TERMO DE REFERÊNCIA

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 **Kaspersky Next Edr Foundations** (antivírus), com gerência centralizada, incluindo atualizações, garantia e suporte técnico pelo período de 36(trinta e seis) meses para continuar cobrindo a segurança da informação da Companhia Docas de Santana (CDSA). conforme especificação e condições constantes neste termo de referência.

2. JUSTIFICATIVA

A contratação de licenças de software antivírus corporativo, objeto desta licitação, justifica-se pela necessidade de garantir a continuidade de proteção e segurança do ambiente de informática da CDSA, principalmente considerando a existência e o aumento contínuo de softwares maliciosos como vírus, trojan, spyware, adware, worms e outros malwares, em destaque, o ransomware devido ao potencial estrago que pode causar a uma organização. A licença da atual solução de antivírus adotada pela CDSA, Kaspersky Endpoint Security for Business - Select ,venceu em 30 de setembro, foi descontinuada e passou a ser comercializada com o nome de **Kaspersky Next Edr Foundations** sendo necessária a presente aquisição para manter o parque da CDSA com proteção atualizada contra as ameaças virtuais mais recentes.

3. DA QUANTIDADE

50 (cinquenta) licenças de uso de solução de antivírus **Kaspersky Next Edr Foundations** 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 deantivírus (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 pelasolução 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 qualquersoftware 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 endpointinstalado 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 gravarum 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 causarincompatibilidade, 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. GERENCIAMENTO DE SISTEMAS

8.1. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;

8.2. 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;

8.3. Capacidade de gerenciar licenças de softwares de terceiros;

8.4. Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;

8.5. 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;
8.6. Possibilitar fazer distribuição de software de forma manual e agendada;
8.7. Suportar modo de instalação silenciosa;
8.8. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;
8.9. Possibilitar fazer a distribuição através de agentes de atualização;
8.10. Utilizar tecnologia multicast para evitar tráfego na rede;
8.11. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;
8.12. Suportar modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;
8.13. Capacidade de gerar relatórios de vulnerabilidades e patches;
8.14. Possibilitar criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;
8.15. Permitir iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;
8.16. Permitir baixar atualizações para o computador sem efetuar a instalação;
8.17. Permitir o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;
8.18. Ter capacidade de instalar correções de vulnerabilidades de acordo com a severidade;
8.19. Permitir selecionar produtos a serem atualizados pela console de gerenciamento;
8.20. Permitir selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc.

9. PRAZO DE ENTREGA

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

10. GARANTIA MÍNIMA

10.1. 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;
10.2. 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/fabricante qualquer despesa de envio e coleta do mesmo;
10.3. Todas as licenças de software utilizadas para atender o objeto deverão possuir garantia de 36 (trinta e seis) meses;
10.4. O serviço de Suporte Técnico do fabricante garante:Reinstalação, reconfiguração e auxilio na utilização de recursos ou solução de problemas relacionados aos sistemas ofertados;
10.5. 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. OBRIGAÇÕES CONTRATUAIS

11.1. DA CONTRATADA
11.1.1. 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;
11.1.2. Fornecer à CDSA o correspondente termo/certificado de garantia dos objetos adquiridos, emitido pelo respectivo fabricante ou pelo seu representante no Brasil;
11.1.3. Assumir a responsabilidade pelo pagamento dos tributos e encargos resultantes da execução do objeto;

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

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

11.2. DA CONTRATANTE

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

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

11.2.3. 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;

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

11.2.5. 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;

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

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

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

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

12. RESPONSÁVEL PELA ELABORAÇÃO DO TERMO DE REFERÊNCIA

Sandro Mauricio O. Silva
Chefe da Divisão de TI
Portaria 010/2023 PRESI-CDSA