TERMO DE CONTRATO DE COMPRA Nº 017/2021, QUE FAZEM ENTRE SI O HOSPITAL OPHIR LOYOLA - HOL E CPDTECH COMÉRCIO DE EQUIPAMENTOS ELETRÔNICOS LTDA.

O HOSPITAL OPHIR LOYOLA, autarquia estadual com sede na Av. Magalhães Barata, nº 992, São Braz, na cidade de Belém, Estado do Pará, inscrito no CNPJ/MF sob o nº 08.109.444/0001-71, neste ato representado pelo Diretor Geral, **JOEL MONTEIRO DE JESUS**, brasileiro, divorciado, Médico, portador do CPF nº 039.523.202-34 e CRM nº 2437/PA, residente e domiciliado nesta cidade, nomeado pelo Decreto Governamental publicado no DOE nº 34.461 de 15 de janeiro de 2021, doravante denominado CONTRATANTE, e **CPDTECH COMÉRCIO DE EQUIPAMENTOS ELETRÔNICOS LTDA**, inscrita no CNPJ/MF sob o nº 19.434.659/0001-84, sediada à QNA 27, LT 06, Loja 01, Parte B, Taguatinga Norte – Brasília/DF, CEP: 72.110-270, Fone: (61) 98221-0101, E-mail: sales@cpdtech,com,br, doravante designada CONTRATADA, neste ato representada pelo Administrador, **CALLEBE ARAUJO DE MEDEIROS MENDES**, portador da CNH nº 06433457336, expedida pelo Detran/DF e CPF/MF nº 049.021.451-70, residente e domiciliado na cidade de Brasília/DF, tendo em vista o que consta no **Processo nº 2020/481.495** e em observância às disposições da Lei Federal nº 8.666, de 21 de junho de 1993, da Lei Federal nº 10.520, de 17 de julho de 2002,da Lei Estadual nº 6.474, de 06 de agosto de 2002, resolvem celebrar o presente Contrato, decorrente do **Pregão nº003/2021**, mediante as cláusulas e condições a seguir enunciadas.

CLÁUSULA PRIMEIRA – DO OBJETO:

1.1 O objeto do presente Contrato é a **Aquisição de Firewalls com licenças,** conforme especificações e quantitativos estabelecidos no Termo de Referência, anexo do Edital.

1.2 - Este Termo de Contrato vincula-se ao Edital do Pregão, identificado no preâmbulo e à proposta vencedora, independentemente de transcrição.

1.3 - Discriminação do objeto:

QTDE	DESCRIÇÃO DO MATERIAL OU SERVIÇO	VALOR UNITÁRIO	VALOR TOTAL
02	02 (dois) Appliance Hardware - 20 x GE RJ45 ports (including 2 x WAN ports, 1 x DMZ port, 1 x Mgmt port, 2 x HA ports, 14 x switch ports), 2 x Shared Media pairs (Including 2 x GE RJ45 ports, 2 x SFP slots); Unified Threat Protection (UTP). Firewall Throughput (1518 / 512 / 64 byte UDP packets) 7.4 / 7.4 / 4.4 Gbps Firewall Latency (64 byte UDP packets) 3 µs Firewall Throughput (Packets Per Second) 6.6 Mpps Concurrent Sessions (TCP) 2 Million New Sessions/Second (TCP) 30,000 Firewall Policies 10,000 IPsec VPN Throughput (512 byte) 1 4	R$ 235.000,00	**R$ 470.000,00**

	Gbps Gateway-to-Gateway IPsec VPN Tunnels 2,000 Client-to-Gateway IPsec VPN Tunnels 10,000 SSL-VPN Throughput 250 Mbps Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode) 300 SSL Inspection Throughput (IPS, HTTP) 3 190 Mbps Application Control Throughput (HTTP 64K) 2 1 Gbps CAPWAP Throughput (1444 byte, UDP) 1.5 Gbps Virtual Domains (Default / Maximum) 10 / 10 Maximum Number of Switches Supported 24 Maximum Number of APs (Total / Tunnel Mode) 64 / 32 Maximum Number of Tokens 1,000 Maximum Number of Registered Clients 2000 High Availability Configurations Active / Active, Active / Passive, Clustering System Performance — Optimal Traffic Mix IPS Throughput 2 1.9 Gbps System Performance — Enterprise Traffic Mix IPS Throughput 2 500 Mbps NGFW Throughput 2, 4 360 Mbps Threat Protection Throughput 2, 5 250 Mbps.System Performance — Optimal Traffic Mix: IPS Throughput 2 1.9 Gbps. System Performance — Enterprise Traffic Mix: IPS Throughput 2 500 Mbps NGFW Throughput 2, 4 360 Mbps Threat Protection Throughput 2, 5 250 Mbps. Licença das aplicações de gerenciamento com prazo mínimo de 36 meses, os equipamentos devem gerir no mínimo 2000 usuários de rede. Com serviços de armazenamento de log junto com as licenças e de igual período. **Design do projeto de acordo com o ambiente e necessidades.** **Confecção de projeto, cronograma de execução seguindo o padrão do PMI.** **Ativação de todas as factories e recursos dos equipamentos e/ou softwares entregues.** **Implementação completa de toda a solução no ambiente do cliente realizado onsite.** **Vinculação com o servidores do hospital seja sistemas windows ou Linux;** **Configuração dos serviços avançados de segurança: IPS, Policy, Trafic Shaping, AntiSpam, Antivírus, Profile, Autenticação e recursos de SD-WAN e compatíveis no equipamento.** **Migração da solução ativa no cliente para a nova plataforma contratada.** **Repasse conhecimento durante instalação da solução para administração básica a toda a equipe de TI;.** **Treinamento administrativo básico para administração das ferramentas contratadas pelo** **cliente toda a equipe de TI,** Suporte Ilimitado Remoto e/ou presencial 24/7; **Reposição Onsite** dos equipamentos em caso de defeito; Monitoramento Proativo com **alertas com a**		

	empresa; Gerenciamento total do ambiente contrato e suporte; Equipamentos fornecidos com **licenciamentos inclusos**.; Os licenciamentos são **fornecidos em todas as soluções comercializadas**, conforme a solução ofertada; **Trade-up** de modelo de equipamento**.** **Marca/Fab: FORTIGATE** **Modelo / Versão: FG-100EF-BDL-950-**		

Requisitos Gerais:

a) Para maior segurança, não serão aceito equipamentos de propósito genérico (PCs ou servidores) sobre os quais podem instalar-se e/ou executar um sistema
operacional regular como Microsoft Windows, FreeBSD, SUN solaris, Apple OS-X o GNU/Linux.

b) Deve vir acompanhado de todas as licenças de software ou hardware necessárias para atendimento às funcionalidades exigidas neste documento.

c) Toda a solução deve ser integrada, de forma que todos os equipamentos,
softwares e assinaturas da solução de Firewall deverão ser do mesmo fabricante, não sendo aceito soluções montadas compostas por itens de fabricantes distintos.

d) A solução deve ser fornecida em Alta Disponibilidade (HA), possuindo suporte a configuração Ativo/Passivo e Ativo/Ativo.

e) Possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades, pelo período de vigência do contrato

f) Devem ser oferecidas integradas à solução, ferramenta própria de gerenciamento, emissão de relatórios e armazenamento de logs.

g) Solução de segurança (UTM) e SDWAN O equipamento de segurança deve ser um sistema integrado UTM (Unified Threat Management) que inclua pelo menos as seguintes características; Firewall de estados (Stateful Firewall).; Filtro de conteúdo com categorías pré-definidas.;Antimalware.; Concentrador VPN para gateways e clientes.;IDS e IPS integrados; Roteamento baseado em políticas.; Balanceamento de, no minimo, dois links WAN e mecanismo para seleção de melhor caminho, automaticamente baseado em, no minimo, jitter, perda de pacotes e delay.

h) Gestão centralizada a partir de uma console de administração baseada na Web e a partir da qual deve ser possível o acesso, configuração e monitoramento de todos os equipamentos de segurança contemplados na solução.

i) Será aceito solução de gerenciamento local, desde que, considerado redundancia de toda parte de hardware, software e funcionalidades. Alem do licenciamento completo para todas funcionalidades exigidas nesse documento.

j) Deve haver mecanismos para agrupar logicamente a administração de um certo número de dispositivos UTM para envio de modificações em suas configurações simultaneamente na plataforma de gerencia deve ser possivel identificar cada uma das localidades remotas com uma identificação administrativa para posteriormente ser usada como filtro de pesquisa

k) O acesso a console de gerenciamento deve ser realizado com o uso de um método de autenticação de dois fatores

l) O acesso a console deve ser por HTTPS (portas 8080 e 443) e seus certificados de segurança devem ser emitidos por entidades reconhecidas na Internet.

m) A console de gerenciamento deve suportar a definição de contas de administrador com base em funções, relatar as alterações às mesmas em um log de eventos e alertas que podem ser consultados por meio da mesma console.

n) O nível hierárquico de administradores da console deve conter:
Administrador de Organização: Um administrador da organização tem visibilidade em todas as redes dentro da organização. Existem dois tipos de administradores da organização: (1) acesso total e (2) somente leitura.

o) O administrador com acesso total pode efetuar as seguintes operações dentro da organização a qual ele pertence:

I. Criar, editar e excluir contas de acesso total e somente leitura para a organização
II. Redefinição de senhas.
III. Criar, editar e excluir redes.
IV. Adicionar novos dispositivos à rede da organização

p) Administrador de Rede: Terão visibilidade nas redes da organização para as quais tenham sido designados como um administrador. Existem dois tipos de administradores de rede: (1) acesso total e (2) somente leitura. Um administrador de rede com acesso total será capaz de efetuar as seguintes operações dentro da organização a qual ele pertence:

I.Criar, editar e excluir outras contas de administrador no âmbito da rede.
II.Criar, editar e excluir redes em que possuam privilégios
III.As alterações de configuração, remoção ou adição de equipamentos deve ser registrada com dia, hora, e nome do administrador que a realizou.
IV. Deve ser possivel identificar tentativas, com sucesso, ou não de login na plataforma de gerencia.
V. Deve haver funcionalidade de criação de templates a fim de facilitar a configuração de diversos equipamentos simultaneamente.
VI. Deve haver um sistema automatizado de upgrade de firmware a fim dos equipamentos estarem sempre com a ultima versão estável de firmware.
VII. Deve ser possível definir período de expiração da senha do administrador.
VIII.Deve ser possível forçar o administrador a não usar as mesmas senhas anteriores
IX. Deve ser possível bloquear o acesso a plataforma após falhas de login

X. Deve ser possível configurar logout da plataforma após minutos sem atividade

XI. Deve ser possível permitir que a plataforma de gerenciamento seja acessível apenas de IP's permitidos

XII.Deve apresentar inventário de equipamentos da solução que estão, ou não, em utilização.

XIII. A console de administração deve possuir ferramenta integrada para captura de pacotes que passam pelos equipamentos de segurança gerenciados. Caso não haja funcionalidade nativa será aceita solução externa.

XIV. Capacidade de identificação de dispositivos que se conectam por meio do appliance, com fio ou sem fio através do endereço IP ou MAC

XV. Suporte para a criação e o gerenciamento de VLANs utilizando o protocolo IEEE 802.1Q.

XVI. Deve suportar criação de rotas estáticas

XVII. Serviço de DNS dinâmico incluído

XVIII. Serviço de NAT para a WAN para tradução de segmentos de rede internos

XIX. Deve ter a capacidade de criar múltiplas instâncias de servidores DHCP. No caso da contratante desejar preservar seu DHCP interno, o equipamento deve ser capaz de se integrar em modo bridge para propagar este serviço para o interior da rede.

XX. Deve ser possível reservar ranges de DHCP assim como configurar entregas fixas de endereço IP

Serviços de segurança

q) Firewall Stateful

- A solução deverá suportar a definição de regras de firewall de camada 3 e Camada 7.
- Regras de políticas de acesso de camada 3 definidas por:
- Protocolo (UDP ou TCP).
- Host, sub-rede ou rede de origem.
- Porta TCP ou UDP de origem.
- Host, sub-rede ou rede de destino.
- Porta TCP ou UDP de destino.
- Através das regras da camada 7, deve suportar a restrição de tráfego a partir de categorias definidas, incluindo:
- Blog.
- E-mail.
- Compartilhamento de arquivos.
- Jogos.
- Noticias.
- Backup on-line.
- Ponto a ponto.
- Redes sociais e compartilhamento de fotos.
- Atualizações de softwares e antivírus.

- Esportes.
- Videoconferência e VoIP.
- Compartilhamento de arquivos via Web.
- hostname http
- Suporte a NAT 1:1 e o redirecionamento de portas (Port Forwarding) para a publicação de sistemas específicos para a Internet.
- Suporte para a criação de zonas desmilitarizadas (DMZ).
- Deve implementar funcionalidade de criação automatizada de túneis IPSEC VPN entre equipamentos dentro da mesma organização
- Deve implementar a criação de VPNs para acesso remoto de usuários usando IPSec L2TP
- As VPNs site-to-site devem poder ser configuradas em modo hub-spoke ou full-mesh
- Deve suportar NAT-transversal
- Deve permitir a criação de tuneis VPN com equipamentos de terceiros.
- Deve permitir a conexão com client VPN
- Deve permitir a integração com active directory

r) SDWAN

I. Deve implementar solução de SDWAN capaz de balancear trafego entre os links WAN;
II. Quando a função de balanceamento de carga estiver desativada, todo o tráfego da WAN deve usar o link principal, com redundância para link secundário e como uma terceira opção a conexão 3G/4G em caso de falha dos links primários e secundários;
III. Deve ser possível configurar a largura de banda dos links principais e backup (celular) de maneira independente;
IV. Deve ser possível definir qual o link principal do equipamento
V. Deve ser possível habilitar ou desabilitar o balanceamento de trafego entre os links
VI. Deve ser possível configurar qual dos links WAN será utilizado para acessar a internet por determinada rede (IP e/ou porta TCP-UDP)
VII. Para trafego encapsulado deve ser possível escolher qual link será utilizado para acessar a localidade central baseado camada 3,4 e 7
VIII. A escolha de qual link será utilizada deve ser automatizada e inteligente baseado em, no mínimo, condições do link como jitter, delay e perda de pacotes
IX. O chaveamento entre os links deve ser automático uma vez atingido níveis não aceitáveis das características citadas acima.
X. Deve ser possível decidir os níveis de qualidade do link e seu chaveamento por aplicação.
XI. A política de modelagem de tráfego deve permitir a atribuição de limites de largura de banda simétricos ou assimétricos por aplicativo, por usuários e por grupo de usuários.
XII. Devem suportar OSPF e roteamento estático para divulgar as rotas as localidades remotas.
XIII. Através da política de modelagem de tráfego devem ser capaz de serem priorizados determinados tipos de tráfego e/ou associados com um rótulo de QoS usando DSCP com pelo

menos 4 classes de serviço (Melhor esforço, background, vídeo e voz)

s) Filtro de Conteúdo

I.A solução deverá implementar recursos de filtro de conteúdo

II.A solução de filtro de conteúdo deverá ter categorias pré definidas para bloqueio

III.Deve permitir a habilitação da funcionalidade "safesearch" ou equivalente assegurando o conteúdo das paginas de busca como google, bing, etc..

IV.Deve ser permitida criação de blacklist baseada em URL, para sites que nunca devem ser acessados.

V.Deve ser permitida também a criação de whitelist, onde estas URL não serão avaliadas pelo filtro de conteúdo

VI.Detecção e prevenção de intrusões:

VII.A solução deve colocar à disposição da instituição a habilidade de ativar o módulo IDS e IPS

VIII.Deve ser possível a ativação ou desativação do módulo IDS/IPS para grupos de usuários.

IX.Deve ser possível a inclusão em whitelist de uma ou várias assinaturas de IDS/IPS para remover da ação de bloqueio.

X. Deve ser possível habilitar o nível de proteção baseado em score CVSS

XI. A solução deve possuir solução de antimalware protection

XII. A funcionalidade de antimalware deve, no mínimo, avaliar os seguintes tipos de arquivos:

XIII. MS OLE2 (.doc, .xls, .ppt)

XIV. MS Cabinet (Microsoft compression type)

XV. MS EXE

XVI. ELF (Linux executable)

XVII. Mach-O/Unibin (OSX executable)

XVIII. Java (class/bytecode, jar, serialization)

XIX. PDF

XX. ZIP (regular and spanned)*

XXI. EICAR (standardized test file)

XXII. SWF (shockwave flash 6, 13, and uncompressed)

XXIII. Caso algum malware seja encontrado deve ser possivel enviar um alerta ao administrador da rede

XXIV. Deve ser possivel adicionar whitelist de URL e de arquivo ao recurso de AMP

XXV. O acesso a rede atraves do equipamento deve poder ser feito apos autenticação em captive portal. Os metodos para essa autenticação devem ser

XXVI. Click-through.

XXVII. Servidor radius

XXVIII. Credenciais de redes sociais.

XXIX. Deve possuir a definição de uma lista de URLs e IPs para que o usuário possa acessar antes de sua autenticação.

XXX. O portal cativo deve ser personalizável.

XXXI. Por meio da mesma console de administração, deve ser possível gerar os relatórios de funcionamento correspondente a todos os equipamentos de segurança da solução.

t) A solução deve suportar atribuição de políticas de segurança, filtro e QoS de acordo com a identidade do usuário conectado a rede baseado em: endereço MAC, IP, nome do usuário no Active directory, LDAP ou RADIUS

I. As políticas acima devem ser aplicadas individualmente ao usuário e/ou em grupos declarados no controlador de domínio da rede.

II. A solução deve entregar, de maneira integrada ou não, ferramentas de visibilidade da rede, usuários, aplicações. Essa ferramenta deve reportar ou permitir no mínimo:

III. Listagem identificando cada um dos clientes conectados a rede, identificando no mínimo: status, descrição, utilização, IP, politica, MAC address e VLAN

IV. Listagem de principais aplicações utilizadas pela rede.

V. Listagem dos usuários que mais acessaram determinada aplicação.

VI. Deve contar com um relatório de utilização por aplicativo, identificando o serviço consultado, a categoria a qual pertence (esporte, música, vídeo, e-mail, tempo real, etc) e a sua utilização em bits por segundo durante o tempo. É necessário identificar o usuário e grupo de usuários que fizeram uso desse aplicativo.

VII. Inventário de equipamentos da solução que estão, ou não, em utilização.

VIII. A ferramenta da gerencia deve apresentar status de cada um dos equipamentos tais como: status das interfaces WAN, LAN, utilização dos links WAN, latência dos links WAN, perda de pacotes nos links WAN

IX. A ferramenta de gerencia deve apresentar funcionalidades de troubleshooting tais como ping, traceroute, DNS lookup, reiniciar o devices

X. A solução deve gerar sob demanda um relatório de segurança da última hora, última semana, última mês ou em um período específico de acompanhamento.

XI. Deve gerar um gráfico no momento de eventos classificados pela sua gravidade (Alta, Média e Baixa), bem como uma lista de eventos de segurança detectada no período de tempo selecionado

XII. Deve apresentar os clientes afetados pelas ameaças de segurança, tipo de dispositivo, qual localidade ele se encontra, data em que foi afetado e quantidade de eventos.

XIII. Deve apresentar as ameaças mais relevantes na rede e breve descritivo da mesma

XIV. Deve apresentar os principais sistemas operacionais afetados na rede.

XV. Deve apresentar em detalhes as ameaças encontradas na rede, com no mínimo as seguintes informações: dia/hora, mecanismo que detectou a ameaça (IDS,IPS, AMP, filtro de conteúdo), origem, destino, ação tomada, e informações da ameaça

XVI. Deve notificar os eventos de segurança aos administradores da rede.

XVII. Caso a solução de gerencia ofertada seja baseada em hardware controlador, deve ser considerada solução de alta disponibilidade total do sistema, incluindo alta disponibilidade para configuração, relatórios e bancos de dados.

XVIII. O sistema de gestão/visibilidade/configuração deve ser acessível via web, e disponível a partir de qualquer dispositivo dentro ou fora da rede

XIX. Deve ser capaz de acessar, configurar e monitorar qualquer dispositivo da solução

XX. Deve implementar autenticação de dois fatores para acesso a administração do sistema

XXI. O acesso deve ser feito via HTTPS

XXII. Deve possuir sistema hierárquico de gerenciamento onde deve ser possível o administrador definir quais redes determinado usuário pode ter gerencia e visibilidade

XXIII. Deve ser possível definir usuários como "somente leitura" sem direito de alteração das configurações

CLÁUSULA SEGUNDA – DA VIGÊNCIA

2.1 - O prazo de vigência deste Termo de Contrato é com **início em 26/02/2021 e encerramento em 25/02/2022.**

CLÁUSULA TERCEIRA – DO PREÇO E DA FORMA DE PAGAMENTO

3.1 – O valor do presente Termo de Contrato é de **R$ 470.000,00 (quatrocentos e setenta mil reais**).

3.2 – No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução contratual, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

3.3 – O pagamento será realizado no prazo máximo de até 30 (trinta) dias, contados a partir do recebimento da Nota Fiscal ou Fatura, através de ordem bancária, para crédito em agência e conta corrente do Banco do Estado do Pará. Caso o prestador não possua conta no banco Banpará, será cobrada pelo Banco taxa referente ao DOC/TED, sendo o valor desta taxa automaticamente descontado no valor depositado para pagamento da prestação do serviço.

3.4 - Considera-se ocorrido o recebimento da nota fiscal ou fatura no momento em que o órgão contratante atestar a execução do objeto do contrato.

3.5 - A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta *on-line* ao Sistema de Cadastramento Unificado de Fornecedores (SICAF) ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 29 da Lei nº 8.666, de 1993.

3.6 - Constatando-se, junto ao SICAF, a situação de irregularidade da Contratada, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do Contratante.

3.7 - Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará

sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para o Contratante.

3.8 - Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

3.9 - Antes de cada pagamento à Contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no Edital.

3.10 - Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, a que se refere o item 10.5 deste Termo.

3.11 - Não havendo regularização ou sendo a defesa considerada improcedente, o Contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da Contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

3.12 - Persistindo a irregularidade, o Contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à Contratada a ampla defesa.

3.13 - Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a Contratada não regularize sua situação junto ao SICAF.

3.13.1 - Será rescindido o contrato em execução com a Contratada inadimplente no SICAF, salvo por motivo de economicidade, segurança estadual ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade do Contratante.

3.14 - Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

3.14.1 - A Contratada regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

CLÁUSULA QUARTA – DA DOTAÇÃO ORÇAMENTÁRIA

4.1 - As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria, prevista no orçamento do Estado do Pará, para o exercício de ***2021*****,** na classificação abaixo:

Gestão/Unidade: 7100/710201

Fonte: 0103/0269

Programa de Trabalho: 10.126.1508.8238

Elemento de Despesa: 3390.40

CLÁUSULA QUINTA – DO REAJUSTE

5.1 - O contrato terá valores fixos e irreajustáveis durante toda a sua vigência.

CLÁUSULA SEXTA – DA ENTREGA E RECEBIMENTO DO OBJETO

6.1. Do Prazo, Local e condições de entrega ou execução

Prazo: 30 dias.

Local: Informática/HOL.

Condição de entrega: Integral.

6.2. Da Garantia: Renovação de Licença por 36 (trinta e seis) meses.

6.3. Do Responsável pelo recebimento, endereço eletrônico e telefone

Recebimento: Informática do HOL.

6.4. Da Qualificação técnica: a Empresa deverá comprovar, por meio de documentos, que é autorizada para fornecer os equipamentos e serviços solicitados, bem como ser apta a execução do serviço de informática proposto.

6.5. Do Resultado esperado: manter a segurança de Informática no HOL.

6.6. Das Condições gerais: a instalação dos programas deve ser feita localmente na sede da contratada, bem como treinamentos, suporte técnico pode ser onsite ou offsite.

6.7. Responsabilidade da Empresa: atualizar o programa remotamente caso necessário ou onsite na sede da CONTRATADA e garantir a permissão de uso (licenças):36 (trinta e seis) meses, bem como as atualizações dos programas em questão pelo período licenciado.

CLAÚSULA SÉTIMA – DA FISCALIZAÇÃO

7.1. A fiscalização da execução do objeto será efetuada pelos servidores designados pela CONTRATANTE, **Sra. Ione Costa Quaresma**, matrícula 5894500/5, e, no seu impedimento, **Sr. Evailson Chaves dos Santos**, matrícula 57229944/1, ambos lotados na Assessoria de Informática, o qual deverá atestar os documentos da despesa, quando comprovada a sua fiel e correta execução, para fins de pagamento.

7.2. A fiscalização ou acompanhamento da execução deste Contrato pela CONTRATANTE não exclui nem reduz a responsabilidade da CONTRATADA, nos termos da legislação referente a licitação e contratos administrativos. Tal responsabilidade de estende-se aos casos de danos causados por defeito relativos à prestação de serviços nos estritos termos do art. 14 da lei 8.078, de 11.9.90 (Código de Defesa do Consumidor;

7.3. Caberá o servidor designado rejeitar, totalmente ou em parte, qualquer produto que não seja comprovadamente novo, assim considerado o de primeiro uso, bem como solicitar a substituição do produto

quando o mesmo não atender as especificações técnicas ou estiver com defeito de fabricação, devendo o fornecedor efetuar a substituição do material no prazo máximo de 05 (cinco) dias a contar da comunicação feita por servidor desta instituição.

CLÁUSULA OITAVA – DAS OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

8.1 - Das obrigações da CONTRATANTE:

I. Proporcionar todas as facilidades para que o fornecedor possa cumprir suas obrigações dentro das condições estabelecidas no contrato;

II. Rejeitar os produtos cujas especificações não atendam, em quaisquer dos itens, aos requisitos mínimos constantes deste Termo de Referência;

III. Acompanhar e fiscalizar a execução do Contrato por intermédio de comissão ou gestor designado para este fim, de acordo com o art. 67 da Lei Federal nº 8.666/93;

IV. Efetuar o(s) pagamento(s) da(s) Nota(s) Fiscal (ais)/Fatura(s) da contratada, após a efetiva entrega dos produtos e emissão dos Termos de Recebimentos Provisório e Definitivo;

V. Notificar a empresa, por escrito, sobre imperfeições, falhas ou irregularidades constantes de cada um dos itens que compõem o objeto deste termo, para que sejam adotadas as medidas corretivas necessárias;

VI. Prestar todas as informações e/ou esclarecimentos que venham a ser solicitados pelos técnicos da contratada;

VII. Estabelecer normas e procedimentos de acesso às suas instalações para substituição de cada um dos itens que compõem o objeto deste termo.

8.2 – Das obrigações da CONTRATADA.

I. Prestar a manutenção preventiva e corretiva dos equipamentos. Para atendimento nas localidades da CONTRATANTE a empresa a ser CONTRATADA deverá respeitar os prazos e metas descritos abaixo:

II. O prazo máximo para o atendimento dos chamados será de até 60 (sessenta) minutos corridas após o início do atendimento do chamado, exceto para parada total do equipamento que deve ser substituído em no máximo 4 (quatro) horas.

III. Nos casos em que não seja possível o reparo do equipamento dentro do prazo estabelecido, será facultado à CONTRATADA a instalação de outro equipamento em perfeitas condições de uso e com a mesma configuração. Nesse caso o chamado será suspenso, até que o equipamento original possa retornar ao parque. No caso de reparo externo de equipamento, a CONTRATADA deverá fornecer equipamento provisório no prazo de 04 (quatro) horas.

IV. Caso o equipamento substituído fique em manutenção por um período superior a 30 dias, o mesmo deverá ser substituído definitivamente por um novo.

V. Caberá à CONTRATADA substituir, obrigatoriamente por equipamentos novos, os equipamentos que porventura apresentarem o mesmo defeito por 3 vezes, em um período de 3 meses.

VI. Em casos de solicitação de alteração do local do equipamento no Hospital Ophir Loyola - HOL, a CONTRATADA deverá providenciar o desligamento, o transporte e a instalação no prazo máximo de 24 (vinte e quatro) horas. Em qualquer caso em que o equipamento for retirado de seu local de instalação original, deverá possuir uma ordem de serviço aberta, que conterá obrigatoriamente o registro do contador do Hardware no momento da saída do equipamento, a homologação do registro pelo responsável da CONTRATANTE, bem como o motivo de sua remoção.

VII. Nos casos de instalação de novos equipamentos, deverá possuir uma ordem de serviço aberta, que conterá obrigatoriamente o registro do Hardware no momento de entrada do equipamento, a homologação do registro pelo responsável da CONTRATANTE, bem como o motivo de sua instalação. O prazo máximo para instalação é 24 (vinte e quatro) horas.

VIII. 4Nos casos de substituição temporária dos equipamentos, os registros do Hardware, tanto do equipamento defeituoso, quanto do substituto instalado, deverão ser associados em um só chamado e comunicados detalhadamente ao gestor do contrato.

IX. Nenhum chamado aberto pela Central de Suporte deverá ficar sem solução depois de decorridos 24 horas após sua abertura.

Caso o atendimento não seja concluído e a CONTRATADA não providencie a substituição do equipamento inoperante nos prazos estabelecidos acima, conforme, o caso, o órgão CONTRATANTE glosará do pagamento o valor da parte fixa estabelecida no contrato, relativo ao equipamento, pelos dias úteis em que o mesmo permanecer parado, sem prejuízo da aplicação de multa, conforme previsto no instrumento contratual. O valor a ser glosado do faturamento será calculado utilizando-se da seguinte fórmula:

Vg = N/22

Onde: Vg = valor a ser glosado do pagamento.

N= número de dias úteis em que o equipamento permaneceu parado e 22 é o número médio de dias úteis/mês.

X. A central poderá ser acionada através de sistema Web, e-mail único e canal de atendimento tipo 0800 (ligação gratuita), disponibilizados pela CONTRATADA. Não serão permitidos ligação a cobrar ou tipos 0300 e 4004.

XI. O suporte técnico deverá ser disponibilizado aos usuários dos serviços 24 horas por dia e 7 dias da semana.

u) Capacitação e Treinamento de Usuários.

Na fase de implantação, a empresa a ser contratada deverá ministrar até 40 (quarenta) horas treinamentos para a equipe de TI do CONTRATANTE, no prazo máximo de 10 (dez) dias a contar do início da implantação.

O conteúdo programático dos cursos para os facilitadores deverá prever todas as funções necessárias para a correta operação de todo equipamento, dos serviços previstos por parte dos usuários e funções administrativas de toda a solução implantada, com entrega de apostila com conteúdo a ser ministrado, manual do operador em português da solução, certificado do treinamento é a documentação de toda solução implantada ao termino do treinamento.

CLÁUSULA NONA – DAS SANÇÕES ADMINISTRATIVAS

9.1-Comete infração administrativa nos termos da Lei nº 10.520, de 2002, a Contratada que:

9.1.1-Inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

9.1.2-Ensejar o retardamento da execução do objeto;

9.1.3-Falhar ou fraudar na execução do contrato;

9.1.4-Comportar-se de modo inidôneo;

9.1.5-Cometer fraude fiscal.

9.2-Pela inexecução total ou parcial do objeto deste contrato, a Administração pode aplicar à Contratada as seguintes sanções:

9.2.1-Advertência**,** por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para o Contratante;

9.2.2-Multa moratória de 0,5% (cinco décimos por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias;

9.2.3-Multa compensatória de até 20% (vinte por cento) sobre o valor total do contrato, no caso de inexecução total do objeto;

9.2.3.1-Em caso de inexecução parcial, a multa compensatória, no mesmo percentual do subitem acima, será aplicada de forma proporcional à obrigação inadimplida;

9.2.4-Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

9.2.5.- Impedimento de licitar e contratar com órgãos e entidades do Estado do Pará com o consequente descredenciamento no SICAF pelo prazo de até cinco anos;

9.2.5.1-A sanção de impedimento de licitar e contratar prevista no subitem 13.2.5 também é aplicável em quaisquer das hipóteses previstas como infração administrativa no edital;

9.2.6-Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir o Contratante pelos prejuízos causados.

9.3- As sanções previstas poderão ser aplicadas à Contratada juntamente com as de multa moratória, descontando-a dos pagamentos a serem efetuados.

9.4-Também ficam sujeitas às penalidades do art. 87, III e IV, da Lei nº 8.666, de 1993, as empresas ou profissionais que:

9.4.1. Tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

9.4.2. Tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

9.4.3-Demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

9.5-A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à Contratada, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente na Lei nº 9.784, de 1999.

9.6. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

9.7. As penalidades serão obrigatoriamente registradas no SICAF e nos demais cadastros.

CLÁUSULA DÉCIMA – DA RESCISÃO

10.1 - O presente Termo de Contrato poderá ser rescindido:

10.1.1 - por ato unilateral e escrito da Administração, nas situações previstas nos incisos I a XII e XVII do art. 78 da Lei nº 8.666, de 1993, e com as consequências indicadas no art. 80 da mesma Lei, sem prejuízo da aplicação das sanções previstas no Termo de Referência, anexo ao Edital;

10.1.2 - amigavelmente, nos termos do art. 79, inciso II, da Lei nº 8.666, de 1993.

10.2 - Os casos de rescisão contratual serão formalmente motivados, assegurando-se à CONTRATADA o direito à prévia e ampla defesa.

10.3 - A CONTRATADA reconhece os direitos da CONTRATANTE em caso de rescisão administrativa prevista no art. 77 da Lei nº 8.666, de 1993.

10.4 - O termo de rescisão será precedido de Relatório indicativo dos seguintes aspectos, conforme o caso:

10.4.1 - Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

10.4.2 - Relação dos pagamentos já efetuados e ainda devidos;

10.4.3 - Indenizações e multas.

CLÁUSULA DÉCIMA PRIMEIRA – DAS VEDAÇÕES

11.1 - É vedado à CONTRATADA:

11.1.1 - caucionar ou utilizar este Termo de Contrato para qualquer operação financeira;

11.1.2 - interromper a execução contratual sob alegação de inadimplemento por parte da CONTRATANTE, salvo nos casos previstos em lei.

CLÁUSULA DÉCIMA SEGUNDA – DAS ALTERAÇÕES

12.1 - Eventuais alterações contratuais reger-se-ão pela disciplina do art. 65 da Lei nº 8.666, de 1993.

12.2 - A CONTRATADA é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessária, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

12.3 - As supressões resultantes de acordo celebrados entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

CLÁUSULA DÉCIMA TERCEIRA – DOS CASOS OMISSOS

13.1 - Os casos omissos serão decididos pela CONTRATANTE, segundo as disposições contidas na Lei nº 8.666, de 1993, na Lei nº 10.520, de 2002 e demais normas federais de licitações e contratos administrativos e,subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 - Código de Defesa do Consumidor - e normas e princípios gerais dos contratos.

CLÁUSULA DÉCIMA QUARTA – DA PUBLICAÇÃO

14.1 - Incumbirá à CONTRATANTE providenciar a publicação deste instrumento, por extrato, no Diário Oficial do Estado, no prazo previsto no §5º do art. 28 da Constituição do Estado do Pará.

CLÁUSULA DÉCIMA QUINTA – DO FORO

•- Fica eleito o Foro da Comarca de Belém, Capital do Estado do Pará, para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não possam ser compostos pela conciliação, conforme art. 55, §2º da Lei nº 8.666/93.

Belém, 26 de Fevereiro de 2021

HOSPITAL OPHIR LOYOLA	**CPDTECH COMÉRCIO DE EQUIPAMENTOS**
JOEL MONTEIRO DE JESUS	**ELETRÔNICOS LTDA**
Diretor Geral	**CALLEBE ARAUJO DE MEDEIROS MENDES**
CONTRATANTE	Representante Legal
	CONTRATADA

TESTEMUNHAS

1. _____	2. _____
Nome:	Nome:
CPF/MF	CPF/MF