÇÃO DE REQUISITOS CONSTITUCIONAIS

Declaramos A Companhia Docas de Santana- CDSA, referente ao Edital da licitação Eletrônica n° 808257/2020-CPL/CDSA, que não possuímos em nosso quadro de pessoal empregado(s) com menos de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e de 16 (dezesseis) anos em qualquer trabalho, salvo na condição de aprendiz, nos termos do inciso XXXIII do art. 7° da Constituição Federal de 1998 (Lei n.o 9.854/99).

(Local)_____ , (Data) ____ de _____ de 2020.

Assinatura e carimbo do representante legal

Observação: Emitir em papel que identifique a licitante.

ANEXO V

MODELO DE DECLARAÇÃO DE INEXISTÊNCIA DE FATO IMPEDITIVO

__(Razão Social da Empresa)__, estabelecida na ___(endereço completo)___, inscrita no CNPJ sob o n.º _____, neste ato representada pelo seu (representante/sócio/procurador), no uso de suas atribuições legais, vem:

DECLARAR, para fins de participação no processo licitatório em pauta, sob as penas da Lei, que INEXISTE qualquer fato impeditivo à sua participação na licitação citada, que NÃO foi declarada inidônea e NÃO está impedida de contratar com o Poder Publico de qualquer esfera, ou suspensa de contratar com a Administração, e que se compromete a comunicar ocorrência de fatos supervenientes.

Por ser verdade, assina a presente.

(Local)_____ , (Data) ____ de _____ de 2020.

_____

Razão Social da Empresa

Nome do responsável/procurador

Cargo do responsável/procurador