PROCESSO PBS-PRC-2022/00641
SELEÇÃO DE FORNECEDORES – PREGÃO ELETRÔNICO
CONTRATO Nº 048/2023

CONTRATAÇÃO PARA AQUISIÇÃO DE LICENÇAS DE SOFTWARE DE ANTIVÍRUS E SUPORTE TÉCNICO, QUE ENTRE SI CELEBRAM A FUNDAÇÃO PARAIBANA DE GESTÃO EM SAÚDE - PB SAÚDE E A EMPRESA INORPEL COMERCIO E SERVICOS LTDA.

FUNDAÇÃO PARAIBANA DE GESTÃO EM SAÚDE - PB SAÚDE, fundação pública de direito privado, entidade da Administração Indireta, inscrita no CNPJ/MF sob o nº. 38.111.778/0001-40, neste ato representada por seu Diretor Superintendente, doravante denominada **CONTRATANTE,** e de outro lado a empresa **INORPEL COMERCIO E SERVICOS LTDA**, pessoa jurídica de direito privado, CNPJ Nº 10.920.030/0001-70, com endereço na RODOVIA BR-230, 1620, KM: 05; BLOCO E; MODULOS 2, 3 E 4; TERREO; RECANTO DO POÇO, CABEDELO/PB, CEP: 58.105-182, através de seu representante legal abaixo assinado, neste ato denominada **CONTRATADA,** considerando tudo que consta no **Processo Administrativo PBS-PRC-2022/00641,** RESOLVEM celebrar o presente **CONTRATO** mediante as seguintes cláusulas e condições.

FUNDAMENTAÇÃO LEGAL

O presente contrato de aquisição rege-se por toda a legislação aplicável à espécie, especialmente, Decreto Estadual nº 40.096/2020, Lei Complementar Estadual nº 157/2020, Regulamento Interno de Compras e Contratações de Itens (RICCS) da Fundação Paraibana de Gestão em Saúde, e nas suas vacâncias nas normas gerais contidas na Lei de Licitações, e na legislação estadual aplicada à matéria, bem como os preceitos de direito público e pelas disposições presente neste instrumento.

CLÁUSULA PRIMEIRA - DO OBJETO

1.1 Aquisição de Licenças de software de antivírus e suporte técnico, nos termos do Regulamento Interno de Compras e Contratações de Itens, de acordo com as especificações do Termo de Referência, parte integrante deste instrumento independentemente de transcrição:

ITEM	DESCRIÇÃO DO ITEM	UND	QTD.	VALOR MENSAL	VALOR ANUAL
1	Aquisição de Licenças de Software de Antivírus e Suporte Técnico. Atendimento para 468 computadores e/ou devices na rede do HMDJMP para o período de 12 meses, incluindo Suporte Técnico Especializado 24x7x365, prestação do serviço continuado "On-site" 24 horas por dia, 7 dias na semana e 365 dias no ano.	UND	468	R$ 181,02	R$ 84.717,36

1.2. Os itens adquiridos através deste contrato se destinam a suprir as necessidades da Fundação Paraibana de Gestão em Saúde – PB SAÚDE, no âmbito das unidades hospitalares que gerencia, **pelo período de 12 (doze) meses.**

CLÁUSULA SEGUNDA – DOS RECURSOS FINANCEIROS

2.1. Os recursos financeiros necessários ao custeio do presente Contrato ocorrerão através da Conta Corrente nº 801271-7 do Banco Bradesco S/A.

CLÁUSULA TERCEIRA – DOS PREÇOS E CONDIÇÕES DE PAGAMENTO

3.1 A CONTRATANTE pagará à CONTRATADA o valor global de R$ 84.717,36 (oitenta e quatro mil e setecentos e dezessete reais e trinta e seis centavos), a ser pago em até 30 (trinta) dias do atesto de cada Nota Fiscal e por meio de Ordem Bancária para a Instituição Financeira cuja proponente mantenha conta corrente de sua titularidade, observado o Decreto nº 37.693/2017, após o recebimento definitivo dos serviços pelo fiscal do contrato.

3.2. Na impossibilidade da aplicação do prazo contido na cláusula anterior e desde que caracterizada condição indispensável para a obtenção dos itens ou propiciar significativa economia de recursos, o pagamento poderá ser realizado em menor período, desde que apresente condição vantajosa à PB SAÚDE.

3.3 Quaisquer taxas, impostos ou tributos fiscais, ou de outra natureza, que possam incidir sobre o presente Contrato, ou que tenham relação com objeto realizado(s) ficarão a cargo da CONTRATADA.

3.4 Com relação a cobrança do percentual de 1,6% devido ao Empreender/PB, a que se refere o Inciso II, do art. 8º, da Lei nº 9.335, de 25 de janeiro de 2011, c/c o Decreto Estadual 32.086/11, a mesma deverá ser feita no momento do processamento do pedido de pagamento dos fornecedores pela Administração, incluindo-se o recolhimento do percentual de 1,6% do valor total da fatura, para a implementação e operacionalização do Fundo Estadual de Apoio ao Empreendedorismo – Fundo Empreender - PB.

3.5. O pagamento será efetuado mediante crédito em conta corrente da CONTRATADA, por ordem bancária, quando deverão ser mantidas as mesmas condições iniciais de habilitação.

3.6. Nenhum pagamento será efetuado à CONTRATADA enquanto pendente de liquidação qualquer obrigação financeira decorrente de penalidade ou inadimplência, sem que isso gere direito a reajustamento de preços ou a atualização financeira.

3.7. A CONTRATADA se obriga a manter, durante a vigência do contrato, todas as condições de habilitação exigidas, inclusive a condição de não empregar trabalhador menor na forma da Lei nº 9.854, de 27.10.99. Assume, ainda, a obrigação de apresentar, junto à Nota Fiscal, os seguintes comprovantes devidamente atualizados:

- prova de regularidade para com a Fazenda Federal, Estadual e Municipal do domicílio ou sede da CONTRATADA, compreendendo a Certidão de Quitação de Tributos e a Certidão quanto à Dívida Ativa – ou outras equivalentes, na forma da Lei – expedidas, em cada esfera do Governo, pelo órgão competente;
- prova de regularidade perante o INSS - Instituto Nacional de Seguro Social, mediante apresentação da CND - Certidão Negativa de Débito;
- prova de regularidade perante o FGTS - Fundo de Garantia do Tempo de Serviço, mediante apresentação do CRF - Certificado de Regularidade de Fundo de Garantia, fornecido pela Caixa Econômica Federal.
- Prova da regularidade trabalhista – CNDT.

3.8. A CONTRATADA fica obrigada a aceitar, nas mesmas condições licitadas, os acréscimos ou supressões que se fizerem necessários, de acordo com as previsões legais.

3.9 O valor estabelecido no contrato não poderá sofrer reajustamento na forma do § 1º da Lei 10.192/01 c/c §1º do art. 28 da Lei nº 9.069/95.

CLÁUSULA QUARTA – DA EXECUÇÃO DO CONTRATO

4.1 REQUISITOS MÍNIMOS PARA A SOLUÇÃO DE ANTIVÍRUS:

4.1.1 Possuir uma única console de gerenciamento para gestão e configurações do antivírus, antispyware, firewall, detecção de intrusão, controle de dispositivos, controle de aplicações e criptografia de discos

4.1.2 A solução deverá ter a capacidade de remoção do atual antivírus instalado e ser capaz de instalar de forma remota o agente do antivírus pela console de gerenciamento, e caso não tenha a capacidade de realização a remoção completa, a contratada deverá remover a atual solução utilizando scripts, softwares de terceiros, ou mesmo de forma manual

4.1.3 O produto deverá possuir no mínimo os seguintes módulos e funcionalidades:

4.1.3.1 Console de gerenciamento fornecendo funcionalidades de gestão e configurações de políticas

4.1.3.2 Módulos para estações físicas, notebooks e servidores

4.1.3.3 Módulo para ambientes virtualizados, sendo criado especialmente para ambientes virtuais

4.1.3.4 Módulo para dispositivos móveis no mínimo para tablets e smartphones com sistema operacional iOS e Android; (Somente em console On-premise)

4.1.3.5 Utilizar o conceito de heurística para combate e ações contra possíveis malwares

4.1.3.6 Oferecer tecnologia onde a solução explore vulnerabilidades de softwares instalados no intuito de reduzir o risco de infecções (anti-exploit)

4.1.3.7 Oferecer tecnologia nativa no intuito de eliminar ameaças que sequestram dados, do tipo ransomware

4.1.3.8 Oferecer inventário de softwares

4.1.3.9 Oferecer tecnologia onde a solução teste arquivos potencialmente perigosos em ambiente isolado antes da execução do mesmo no ambiente de produção

4.1.3.10 Oferecer proteção por base de assinaturas (vacinas).

4.2 CONSOLE DE GERENCIAMENTO:

4.2.1 Instalação e configuração:

4.2.2 Permitir instalação de console local (on-premise) com banco de dados local ou instalação em nuvem (cloud) com banco de dados também em nuvem

4.2.3 Para a opção de console local de ser fornecido como um appliance virtual ou executável para instalação em servidores Windows. Deverá suportar no mínimo as seguintes plataformas de virtualização:

4.2.4 VMWare vSphere

4.2.5 Citrix XenServer; XenDesktop, VDI-in-a-Box

4.2.6 Microsoft Hyper-V

4.2.7 Red Hat Enterprise Virtualization

4.2.8 Kernel-based Virtual Machine ou KVM

4.2.9 Oracle VM

4.2.10 Deverá ser fornecido com base de dados embutida e proprietária ou com possibilidade de utilização de banco de dados externo SQL ou Oracle.

4.2.11 Para instalação da console em nuvem (cloud), a nuvem deve ser privada e do mesmo fabricante.

4.2.12 Permitir instalação remota via console WEB de gerenciamento para ambientes virtuais VMWare ou Citrix.

4.2.13 O mecanismo de varredura deverá estar disponível para download separadamente.

4.2.14 A solução deverá permitir a inclusão de um modulo de balanceamento para casos em que vários servidores tenham a mesma função (para alta disponibilidade, recuperação de desastres, performance, dentre outras necessidades).

4.2.15 Deve ser totalmente em português.

4.3 FUNCIONALIDADES GERAIS:

4.3.1 Licenciamento flexível.

4.3.2 O console de gerenciamento deve incluir informações detalhadas sobre as estações e servidores com no mínimo as seguintes informações:

4.3.2.1 Nome

4.3.2.2 IP

4.3.2.3 Sistema Operacional

4.3.2.4 Política Aplicada

4.3.2.5 A console de gerenciamento deverá incluir sessão de log com as seguintes informações:

4.3.2.6 Login

4.3.2.7 Edição

4.3.2.8 Criação

4.3.2.9 Log-out

4.3.3. Arquitetura simples de atualização, com um simples clique deve ser possível atualizar todas funções e serviços da solução

4.3.4 Permitir que o administrador escolha qual o pacote será atualizado

4.3.5 As notificações devem ser destacadas como item não lido e notificar o administrador por e-mail

4.3.6 No mínimo enviar notificações para as seguintes ocorrências:

4.3.6.1 Problemas com licenças

4.3.6.2 Alertas de surto de vírus

4.3.6.3 Máquinas desatualizadas

4.3.6.4 Eventos de antimalware

4.3.7 Deverá prover o acesso via HTTPS

4.3.8 Deverá permitir a importação de certificados digitais

4.3.9 O gerenciamento e a comunicação com dispositivos móveis devem ser feitos de forma segura utilizando certificados digitais.

4.4 MONITORAMENTO:

4.4.1 Baseado em "portlets" configuráveis com no mínimo as seguintes especificações:

4.4.1.1 Nome

4.4.1.2 Tipo de relatório

4.4.1.3 Alvo do relatório

4.4.2 Deverá disponibilizar "portlets" para gerência e monitoramento de qualquer tipo de endpoint, máquinas físicas, virtuais e dispositivos móveis.

4.5 INVENTÁRIO DA REDE:

4.5.1 Possuir no mínimo as integrações abaixo:

4.5.1.1 Múltiplos domínios do Active Directory

4.5.1.2 Múltiplos VMWare vCenters

4.5.1.3 Múltiplos Citrix Xen Servers

4.5.1.4 Possuir a possibilidade de definição de sincronização com o Active Directory em horas

4.5.1.5 Descoberta de rede para máquinas em grupo de trabalho

4.5.1.6 Possuir busca em tempo real pelo menos com os seguintes filtros:

4.5.1.7 Nome

4.5.1.8 Sistema Operacional

4.5.1.9 Endereço IP

4.5.1.10 Possibilitar a instalação remota e desinstalação remota do antivírus

4.5.1.11 Possibilitar a configuração de pacotes de instalação do produto de antivírus

4.5.1.12 Possuir tarefas remotas e configuráveis de scan

4.5.1.13 Possuir tarefa de reinicialização remota de estação ou servidor

4.5.1.14 Assinar políticas para no mínimo os níveis:

4.5.1.15 Computador

4.5.1.16 Máquina Virtual

4.5.1.17 Grupo de Endpoints

4.5.1.18 Usuário do AD

4.5.1.19 Grupo do AD

4.5.1.20 Possuir a propriedade detalhada de objetos gerenciados para:

4.5.1.21 Nome

4.5.1.22 IP

4.5.1.23 Sistema Operacional

4.5.1.24 Grupo

4.5.1.25 Política Assinada

4.5.1.26 Último status de malware.

4.6 POLÍTICAS:

4.6.1 Modelo único para todos os equipamentos, sejam físicos ou virtuais;

4.6.2 Cada serviço de segurança deve ter seu modelo configurável de política com opções específicas de ativar/desativar;

4.6.3 Através do console de gerenciamento o administrador poderá ser capaz de enviar uma política única para configurar o antivírus;

4.6.4 Deverá configurar as funcionalidades como escaneamento do antivírus, firewall de duas vias de detecção de intrusão, controle de acesso a rede, controle de aplicação, controle de acesso web, criptografia (Windows, Mac e Android), localização de dispositivo (Mobile), autenticação e ações para serem aplicadas em caso de vírus e dispositivos em não conformidade.

4.7 RELATÓRIOS:

4.7.1 Deverá apresentar as seguintes funcionalidades:

4.7.1.1 Relatório para cada serviço de segurança

4.7.1.2 Facilidade de usar e visualização simplificada

4.7.1.3 Agendamento, com opção de envio por e-mail para qualquer destinatário conforme escolha do administrador

4.7.1.4 Filtros de agendamento de relatórios

4.7.1.5 Arquivo com todas as instâncias de relatório agendados

4.7.1.6 Exportar o relatório nos formatos .pdf e/ou .csv

4.7.1.7 Oferecer possibilidade de criar relatórios de maneira dinâmica no dashboard da da console de gerenciamento.

4.8 ADMINISTRAÇÃO DE USUÁRIOS:

4.8.1 Deverá apresentar no mínimo as seguintes funcionalidades:

4.8.1.1 Administração baseada em regras

4.8.1.2 Disponibilizar tipos de usuários pré-definidos como no mínimo:

4.8.1.3 Administrador – Gerente dos componentes da solução

4.8.1.4 Administrador de rede - Gerente dos serviços de segurança

4.8.1.5 Relatório – Monitorar e cria relatórios

4.8.1.6 Deverá ser possível customizar um tipo de usuário

4.8.1.7 Deverá permitir a integração de usuários com o Active Directory para autenticação da console de gerenciamento

4.8.1.8 Registrar as ações do usuário na console de gerenciamento

4.8.1.9 Detalhar cada ação do usuário

4.8.1.10 Permitir busca complexa baseada em ações do usuário, intervalos de tempo.

4.9 SEGURANÇA PARA ESTAÇÕES E SERVIDORES:

4.9.1 Proteção para ambientes físicos

4.9.2 Deverá proteger em tempo real e agendado as máquinas físicas em qualquer plataforma de sistema operacional, seja Windows, Linux ou Mac, tanto na console local (on-premises) como na console em nuvem (cloud).

4.9.3 Deverá suportar no mínimo os seguintes sistemas operacionais para estação de trabalho:

4.9.3.1 Windows 10 64Bits

4.9.3.2 Windows 8.1 64Bits

4.9.3.3 Windows 8 64Bits.

4.9.4 Deverá suportar no mínimo os seguintes sistemas operacionais para servidores:

4.9.4.1 Windows Server 2022

4.9.4.2 Windows Server 2019

4.9.4.3 Windows Server 2012R2

4.9.4.4 Windows Server 2012.

4.9.5 Deverá suportar no mínimo os seguintes sistemas operacionais para distribuição Linux:

4.9.5.1 Ubuntu 18.04 LTS ou superior

4.9.5.2 Red Hat Enterprise Linux / CentOS 9 ou superior

4.9.5.3 Linux Mint 19 LTS ou superior

4.9.5.4 Debian 11 ou superior.

4.9.6 Deverá suporte no mínimo os seguintes sistemas operacionais para distribuição MacOS:

4.9.6.1 MacOS 10 ou superior

4.9.6.2 Proteção para ambientes virtuais

4.9.6.3 Deverá proteger em tempo real e agendado as máquinas virtuais em qualquer plataforma de sistema operacional, seja Windows, Linux ou Mac, tanto na console local (on-premises) como na console em nuvem (cloud).

4.9.7 O produto deverá oferecer agente para virtualização dos seguintes produtos:
4.9.7.1 Citrix Xen Server;
4.9.7.2 Microsoft Hyper-V
4.9.7.3 VMware ESXi
4.9.7.4 Red Hat Virtualization
4.9.7.5 Oracle KVM
4.9.7.6 KVM.

4.10 INSTALAÇÃO E CONFIGURAÇÃO REMOTA:

4.10.1 Deverá permitir ao administrador customizar a instalação
4.10.2 Deverá permitir a instalação customizada do antivírus com no mínimo:
4.10.2.1 Instalar o antivírus sem o controle de acesso à internet; (Windows Desktop);
4.10.2.1 Instalar o antivírus sem o módulo de firewall; (Windows Desktop)
4.10.3 A instalação deverá ser possível executar com no mínimo das seguintes maneiras:
4.10.3.1 Executar o pacote de antivírus diretamente na estação de trabalho
4.10.3.2 Instalar remotamente, distribuído via console de gerência web
4.10.4 Deverá ser possível ter um relatório com as estações instaladas e as faltantes da instalação
4.10.5 Ter a capacidade de criar um único pacote independente ser for para 32 bits ou 64 bits
4.10.6 Deverá permitir ao administrador criar grupos e subgrupos para mover as estações de trabalho
4.10.7 O agente utilizado na sincronização deve ser incluído no cliente do antivírus e não ser necessário a distribuição em um agente separado.

4.11 FUNÇÕES GERAIS:
4.11.1 Deverá ter métodos de detecção de vírus, spyware, rootkits e outros mecanismos de segurança
4.11.2 Deverá permitir a configuração do scan do antivírus do cliente como:
4.11.2.1 Scan local
4.11.2.2 Scan híbrido (local\remoto)
4.11.2.3 Scan remoto
4.11.3 Deverá reportar o estado atual das máquinas virtuais no mínimo, protegida/desprotegida

4.11.4 Deverá fazer scan em tempo real e automático

4.11.5 Deverá ser configurável para não escanear arquivos conforme necessidade do administrador, ou seja, por tamanho ou por tipo de extensão

4.11.6 Deverá possuir escaneamento baseado em análise heurística

4.11.7 Deverá permitir a escolha e configuração de pastas a serem scaneadas.

4.11.8 Para melhor proteção, o antivírus deverá ter no mínimo 3 tipos de detecção:

4.11.8.1 Baseada em assinaturas

4.11.8.2 Baseada em heurística

4.11.8.3 Baseada em monitoramento contínuo de processos

4.11.9 Módulo de Antiexploit disponível para servidores e estações de trabalho baseado em Machine Learning para proteger contra vulnerabilidades de softwares

4.11.10 Deve possuir módulo de mitigação de Ransomware para detecção e recuperação de possíveis arquivos criptografados

4.11.11 Deverá ter a capacidade de escaneamento nos protocolos HTTP e SSL nas estações de trabalho

4.11.12 O cliente do antivírus deverá ter o módulo de Antiphishing que deverá ter a opção de verificar links pesquisados com os sites de pesquisas Search Advisor nas estações de trabalho

4.11.13 Deverá possuir módulo de firewall que de acordo com o administrador poderá ou não ser instalado/desinstalado nas estações de trabalho

4.11.14 No módulo de firewall deverá ser possível configurar o modo invisível tanto a nível de rede local ou Internet nas estações de trabalho

4.11.15 Deve possuir módulo de proteção contra ataques de rede que fornece uma camada de segurança a mais que detecta e executa ações contra ataques de rede projetados para obter acesso em endpoints através de técnicas específicas, tais como: ataques de força bruta, explorações de rede, ladrões de senha, movimentação lateral, etc.

4.11.16 Deverá ter os seguintes requisitos mínimos de sistema:

4.11.16.1 Plataformas de Virtualização:

4.11.16.2 Citrix Xen Server

4.11.16.3 VMware vSphere ESX 6 ou superior

4.11.16.4 VMware vCenter Server 6 ou superior

4.11.16.5 Microsoft Hyper-V Server 2012 R2 ou Superior

4.11.16.6 VMware ESXi 6 ou superior

4.11.16.7 KVM.

4.11.17 Sistemas Operacionais para Desktops:

4.11.17.1 Windows 10 64Bits
4.11.17.2 Windows 8.1 64Bits
4.11.17.3 Windows 8 64Bits
4.11.17.4 Linux Mint 19 LTS ou superior
4.11.17.5 Debian 11 ou superior
4.11.17.6 MacOS 10 ou superior.

4.11.18 Sistemas Operacionais para Servidores:
4.11.18.1 Windows Server 2022
4.11.18.2 Windows Server 2019
4.11.18.3 Windows Server 2012R2
4.11.18.4 Windows Server 2012
4.11.18.5 Ubuntu 18.04 LTS ou superior.

4.12 QUARENTENA:

4.12.1 Deverá permitir restauração remota, com configuração de localidade e deleção
4.12.2 Criação e exclusão para arquivos restaurados
4.12.3 Deverá permitir o envio automático de arquivos da quarentena para o laboratório de vírus
4.12.4 Deverá fazer a remoção automática de arquivos antigos, pré-definidos pelo administrador
4.12.5 Deverá permitir a movimentação do arquivo da quarentena para seu local original ou outro destino que o administrador definir
4.12.6 Deverá de forma automática criar exclusão para arquivos restaurados da quarentena
4.12.7 Deverá permitir escanear a quarentena após a atualização de assinaturas.

4.13 CONTROLE DE USUÁRIO:

4.13.1 Deverá ter módulo de controle de usuário integrando com as seguintes características:
4.13.1.1 Bloqueio de acesso a internet
4.13.1.2 Bloqueio de acesso a aplicações definidas pelo administrador.

4.14 CONTROLE DO DISPOSITIVO:

4.14.1 Deverá ser possível a instalação do módulo de controle de dispositivos através da console de gerenciamento
4.14.2 Através do módulo de controle de dispositivo deverá ser possível controlar:

4.14.2.1 Bluetooth
4.14.2.2 CDROM/DVDROM
4.14.2.3 IEEE 1284.4
4.14.2.4 IEEE 1394
4.14.2.5 Windows Portable
4.14.2.6 Adaptadores de Rede
4.14.2.7 Adaptadores de rede Wireless
4.14.2.8 Discos Externos.

4.14.3 Deverá escanear em tempo real qualquer informação localizada em mídias de armazenamento como:
4.14.3.1 CD/DVD
4.14.3.2 Discos Externos
4.14.3.3 Pen-Drivers
4.14.4 Deverá permitir regras de definição de bloqueio/desbloqueio
4.14.5 Deverá permitir regras de exclusão.

4.15 ATUALIZAÇÃO:

4.15.1 Após a atualização o administrador deverá ter a capacidade de configurar uma reinicialização
4.15.2 Possibilidade de utilizar um servidor local para efetuar as atualizações das estações de trabalho
4.15.3 Permitir atualizações de assinatura de hora em hora
4.15.4 Permitir motor de varredura local, no servidor de rede ou em nuvem afim de aumentar o desempenho da estação de trabalho quando a mesma estiver sendo escaneada.

4.16 SEGURANÇA PARA DISPOSITIVOS MÓVEIS:

4.16.1 Requisitos mínimos do Sistema Operacional
4.16.2 Android 4.1 ou superior
4.16.3 Recursos
4.16.4 Permitir atribuir dispositivo com usuário do Active Directory
4.16.5 A ativação do dispositivo da console de gerenciamento deverá ser através de um QR code
4.16.6 Os pacotes de instalação devem estar disponíveis nas lojas dos Sistemas Operacionais.

4.16.7 Deverá permitir no mínimo as seguintes ações:

4.16.7.1 Impor bloqueio de tela e autenticação

4.16.7.2 Desbloquear o dispositivo

4.16.7.3 Restaurar as configurações de fábrica

4.16.7.4 Localizar o Dispositivo

4.16.8 Análise de dispositivos para o Sistema Operacional Android

4.16.9 Criptografia de memória do dispositivo para o Sistema Operacional Android.

4.17 CONFIGURAÇÕES DE SEGURANÇA:

4.17.1 Caso o dispositivo não esteja em conformidade com as políticas estabelecidas deverá ser possível as ações abaixo:

4.17.1.1 Ignorar

4.17.1.2 Bloquear acesso

4.17.1.3 Bloquear o dispositivo

4.17.1.4 Restaurar as configurações de fábrica

4.17.1.5 Remover o dispositivo da console de gerenciamento.

4.17.1.6 Deverá permitir o uso de senha. A senha pode ser configurada conforme necessidade do administrador com no mínimo os seguintes recursos:

4.17.1.6.1 Senha simples ou complexa

4.17.1.6.2 Números e caracteres

4.17.1.6.3 Comprimento mínimo

4.17.1.6.4 Caracteres especiais mínimos

4.17.1.6.5 Período de expiração da senha

4.17.1.6.6 Definir restrição de reutilização de senha

4.17.1.6.7 Definir o número de tentativas de entradas de senha incorretas

4.17.1.6.8 Período de bloqueio do dispositivo.

4.18 SEGURANÇA DE E-MAILS:

4.18.1 Fornecer proteção de antispam para ambiente com instalação local (on-premise) do MS Exchange

4.18.2 Oferecer análise comportamental e proteção para zero-day

4.18.3 Oferecer proteção contra vírus e tentativas de phishing.

4.19 CRIPTOGRAFIA

4.19.1 Possibilidade de criptografia de disco através da console de gerenciamento seja em nuvem ou on-premise com módulo de Criptografia presente na mesma Console do Antivirus.

4.19.2 Deverá utilizar quando necessários serviços de criptografia através agentes nativos da estação de trabalho baseada em Windows (BitLocker) ou Mac (FileVault)

4.19.3 Deverá solicitar autenticação quando iniciado o sistema operacional do equipamento

4.19.4 Deverá ser compatível com Mac OS Mojave.

4.20 PROTEÇÃO AVANÇADA

4.20.1 Detectar e bloquear todos os tipos de ameaças sofisticadas e malwares desconhecidos bem como eliminar malwares desconhecidos e ameaças avançadas que ignoram as soluções tradicionais de proteção de endpoints, incluindo o ransomware. Detectar e bloquear ataques avançados, como os ataques do PowerShell, baseados em scripts, ataques sem arquivos e malware sofisticado, devendo ser detectados e bloqueados antes de serem executados.

4.20.2 Detectar e parar, bloquear e interromper malwares sem arquivos:

4.20.2.1 Parar os ataques com base em macros e scripts. Analisar scripts, como Powershell, WMI, intérpretes de Javascript, etc, bem como adicionar técnicas de analisador de linha de comando para interceptar e proteger scripts, enquanto alerta os administradores e bloqueia a execução de scripts no caso de executar comandos maliciosos.

4.20.3 Reparo e resposta automatizada a ameaças:

4.20.3.1 Quando uma ameaça é detectada, a ferramenta deve neutraliza-la imediatamente por meio de ações que incluem a conclusão do processo, a quarentena, a exclusão e a reversão de alterações mal intencionadas. Compartilhar as informações sobre ameaças em tempo real com a GPN, o serviço de inteligência contra ameaças baseadas na nuvem do fabricante, para impedir ataques semelhantes

4.20.3.2 Obter visibilidade e contexto sobre ameaças devendo identificar e reportar atividades suspeitas alertando antecipadamente para comportamentos maliciosos, como ações suspeitas do sistema operacional

4.20.3.3 Operar com um único agente e console integrados bem como personalizar automaticamente o pacote de instalação e minimizar o carregamento do agente

4.20.3.4 Deverá ter um nível de proteção na fase de pré-execução com modelos locais de aprendizado de máquina e heurística avançada e treinada para detectar ferramentas de hackers, explorações e técnicas de ocultação de malware, a fim de bloquear ameaças sofisticadas antes que elas sejam executadas. Também deverá detectar técnicas de

propagação e sites que hospedam kits de exploração, além de bloquear tráfego suspeito na web. Deverá permite que os administradores de segurança ajustem a proteção para combater os riscos.

4.20.4 Machine Learning:

4.20.4.1 As técnicas de Machine Learning devem utilizar modelos e algoritmos extensamente treinados para prever e bloquear os ataques avançados

4.20.4.2 A ferramenta de Machine Learning deve se basear em características estáticas e dinâmicas, e se treinarem continuamente com bilhões de amostras de arquivos legítimos e maliciosas devendo melhorar significativamente a efetividade da detecção de malware e minimizar os falsos positivos. ações evasivas e conexões a centros de comando e controle.

4.20.5 Sandbox:

4.20.5.1 Sandbox integrado nos terminais que deverá analisar arquivos suspeitos em profundidade, acionar ações destrutivas em um ambiente virtual isolado, hospedado pelo fabricante, analisando seu comportamento e informando sobre intenções maliciosas. O Sandbox deve ser integrado com o agente e encaminhar automaticamente os arquivos suspeitos para análise. Ao retornar uma análise com resultado "malicioso", o Sandbox deverá bloquear automaticamente o arquivo malicioso em sistemas em toda rede imediatamente. O recurso de envio automático deve permitir que os administradores de segurança da empresa escolham o modo de monitoramento ou bloqueio, o que impede o acesso a um arquivo até que um resultado seja emitido. Os administradores também podem enviar arquivos manualmente para análise. As informações forenses devem fornecer um contexto claro das ameaças e ajudar a entender o comportamento delas.

4.20.6 Antiexploit Avançado:

4.20.6.1 Deverá conter antiexploit avançado para prevenção de exploração e proteção a memória e aplicativos vulneráveis, como navegadores, leitores de documentos, arquivos multimídia e tempo de execução (ou seja:Flash ou Java). Os mecanismos avançados devem observar a rotina de acesso na memória para detectar e bloquear técnicas de exploração, como verificação de chamadas de API, pivotamento de pilha, ROP (returnoriented programming), etc.

4.20.7 Inspetor de processo:

4.20.7.1 Inspetor de Processos deverá operar em um modo de confiança zero, monitorando continuamente todos os processos em execução no sistema operacional. Deverá procurar atividades suspeitas ou comportamentos anormais de processos, como tentativas de ocultar o tipo de processo, executar código no espaço de outro processo (sequestro de memória do

processo para escalonamento de privilégios), replicar, descartar arquivos, ocultar para processar aplicativos de listagem, etc. Tomar as medidas de reparação adequadas, incluindo o encerramento do processo e a reversão das alterações efetuadas. Deverá detectar de malwares desconhecidos, avançados e ataques sem arquivos, incluindo ransomware.

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

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

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

CLÁUSULA QUINTA - DAS OBRIGAÇÕES DAS PARTES

5.1. Das obrigações da CONTRATANTE:

5.1.1. Além de outras obrigações previstas no Termo de Referência, a Fundação Paraibana de Gestão em Saúde (PB SAÚDE) terá as seguintes obrigações:

a) Receber o objeto no prazo e condições estabelecidas no Termo de Referência e seus anexos;
b) Verificar minuciosamente, no prazo fixado, a conformidade dos itens recebidos provisoriamente com as especificações constantes do Termo de Referência e da proposta, para fins de aceitação e recebimento definitivos;
c) Comunicar à CONTRATADA, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;
d) Acompanhar e fiscalizar o cumprimento das obrigações da CONTRATADA, através de comissão/servidor especialmente designado;

e) Efetuar o pagamento à CONTRATADA no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no Termo de Referência e seus anexos;

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

5.2 Das obrigações da CONTRATADA:

5.2.1. A Contratada compromete-se conforme o exposto a seguir:

a) A CONTRATADA deve cumprir todas as obrigações constantes no Termo de Referência, anexos e sua proposta, assumindo como exclusivamente seus riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:

b) Efetuar a entrega do objeto em perfeitas conformidades de velocidade e IPs, conforme especificações, prazo e local constantes no Termo de Referência e seus anexos, acompanhado da respectiva nota fiscal de serviço mensal, na qual constarão as indicações referente a: competência do mês de execução do serviço;

c) Fica responsável em refazer às suas custas, em prazo a ser acordado com a CONTRATANTE, a reposição de peças danificadas durante a manutenção;

d) Concluir as manutenções corretivas iniciadas mesmo que isto implique a ultrapassagem do horário normal de trabalho da equipe;

e) Ficar responsável pelo descarte dos materiais substituídos;

f) Apresentar para a prestação de serviços de manutenção preventiva ou corretiva sempre técnicos especializados, devidamente treinados, uniformizados e identificados, habilitados a manter o equipamento devidamente ajustado e em perfeitas condições de funcionamento e segurança;

g) Traçar cronograma de prazo para instalação dos equipamentos cumprindo rigorosamente com os prazos;

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

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

j) Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12,13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990).

k) Observar e cumprir o que determina o Regimento Interno da Fundação Paraibana de Gestão em Saúde – Fundação PB Saúde e das unidades em que houver a entrega dos itens.

l) Comunicar imediatamente à Administração, qualquer anormalidade verificada, inclusive de ordem funcional, para que sejam adotadas as providências de regularização necessárias.

m) Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas no termo de referência;

n) Indicar preposto para representá-la durante a execução do contrato.

o) Não divulgar nem fornecer dados ou informações obtidas em razão do contrato, e não utilizar o nome da CONTRATANTE para fins comerciais ou em campanhas e material de publicidade, salvo com autorização prévia.

p) Substituir, reparar, corrigir, remover, ou reconstruir, às suas expensas, imediatamente, o produto com avarias ou defeitos ou justificar adequadamente o motivo da não substituição imediata, ficando a empresa obrigada a fornecer a data para troca, sendo obrigatório o aceite da Administração Pública.

q) Comunicar à Administração, no **prazo máximo de 24 (vinte e quatro) horas** que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação.

r) Indicar dados bancários, número da agência e conta do CONTRATADO para fins de pagamento (EXCLUSIVAMENTE BRADESCO, conforme Decreto Estadual 37.693/2017).

CLÁUSULA SEXTA – DA VIGENCIA E EFICÁCIA

6.1. O prazo de vigência deste Termo de Contrato é de 12 (doze) meses, com início na data de publicação de seu extrato no DOE/PB.

CLÁUSULA SÉTIMA – DAS SANÇÕES

7.1. Com fundamento no artigo 47 do Regulamento Interno de Compra e Contratação de Itens da FUNDAÇÃO PARAIBANA DE GESTÃO EM SAÚDE – RICCS/PB SAÚDE, a CONTRATADA ficará sujeita, no caso de atraso injustificado assim considerado pela Administração, de execução parcial ou inexecução da obrigação, sem prejuízo das responsabilidades civil e criminal, assegurada prévia e ampla defesa, às seguintes penalidades, cumulativamente ou não:

7.1.1. Advertência escrita, comunicando formalmente desacordo quanto à conduta do fornecedor sobre o descumprimento de contratos e outras obrigações assumidas, e a determinação da adoção das necessárias medidas de correção;

7.1.2. Multas, observando os seguintes limites máximos:

7.1.2.1. 0,3 % (três décimos por cento) por dia, até o trigésimo dia de atraso, sobre o valor do serviço ou entrega de itens não realizados;

7.1.2.2. 10% (dez por cento) sobre o valor da ordem de itens/fornecimento ou do contrato, em caso de recusa do adjudicatário em efetuar o reforço de garantia (quando exigida no contrato;

7.1.2.3. 20% (vinte por cento) sobre o valor do serviço não realizado, no caso de atraso superior a 30 (trinta) dias, ou entrega de objeto com vícios ou defeitos ocultos que o tornem impróprio ao uso a que é destinado, ou diminuam-lhe o valor ou, ainda, fora as especificações contratadas.

7.1.3. Ocorrerá a retenção ou glosa no pagamento sem prejuízo das sanções cabíveis, nas hipóteses em que a CONTRATADA:

a) não produzir os resultados, deixar de executar ou não executar com a qualidade mínima exigida as atividades contratadas.

b) deixar de utilizar os recursos humanos exigidos para a execução dos itens, ou utilizá-los com quantidade inferior à demandada.

7.1.4. Suspensão temporária de participação em procedimentos e impedimento de contratar com a Administração Pública Estadual, pelo prazo de até 24 (vinte e quatro) meses.

7.1.5. As penalidades de advertência e multa serão aplicadas de ofício ou por provocação do fiscal por meio de termo circunstanciado que deverá ser encaminhado ao Diretor Superintendente da PB SAÚDE, nos termos do art. 51, do RICCS.

7.1.6. As demais sanções previstas poderão ser aplicadas cumulativamente com a de multa, assegurado o direito de defesa prévia do interessado no prazo de 5 (cinco) dias úteis, a contar da intimação do ato, no respectivo processo.

7.2. A justificativa para o não cumprimento da obrigação, não se aplicando à multa referida no subitem anterior, só será considerada em casos fortuitos ou de força maior, devendo ser apresentada por escrito.

7.3. Com fundamento no artigo 48, § 6º, do Regulamento Interno de Compra de Itens e Contratação de Itens da FUNDAÇÃO PARAIBANA DE GESTÃO EM SAÚDE (RICCS - PB SAÚDE), ficará impedida de participar de procedimentos de Seleção de Fornecedores da PB SAÚDE ou com ela celebrar contrato, pelo prazo de até 24 (Vinte e quatro) meses, garantido o direito prévio da citação e da ampla defesa, sem prejuízo de multa de até 30% do valor estimado para a contratação e demais cominações legais, ao fornecedor que:

a) não celebrar o contrato;

b) deixar de entregar documentação exigida no certame;

c) ensejar o retardamento da execução do objeto deste procedimento;

d) não mantiver a proposta, injustificadamente;

e) falhar ou fraudar na execução do contrato;

f) comportar-se de modo inidôneo;

g) cometer fraude fiscal;

h) fizer declaração falsa;

i) apresentar documentação falsa.

7.4 A aplicação da sanção multa gera crédito em favor da PB SAÚDE, que pode ser descontado da garantia contratual, dos pagamentos eventualmente devidos, compensada com outros créditos ou cobrada judicialmente.

7.5. A sanção multa pode ser aplicada cumulativamente às demais sanções deste artigo.

7.6. Poderá ser relevada, justificadamente, a execução de multa cujo montante for inferior aos respectivos custos de cobrança.

7.7. A suspensão temporária restringe, por até 24 (Vinte e quatro) meses, o direito de participar de procedimentos de Seleção de Fornecedores da PB SAÚDE ou com ela celebrar contrato.

7.8 Após o trigésimo dia de atraso, o CONTRATANTE poderá rescindir o contrato, caracterizando-se a inexecução total do seu objeto.

CLÁUSULA OITAVA – DOS RECURSOS ADMINISTRATIVOS

8.1. Da decisão de aplicar a multa, é cabível recurso, sem efeito suspensivo, no prazo de 5 (cinco) dias úteis, contados a partir da data do recebimento da notificação pelo CONTRATADO, nos termos do REGULAMENTO INTERNO DE COMPRA DE ITENS E CONTRATAÇÃO DE SERVIÇOS DA FUNDAÇÃO PARAIBANA DE GESTÃO EM SAÚDE (RICCS - PB SAÚDE).

CLÁUSULA NONA – DO ACOMPANHAMENTO E DA FISCALIZAÇÃO

9.1. O contrato será acompanhado e fiscalizado por responsável indicado pela Unidade de Inteligência de Gestão de Contratos, o qual reunirá qualificação técnica para o exercício da tarefa e a imparcialidade necessária ao adequado relacionamento com o Contratado.

9.2. Identificado indício de irregularidade, por parte do contratado, na execução de suas obrigações contratuais, a Unidade de Inteligência de Gestão de Contratos deve adotar as medidas cabíveis para solução do problema, comunicando a Assessoria Executiva de Assuntos Jurídicos para que sejam tomadas as medidas de sua competência.

9.3. A fiscalização de que trata este item não exclui, tampouco, reduz a responsabilidade da CONTRATADA, inclusive, perante terceiros, por qualquer irregularidade, ainda que resultante de

imperfeições técnicas ou emprego de técnicas inadequadas, e, na ocorrência desta, não implica em corresponsabilidade da Administração ou de seus agentes e prepostos.

9.4. A fiscalização primária do escopo contratual será exercida por Rivaldo Gonçalves Pedrosa Filho, denominado fiscal, que deverá ser designado em portaria, ao qual competirá o acompanhamento direto do contrato, diligenciando sobre fiel a execução do ajuste e dando ciência à CONTRATANTE de eventuais irregularidades detectadas;

9.5. O Fiscal do Contrato anotará em registro próprio todas as ocorrências relacionadas à execução do contrato, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das faltas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis. Será de responsabilidade do Gestor do Contrato identificar e aplicar o sistema de glosas escalonada, mediante autorização da Fundação Paraibana de Gestão em Saúde PB Saúde.

CLÁUSULA DÉCIMA - DA RESCISÃO

10.1 O contrato poderá ser extinto:

I. Pela plena execução do respectivo objeto;
II. Pelo advento de termo ou condição prevista no contrato;
III. Por ato unilateral da parte interessada, quando autorizado no contrato ou na legislação em vigor;
IV. Por acordo entre as partes, desde que a medida seja conveniente para PB SAÚDE;
V. Pela via judicial ou arbitral.
VI. Poderá ser rescindido antes de seu termo final, mediante notificação prévia à CONTRATADA com antecedência de 30 (trinta) dias, em face da conclusão de procedimento licitatório contemplando idêntico objeto

10.2 Constituem motivos para a rescisão do contrato:

I - O não cumprimento de cláusulas contratuais, especificações, termo de referência ou prazos;
II - O cumprimento irregular de cláusulas contratuais, especificações, termo de referência e prazos;
III - O atraso injustificado no fornecimento;
IV - A paralisação do fornecimento, sem justa causa e prévia comunicação à PB SAÚDE;
V - A subcontratação total ou parcial do seu objeto, a associação do contratado com outrem, a cessão ou transferência, total ou parcial, bem como a fusão, cisão ou incorporação, não admitidas no edital e no contrato;

VI - A decretação de falência ou a instauração de insolvência civil;

VII - A dissolução da sociedade ou o falecimento do contratado;

VIII - A alteração social ou a modificação da finalidade ou da estrutura da empresa, que prejudique a execução do contrato;

CLÁUSULA DÉCIMA PRIMEIRA – DA PUBLICAÇÃO

11.1. O presente instrumento será publicado por extrato, no Diário Oficial do Estado da Paraíba e disponibilizado no site da CONTRATADA.

CLÁUSULA DÉCIMA SEGUNDA – DAS DISPOSIÇÕES GERAIS

12.1. As dúvidas e os casos omissos serão resolvidos pela autoridade competente da CONTRATANTE, observando-se, sempre, as normas do Instrumento Convocatório para o processo de seleção de fornecedores, que se aplicam integralmente ao presente Contrato.

12.2. Fica eleito o Foro da Comarca da Capital, Estado da Paraíba, como competente para dirimir quaisquer questões oriundas da execução deste Contrato.

12.3. E por estarem avençadas, as partes assinam o presente instrumento em três vias de igual teor e forma, para que produza os seus devidos e efeitos legais, na presença das testemunhas abaixo consignadas.

Santa Rita/PB, 11 / 05 / 2023.

[redacted]

FUNDAÇÃO PARAIBANA DE GESTÃO EM SAÚDE

CONTRATANTE

INORPEL COMERCIO E SERVICOS LTDA

CONTRATADA

TESTEMUNHA 1
NOME: [redacted]
CPF:

TESTEMUNHA 2
NOME: [redacted]
CPF:

[redacted]