AO
MINISTÉRIO PÚBLICO
PROCURADORIA-GERAL DE JUSTIÇA
COMISSÃO PERMANENTE DE LICITAÇÃO
REF.: PREGÃO Nº 43/2020 – PGJ/MA

PROPOSTA COMERCIAL

Prezados Senhores,

Após cuidadoso exame e estudo do Edital do PREGÃO em referência, seus anexos e apensos, com os quais concordamos, vimos apresentar a nossa Proposta, em conformidade com as condições estabelecidas no referido Edital, conforme descrições a seguir:

1. **DOS PREÇOS**

ITEM	OBJETO	QTD	VLR UNT (R$)	VLR TOTAL (R$)
1	**Licença de software antivírus, para fins de proteção da rede lógica, equipamentos de TI e informações, por um período de atualização, suporte e assistência técnica de 36 (trinta e seis) meses, e demais detalhamentos descritos no termo de referência.**	**3000**	**R$64,7110**	**R$ 194.133,00**
	VALOR TOTAL = Cento e noventa e quatro mil, cento e trinta e três reais.			

Validade da Proposta: 60 (Sessenta) dias corridos, contados da data de abertura da sessão pública estabelecida no preâmbulo deste Edital;

IDENTIFICAÇÃO DA LICITANTE:

- ALLSEC SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO LTDA
- CNPJ: 13.497.079/0001-50 - Inscrição Estadual: 0438842-96
- Rua Ribeiro de Brito, 830 - Boa Viagem - Recife/PE CEP: 51.021-310
- **Representante Legal:** Francisca Andrea Caminha Cirino, Brasileira, Casada, Diretora Executiva, RG de n° 2001002296402 e CPF n° 82453306391, residente e domiciliado na Av. Coronel Miguel Dias, nº 1010, Aptº 1301, Torre A, Água Fria - Fortaleza/CE.
- Telefone: (81) 3224-2267, E-mail: licitacoes@allsec.com.br

DADOS BANCÁRIOS

NOME DO BANCO	NOME DA AGÊNCIA	NÚMERO	AGÊNCIA	CONTA
BRASIL	ALDEOTA	001	3515-7	15.328-1
BRADESCO	ALDEOTA	237	0564-9	130466-6

Recife, 23 de Dezembro de 2020.

13.497.079/0001-50
ALLSEC SERV. EM TECNOL. DA INFORMAÇÃO LTDA
RUA: RIBEIRO DE BRITO 830 SALA 1901 E 1902
CTR EMP IBERBRAS -
BOA VIAGEM - CEP: 51.021-310
RECIFE PERNAMBUCO

YURE LEOPOLDO SABINO DE FREITAS
CPF: 525.285.023-20
DIRETOR COMERCIAL

ALLSEC
IT SECURITY

TERMO DE REFERÊNCIA

18.1 Constitui objeto desta LICITAÇÃO a aquisição de licenças de uso de software antivírus, para fins de proteção da rede lógica, equipamentos de TI e informações, por um período de atualização, suporte e assistência técnica de 36 (trinta e seis) meses, aplicação das novas licenças e versões do software, configurações e suporte técnico remoto e on-site, todos necessários para manter atualizada a solução de segurança contra códigos maliciosos, minimizando, assim, os riscos de segurança da informação. O objeto deverá ser entregue de acordo com as especificações técnicas a seguir:

18.1.1 Estações de Tabalho Windows nas versões 32 e 64 bits

18.1.2 Compatibilidade:

18.1.2.1 Microsoft Windows 7 Professional/Enterprise/Ultimate x86 / x64 e posterior;

18.1.2.2 Microsoft Windows 8 Professional/Enterprise x86 / x64;

18.1.2.3 Microsoft Windows 8.1 Pro / Enterprise x86 / x64;

18.1.2.4 Microsoft Windows 10 Pro / Enterprise x86 / x64;

18.1.3 Estações de Trabalho Linux nas versões 32 e 64 bits

18.1.3.1 Compatibilidade:

18.1.3.1.1 Ubuntu 16.04 32/64 bits ou superiores;

18.1.3.1.2 Debian GNU/Linux 8.10 32/64 bits ou superiores;

18.1.3.1.3 OpenSUSE® 42.3 32/64 bits ou superiores;

18.1.3.1.4 Fedora 28 32/64 bits ou superiores;

18.1.4 Servidores Windows nas versões 32 e 64 bits

18.1.4.1 Compatibilidade:

18.1.4.1.1 Windows Server 2008 Standard/Enterprise/Datacenter SP1 e posterior nas versões 32 e 64 bits;

18.1.4.1.2 Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter;

18.1.4.1.3 Windows Server 2016 Essentials/Standard/Datacenter/MultiPoint Premium Server;

18.1.5 Servidores Linux nas versões 32 e 64 bits

18.1.5.1 Compatibilidade:

18.1.5.1.1 Red Hat® Enterprise Linux® 6.9 Server e/ou superiores;

18.1.5.1.2 CentOS-6.9 e/ou superiores;

18.1.5.1.3 Ubuntu 16.04.2 LTS e/ou superiores;

18.1.5.1.4 Debian GNU / Linux 8.10 e/ou superiores;

18.1.5.1.5 OpenSUSE® 42.3 e/ou superiores;

18.1.6 Deve prover as seguintes proteções:

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

18.1.6.2 Antivírus de Web (módulo para verificação de sites e downloads contra vírus);

18.1.6.3 Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);

18.1.6.4 O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;

18.1.6.5 Firewall com IDS;

18.1.6.6 Autoproteção (contra-ataques aos serviços/processos do antivírus);

18.1.6.7 Controle de dispositivos externos;

18.1.6.8 Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc;
18.1.6.9 Controle de execução de aplicativos;
18.1.6.10 Controle de vulnerabilidades do Windows e dos aplicativos instalados;
18.1.6.11 Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
18.1.6.12 As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
18.1.6.13 Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
18.1.6.14 Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
18.1.6.15 Capacidade de adicionar aplicativos a uma lista de "aplicativos confiáveis", onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;
18.1.6.16 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
18.1.6.17 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
18.1.6.18 Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas;
18.1.7 Servidor de Administração e Console Administrativa
18.1.7.1 Compatibilidade
18.1.7.1.1 Microsoft Windows Server 2008/2012/2016 (todas as edições) em 32 ou 64 bits;
18.1.7.1.2 Vmware: vSphere 5.5, vSphere 6 e superiores;
18.1.7.2 Características
18.1.7.2.1 A console deve ser acessada via WEB (HTTPS) ou MMC;
18.1.7.2.2 Console deve ser baseada no modelo cliente/servidor;
18.1.7.2.3 Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;
18.1.7.2.4 Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;
18.1.7.2.5 Deve permitir incluir usuários do AD para logarem na console de administração
18.1.7.2.6 Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM;
18.1.7.2.7 As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;
18.1.7.2.8 Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;
18.1.7.2.9 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;
18.1.7.2.10 Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
18.1.7.2.11 Deve armazenar histórico das alterações feitas em políticas;

18.1.7.2.12 Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada;
18.1.7.2.13 Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas;
18.1.7.2.14 A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;
18.1.7.2.15 Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;
18.1.7.2.16 Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS e Android;
18.1.7.2.17 Capacidade de instalar remotamente qualquer "app" em smartphones e tablets de sistema iOS;
18.1.7.2.18 A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;
18.1.7.2.19 Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário;
18.1.7.2.20 Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;
18.1.7.2.21 Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança;
18.1.7.2.22 Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede;
18.1.7.2.23 Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;
18.1.7.2.24 Capacidade de atualizar os pacotes de instalação com as últimas vacinas;
18.1.7.2.25 Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;
18.1.7.2.26 A comunicação entre o cliente e o servidor de administração deve ser criptografada;
18.1.7.2.27 Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;

Recife, 23 de Dezembro de 2020

13.497.079/0001-50
ALLSEC SERV. EM TECNOL. DA INFORMAÇÃO LTDA
RUA: RIBEIRO DE BRITO 830 SALA 1901 E 1902
CTR EMP IBERBRAS -
BOA VIAGEM - CEP: 51.021-310
RECIFE PERNAMBUCO

YURE LEOPOLDO SABINO DE FREITAS
CPF: 525.285.023-20
DIRETOR COMERCIAL