

MINUTA CONTRATUAL
CONTRATO XX/XX – HMAP
CONTRATO DE NA PRESTAÇÃO DE SERVIÇOS DE INTERNET

QUADRO 01 – DOS DADOS DAS PARTES	
CONTRATANTE:	
INSTITUTO BRASILEIRO DE GESTÃO HOSPITALAR – IBGH	CNPJ: 18.972.378/0009-70
	ENDEREÇO: Av. V-5, S/N, Qd. A, Área Lt.001-E SALA 01, Cidade Vera Cruz, Aparecida de Goiânia – Goiás, CEP: 74.936-600
	NESTE ATO REPRESENTADO POR SEU SUPERINTENDENTE: Estêvão Costa Daltro
	CPF: 467.255.551-87
CONTRATADA	
XXX	CNPJ: XXX
	ENDEREÇO: XXX
	REPRESENTANTE LEGAL: XXX
	CPF: XXX
	RG: XXX

QUADRO 02 – DA UNIDADE DE SAÚDE, VIGÊNCIA CONTRATUAL E OBJETO

UNIDADE DE SAÚDE

HOSPITAL MUNICIPAL DE APARECIDA DE GOIÂNIA HMAP	MUN./UF Aparecida de Goiânia – GO.
	CONTRATO DE GESTÃO: 1095/2018 -SEL
VIGÊNCIA CONTRATUAL: 12 (doze) meses.	
INÍCIO: A partir da emissão da ordem de serviço	
POSSIBILIDADE DE PRORROGAÇÃO: Podendo ser renovado anualmente (ou na data de vencimento) formalizado por meio de aditivo em razão da necessidade ou conveniência de continuação da prestação do serviço/fornecimento dos produtos devidamente justificada, sendo limitado a vigência do Contrato de Gestão em referência.	
PRAZO VINCULADO AO CONTRATO DE GESTÃO: Em caso de rescisão, por qualquer motivo, do Contrato de Gestão ao qual esta contratação está vinculada, o contrato firmado entre a CONTRATANTE e a CONTRATADA será rescindido, independente de prévio aviso ou notificação.	
ESPECIFICAÇÃO DO OBJETO E NATUREZA DO CONTRATO	
OBJETO: CONTRATO DE NA PRESTAÇÃO DE SERVIÇOS DE INTERNET	
NATUREZA: Prestação de serviços	

QUADRO 03 – DOS SERVIÇOS E ATUAÇÃO TÉCNICA

SERVIÇOS A SEREM EXECUTADOS

1. ESPECIFICAÇÕES TÉCNICAS DO OBJETO:

1.1 REQUISITOS GERAIS

- Contratação de empresa especializada para o fornecimento de acesso à Rede Mundial de Internet com 100% de garantia de banda downstream e upstream, full-duplex, com conectividade em protocolos IPv4 e IPv6.
- Toda a infraestrutura de rede, acesso e CPE da CONTRATADA deverão ser dimensionadas e preparadas para suportar a totalidade do serviço.
- A CONTRATADA deverá reservar os canais de comunicação e as portas de acesso à sua infraestrutura para uso exclusivo da CONTRATANTE, não sendo admitido o compartilhamento desses recursos com outro de seus clientes ou usuários
- acesso referido no item anterior deverá ser provido por meio de backbone próprio da prestadora de serviço.
- Os equipamentos da CONTRATADA utilizados em toda a solução deverão ser novos e compatíveis com ambientes corporativos ou institucionais modernos.
- A CONTRATADA obriga-se e se responsabiliza a prestar o serviço objeto da licitação, por meio de mão de obra especializada e devidamente qualificada, necessário à completa e perfeita execução dos serviços, em conformidade com as especificações do Termo de Referência.
- Será de responsabilidade da CONTRATANTE o fornecimento de energia elétrica para alimentação dos equipamentos nas dependências das unidades, o aterramento da rede elétrica e a climatização das dependências.

2. CARACTERÍSTICAS DO LINK INTERNET

- Fornecer e instalar link de Internet na taxa de 200Mbps dedicado.
- CONTRATADA deverá disponibilizar 04 endereços IPV4 e 04 endereços IPV6 fixos e válidos para provimento da solução de Internet.
- A conexão entre o CPE da CONTRATADA e o equipamento da CONTRATANTE deverá ser realizada através de interface Gigabit Ethernet 1000BASE-TX.
- A CONTRATADA poderá utilizar acessos de terceiros como última milha, sendo de inteira responsabilidade da CONTRATADA o cumprimento dos SLAs especificados 99.5%.
- A velocidade do link do serviço entregue à CONTRATANTE deverá ser correspondente a 100% da banda contratada.

- acesso físico (conexão entre o ponto de presença da CONTRATADA e os equipamentos de comunicação de dados da CONTRATADA instalados nas dependências da CONTRATANTE) deverá ser realizado exclusivamente por meio de fibra óptica, sendo vedada a utilização de qualquer outra tecnologia de acesso.
- O serviço de Internet deverá ser entregue em rede roteada, utilizando protocolos de camada 3, com SLA 99,5% de disponibilidade e MTTR de vinte quatro (24) horas
- Disponibilizar serviço de Domain Name Resolution (DNS) da CONTRATADA, capaz de resolver direta e reversamente endereços de Internet, para registro no servidor DNS primário.
- Ser monitorado em regime 24x7 por centro de monitoração da CONTRATADA, sendo responsável pela administração e gerência de equipamentos e links de comunicação de dados, manutenção dos níveis mínimos de serviços exigidos e prevenção e recuperação de falhas de serviço.
- Disponibilizar informações sobre os serviços de acesso à Internet por meio de um portal de monitoramento, com acesso restrito, utilizando protocolo seguro (HTTPS), contendo estatísticas de desempenho e de disponibilidade do acesso.
- Possibilitar que a equipe técnica da CONTRATANTE realize consultas no portal de monitoramento, bem como visualize relatórios das informações de desempenho dos serviços contratados
- A CONTRATADA não poderá:
 - a) Implementar nenhum tipo de filtro de pacotes que possa incidir sobre o tráfego originado ou destinado à CONTRATANTE, a menos que tenha expressa concordância com esta.
 - b) Implementar nenhum tipo de cache transparente, a menos que tenha expressa concordância da CONTRATANTE.

3. CARACTERÍSTICAS DO ROTEADOR

- O roteador a ser instalado no ambiente da CONTRATANTE deverá ter no mínimo as seguintes características técnicas:
 - a) O equipamento e seus módulos e softwares não deverão constar em nenhuma lista do fabricante com as situações de “End-of-Sale”, “End-of-Order”, “End-of-Life” ou “End-of-Support”.
 - b) Deve possuir no mínimo quatro (04) interfaces Gigabit Ethernet padrão 1000BASE-TX.

- Possuir protocolo SNMP habilitado com acesso de leitura.
- Deve implementar os protocolos de roteamento RIP, OSPFv2, OSPFv3 e BGP-4.
- Deve possuir suporte nativo ao protocolo IPv6.
- Deve possuir suporte ao protocolo Netflow v9 ou superior.
- Deve possuir suporte ao protocolo 802.1q.
- Deve possuir suporte aos protocolos Telnet e SSHv2.
- Deve possuir gerenciamento local através de uma porta console, sendo que todos os cabos e adaptadores necessários para o gerenciamento através da porta console deverão ser fornecidos pela CONTRATADA de forma a propiciar o gerenciamento do roteador a partir de uma porta USB.
- Deverá ser disponibilizado para a CONTRATANTE com o último release de software estável disponibilizado pelo fabricante, capaz de atender a todos os requisitos acima, incluindo o suporte à atualização do referido software durante o período de vigência do contrato.
- Deve ser montável em rack padrão EIA-310 com largura padrão 19” ocupando no máximo 1U de altura.

4. CARACTERÍSTICAS DO SERVIÇO Anti DDoS

- A CONTRATADA deverá prover, no âmbito do serviço de segurança do link de Internet, uma solução para identificação, tratamento e mitigação transparente de ataques volumétricos do tipo negação de serviço distribuído (DDoS – Distributed Denial of Service).
- A CONTRATADA deve possuir infraestrutura de mitigação própria com capacidade para conter ataques de grande volume, sendo eles de origem nacional ou internacional. Deverá possuir pelo menos 2 (dois) centros de limpeza, cada um com capacidade de mitigação de 40 Gbps (quarenta gigabits por segundo).
- A CONTRATADA deverá disponibilizar em seu backbone, proteção contra ataques volumétricos de negação de serviço, evitando assim a saturação da banda da Internet e indisponibilidade dos serviços em momentos de ataques DDoS (Distributed Denial of Service).
- A CONTRATADA deverá prover o serviço de mitigação sem limitação de tempo de duração do ataque e com quantidade ilimitada de eventos de ataque ao longo da vigência contratual.

- O ataque deve ser mitigado separando o tráfego legítimo do tráfego malicioso, de modo que os serviços de Internet providos pelo cliente continuem disponíveis.
- A solução deve possuir mecanismos para filtragem de pacotes anômalos, garantindo a validade das conexões, sem efetuar qualquer limitação com base no número de sessões ou de pacotes por endereço, de modo a evitar o bloqueio de usuários legítimos.
- Em casos de ataques não detectados pela solução, quando identificados pela CONTRATANTE, deverão ser mitigados imediatamente pelas CONTRATADA após a abertura de chamado através da Central de Atendimento sempre como um chamado com Prioridade Máxima, e deverá realizá-la, sem nenhum ônus ao CONTRATANTE.
- O serviço deve prover suporte à mitigação automática de ataques, utilizando múltiplas técnicas incluindo, mas não se restringindo a: White Lists, Black Lists, limitação de taxa de tráfego, descarte de pacotes mal formados, técnicas de mitigação de ataques aos protocolos HTTP, NTP e DNS, bloqueio por localização geográfica de endereços IP.
- A CONTRATADA deve realizar a detecção de ataques utilizando-se dos recursos mais atuais para detecção de ataques de negação de serviço, tais como análise estatística de tráfego, padrões predefinidos para bloqueios de ataques, correlacionamento com ataques que estejam ocorrendo simultaneamente em outras partes do mundo e atualização para detecção de ataques de negação de serviço desconhecidos.
- O serviço deve prover também análise de tráfego baseado em reputação de endereços IP, possuindo base de informações própria, que pode ser gerada durante a filtragem de ataques e interligada com os principais centros mundiais de avaliação de reputação de endereços IP.
 - O serviço deve prover mecanismos capazes de detectar e mitigar todos e quaisquer ataques de DDoS que façam o uso não autorizado de recursos de rede, tanto para IPv4 Ataques de inundação (Bandwidth Flood), Floods de UDP, TCP e ICMP.
 - Ataques à pilha TCP, incluindo mal uso das Flags TCP, ataques de RST e FIN, SYN Flood e TCP Idle Resets.
 - Ataques que utilizam Fragmentação de pacotes, incluindo pacotes IP, TCP e UDP.
 - Ataques provenientes de Botnets, Worms e que utilizam falsificação de endereços IP origem (IP Spoofing).
 - Ataques à camada de aplicação, incluindo protocolos HTTP, DNS, NTP, dentre outros.

- O serviço deve manter uma lista dinâmica de endereços IP bloqueados, retirando dessa lista os endereços que não enviarem mais requisições maliciosas após um período de tempo considerado seguro pela CONTRATADA.
- O serviço deve permitir a configuração de níveis diferenciados de proteção por grupo de hosts ou subnets.
- O serviço deve ser capaz de bloquear tráfego baseado em assinaturas em até 15 minutos.
- O serviço deve ser capaz de analisar e aprender o comportamento do tráfego para criar automaticamente parâmetros de bloqueio (Limite de conexão HTTP, TCP, UDP, ICMP, etc.).
- O serviço deve ser capaz de detectar anomalias no tráfego, ataques ainda não conhecidos e criar bloqueios em tempo real sem intervenção manual do administrador.
- como para Ipv6, incluindo, mas não se restringindo aos seguintes:
- O Serviço deve ser capaz de mitigar ataques DDoS na nuvem de forma automatizada, configurando thresholds diferenciados para os níveis de proteção criados que, se atingidos, redirecionem o tráfego para o centro de limpeza da CONTRATADA, para posterior devolução do tráfego limpo à rede da CONTRATANTE.
- A CONTRATADA deve realizar a mitigação de ataques e limpeza do tráfego ilegítimo sem prejudicar ou impedir o tráfego legítimo, seja ele originado de uma ou mais fontes.
- A CONTRATADA deve atuar na detecção de Falsos-Positivos e promover medidas proativas para que bloqueios indevidos não ocorram e nem impacte no tráfego de negócio da CONTRATANTE, desde que as atividades relacionadas estejam devidamente autorizadas pela CONTRATANTE por e-mail ou mediante atendimento de chamado técnico.

5. CARACTERÍSTICAS DA SOLUÇÃO DE SEGURANÇA (NGFW)

5.1 CARACTERÍSTICAS GERAIS DA SOLUÇÃO NGFW

- A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração.
- Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.
- As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação.
- A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada

- Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3ad e LACP.
- Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding.
- Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM).
- Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay.
- Os dispositivos de proteção de rede devem possuir suporte a DHCP Server.
- Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames.
- Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas.
- Deve suportar NAT dinâmico (Many-to-1).
- Deve suportar NAT dinâmico (Many-to-Many).
- Deve suportar NAT estático (1-to-1).
- Deve suportar NAT estático (Many-to-Many).
- Deve suportar NAT estático bidirecional 1-to-1.
- Deve suportar Tradução de porta (PAT).
- Deve suportar NAT de Origem.
- Deve suportar NAT de Destino.
- Deve suportar NAT de Origem e NAT de Destino simultaneamente.
- Deve poder combinar NAT de origem e NAT de destino na mesma política
- Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico.
- Deve suportar NAT64 e NAT46.
- Deve implementar o protocolo ECMP.
- Deve implementar balanceamento de link por hash do IP de origem.
- Deve implementar balanceamento de link por hash do IP de origem e destino.
- Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links.
- Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais.

- Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede.
- Enviar log para sistemas de monitoração externos, simultaneamente.
- Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL.
- Proteção anti-spoofing.
- Implementar otimização do tráfego entre dois equipamentos.
- Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2).
- Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3).
- Suportar OSPF graceful restart.
- Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3).
- Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.
- Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego.
- Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego.
- Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.
- Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente.
- Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3
- Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster.
- A configuração em alta disponibilidade deve sincronizar: Sessões.
- A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede.
- A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs.
- A configuração em alta disponibilidade deve sincronizar: Tabelas FIB.
- O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link.
- Deve possuir suporte a criação de sistemas virtuais no mesmo appliance.
- Em alta disponibilidade, deve ser possível o uso de clusters virtuais, seja ativo-ativo ou ativo-passivo, permitindo a distribuição de carga entre diferentes contextos.

- Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas.
- Controle, inspeção e descryptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos).
- Deve apoiar um tecido de segurança para fornecer uma solução de segurança holística abrangendo toda a rede.
- O tecido de segurança deve identificar potenciais vulnerabilidades e destacar as melhores práticas que poderiam ser usadas para melhorar a segurança e o desempenho geral de uma rede.
- Deve existir um Serviço de Suporte que oferece aos clientes uma verificação de saúde recorrente com um relatório de auditoria mensal personalizado de seus appliances NGFW.

5.2 CONDIÇÕES DO FORNECIMENTO DOS APPIANCES

- a) A CONTRATADA deverá comunicar à CONTRATANTE, antecipadamente, a data e o horário da entrega, não sendo aceitos os produtos que estiverem em desacordo com as especificações constantes deste instrumento.
- b) A CONTRATADA deverá se responsabilizar por todos os ônus relativos ao fornecimento dos equipamentos inclusive frete, seguro, cargas e descargas desde a origem até sua entrega no local de instalação

5.3 MANUAIS E DOCUMENTAÇÃO

- a) A CONTRATADA deverá indicar os sites dos fabricantes envolvidos nesta solução que devem obrigatoriamente oferecer download gratuito de todas as atualizações de drivers de dispositivos e firmwares para os equipamentos ofertados bem como dispor dos manuais técnicos com informações detalhadas e atualizadas sobre instalação, configuração, operação e administração dos equipamentos.

5.4 TRANSFERÊNCIA DE CONHECIMENTO

- a) A CONTRATADA deverá fazer a transferência de conhecimento de no mínimo 40 (quarenta) horas para até 6 (seis) funcionários a ser definidos pela CONTRATANTE. O repasse de conhecimento visa um treinamento básico de startup das soluções e não um treinamento oficial.

A transferência de conhecimento será feita nas dependências da CONTRATANTE e não inclui nenhum tipo de material didático ou certificado.

5.5 TREINAMENTO OFICIAL

- Deverão ser ofertadas 3 (três) vagas para treinamento oficial de configuração, administração e utilização de **TODOS OS COMPONENTES DE HARDWARE E SOFTWARE** desta solução. Todos os materiais didáticos, ou seja, cada um dos 3 (três) participantes deverão receber o seu material didático oficial do fabricante.
- A CONTRATADA não será responsável pelos valores de logística, hospedagem e alimentação. Somente pelo fornecimento dos vouchers para o treinamento oficial, estes citados acima.
- Os treinamentos deverão ser ministrados por instrutores especialistas nos respectivos componentes da solução e que detenha todas as condições técnicas (teóricas e práticas) necessárias para desempenhar tal função.
- Na conclusão de cada treinamento, deverão ser entregues a cada um dos 3 (três) participantes um certificado de conclusão do treinamento.

5.6 CONSOLE DE GERÊNCIA E MONITORAMENTO

- Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento.
- O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta.
- Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows e Linux.
- O gerenciamento deve permitir/possuir:
 - . Criação e administração de políticas de firewall e controle de aplicação.
 - . Criação e administração de políticas de IPS, Antivírus e Anti-Spyware.
 - . Criação e administração de políticas de Filtro de URL.
 - . Monitoração de logs.
 - . Ferramentas de investigação de logs.
 - . Debugging.
 - . Captura de pacotes.
- Acesso concorrente de administradores.
- Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos.

- Criação de regras que fiquem ativas em horário definido.
- Criação de regras com data de expiração.
- Backup das configurações e rollback de configuração para a última configuração salva.
- Suportar Rollback de Sistema Operacional para a última versão local.
- Habilidade de upgrade via SCP, TFTP e interface de gerenciamento.
- Validação de regras antes da aplicação.
 1. É permitido o uso de appliance externo para permitir a validação de regras antes da aplicação.
- Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing).
 1. É permitido o uso de appliance externo para permitir a validação de políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing).
- Deve possibilitar a visualização e comparação de configurações Atuais, configuração anterior e configurações antigas.
- Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors)
- Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração.
- Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado.
- Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição.
- Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus e Anti-Spware), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes.
- O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança.
- Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Spware), etc.
- Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e Anti-Spware), e URLs que passaram pela solução.

- Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime.
- Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso.
- Deve ser possível exportar os logs em CSV.
- Deverá ser possível acessar o equipamento a aplicar configurações durante momentos onde o trafego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada.
- Rotação do log.
- Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):
 1. Situação do dispositivo e do cluster.
 2. Principais aplicações.
 3. Principais aplicações por risco.
 4. Administradores autenticados na gerência da plataforma de segurança.
 5. Número de sessões simultâneas.
 6. Status das interfaces.
 7. Uso de CPU
- Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:
 1. Resumo gráfico de aplicações utilizadas.
 2. Principais aplicações por utilização de largura de banda de entrada e saída.
 3. Principais aplicações por taxa de transferência de bytes.
 4. Principais hosts por número de ameaças identificadas.
 5. Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Spware), de rede vinculadas a este tráfego.
 6. Deve permitir a criação de relatórios personalizados.
- Em cada critério de pesquisa do log deve ser possível incluir múltiplas entradas (ex. 10 redes e IP's distintos. serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa.
- Gerar alertas automáticos via:
 1. Email.
 2. SNMP.
 3. Syslog.

5.7 CAPACIDADE DO APPLIANCE

- Hardware Specifications
- GE RJ45 WAN Interfaces 2
- GE RJ45 Management/HA Ports 2
- GE RJ45 Ports 14
- GE SFP Slots 4
- USB port 1
- Console (RJ45) 1
- Local Storage — 1x 480 GB SSD
- Included Transceivers 0
- PS Throughput 2 2.2 Gbps
- NGFW Throughput 2, 4 1.8 Gbps
- Threat Protection Throughput 2, 5 1.2 Gbps
- Firewall Throughput
- (1518 / 512 / 64 byte UDP packets)
- 20 / 20 / 9 Gbps
- Firewall Latency (64 byte UDP packets) 3 μ s
- Firewall Throughput (Packets Per Second) 13.5 Mpps
- Concurrent Sessions (TCP) 2 Million
- New Sessions/Second (TCP) 135,000
- Firewall Policies 10,000
- IPsec VPN Throughput (512 byte) 1 7.2 Gbps
- Gateway-to-Gateway IPsec VPN Tunnels 2,000
- Client-to-Gateway IPsec VPN Tunnels 10,000
- SSL-VPN Throughput 900 Mbps
- Concurrent SSL-VPN Users
- (Recommended Maximum, Tunnel Mode)
- 500
- SSL Inspection Throughput (IPS, avg. HTTPS) 3 820 Mbps
- SSL Inspection CPS (IPS, avg. HTTPS) 3 1,000
- SSL Inspection Concurrent Session
- (IPS, avg. HTTPS) 3
- 240,000
- Application Control Throughput (HTTP 64K) 2 3.5 Gbps
- CAPWAP Throughput (1444 byte, UDP) 1.5 Gbps
- Virtual Domains (Default / Maximum) 10 / 10
- Maximum Number of FortiSwitches Supported 24
- Maximum Number of FortiAPs
- (Total / Tunnel Mode)
- 128 / 64
- Maximum Number of FortiTokens 5,000
- Maximum Number of Registered FortiClients 600
- High Availability Configurations Active / Active, Active / Passive, Clustering

- Height x Width x Length (inches) 1.75 x 17.0 x 11.9
- Height x Width x Length (mm) 44.45 x 432 x 301
- Weight 11.9 lbs (5.4 kg) 12.12 lbs (5.5 kg)
- Form Factor Rack Mount, 1 RU
- Power 100–240V AC, 50–60 Hz
- Maximum Current 110 V / 3 A, 220 V / 0.42 A
- Power Consumption (Average / Maximum) 70.98 / 109.9 W
- Heat Dissipation 374.9 BTU/h
- Operating Temperature 32–104°F (0–40°C)
- Storage Temperature -31–158°F (-35–70°C)
- Humidity 10–90% non-condensing
- Noise Level 31.1 dBA
- Operating Altitude Up to 7,400 ft (2,250 m)
- Compliance FCC Part 15B, Class A, CE, RCM, VCCI, UL/cUL,
- CB, BSMI
- Certifications ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN;
- IPv6

5.8 CONTROLE POR POLÍTICA DE FIREWALL

- Deverá suportar controles por zona de segurança.
- Controles de políticas por porta e protocolo.
- Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.
- Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.
- Firewall deve ser capaz de aplicar a inspeção UTM (Application Control e Webfiltering no mínimo) diretamente às políticas de segurança versus via perfis.
- Além dos endereços e serviços de destino, objetos de serviços de Internet devem poder ser adicionados diretamente às políticas de firewall.
- Deve suportar o armazenamento de logs em tempo real tanto para o ambiente de nuvem quanto o ambiente local (on-premise).
- Deve suportar o padrão de indústria 'syslog' protocol para armazenamento usando o formato Common Event Format (CEF).
- Deve haver uma maneira de assegurar que o armazenamento dos logs em tempo real não supere a velocidade de upload.
- Deve suportar o protocolo padrão da indústria VXLAN.

5.9 CONTROLE DE APLICAÇÕES

- Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo.
- Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.
- Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail.
- Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs.
- Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo.
- Deve detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Bittorrent e aplicações VOIP que utilizam criptografia proprietária.
- Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor.
- Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante.
- Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex.
- Identificar o uso de táticas evasivas via comunicações criptografadas.
- Atualizar a base de assinaturas de aplicações automaticamente.
- Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos.

- Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários.
- Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras.
- Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos.
- Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas.
- Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante.
- A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, RTSP e SSL.
- O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações.
- Deve alertar o usuário quando uma aplicação for bloqueada.
- Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos.
- Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos.
- Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo.
- Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos.
- Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc).
- Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação.

Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação.

5.10 PREVENÇÃO DE AMEAÇAS

- Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall.
- Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware).
- As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.
- Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade.
- Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset.
- As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração.
- Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança.
- Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura.
- Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.
- Deve permitir o bloqueio de vulnerabilidades.
- Deve permitir o bloqueio de exploits conhecidos.
- Deve incluir proteção contra ataques de negação de serviços.
- Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise de padrões de estado de conexões.
- Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise de decodificação de protocolo.
- Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise para detecção de anomalias de protocolo.
- Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise heurística.
- Deverá possuir o seguinte mecanismo de inspeção de IPS: IP Defragmentation.
- Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc.
 - Detectar e bloquear a origem de portscans.
 - Bloquear ataques efetuados por worms conhecidos.
 - Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS.

- Possuir assinaturas para bloqueio de ataques de buffer overflow.
- Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto.
- Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações.
- Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3.
- Identificar e bloquear comunicação com botnets.
- Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.
- Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação.
- Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos.
- Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas.
- Os eventos devem identificar o país de onde partiu a ameaça.
- Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.
- Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.
- Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.
- O Firewall deve permitir que se analise a implantação de Tecido de Segurança para identificar potenciais vulnerabilidades e destaque as práticas recomendadas que podem ser usadas para melhorar a segurança e o desempenho geral da rede.
- Caso o firewall possa ser coordenado por software de segurança do computador do usuário final (laptop, desktop, etc.) deve ter um perfil onde se possa executar a análise de vulnerabilidade nestes equipamentos de usuário e assegurar que estes executem versões compatíveis.
- Análise de postura de segurança devem existir para permitir que o software de segurança do endpoint aplique proteção em tempo real, antivírus, filtragem da Web e controle de aplicativos no endpoint.
- Fornecer proteção contra ataques de dia zero por meio de estreita integração com os componentes Security Fabric, incluindo NGFW, Sandbox (on-premise e nuvem).

5.11 FILTRO DE URL

- Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).
- Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança.
- Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local.
- Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL.
- Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs.
- Possuir pelo menos 60 categorias de URLs.
- Deve possuir a função de exclusão de URLs do bloqueio, por categoria.
- Permitir a customização de página de bloqueio.
- Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site).
- Além do Explicit Web Proxy, suportar proxy Web transparente.

5.12 IDENTIFICAÇÃO DE USUÁRIOS

- Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local.
- Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.
- Deve possuir integração e suporte a Microsoft Active Directory para os seguintes sistemas operacionais: Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 e Windows Server 2012 R2.
- Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à, utilização de sistemas virtuais, segmentos de rede, etc.

- Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.
- Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários.
- Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal).
- Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços.
- Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD.
- Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso a internet e gerenciamento da solução.
- Prover no mínimo um token nativamente, possibilitando autenticação de duplo fator.

5.13 QoS E TRAFFIC SHAPING

- Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube, Ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.
- Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem.
- Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino.
- Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo.
- Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus.
- Suportar a criação de políticas de QoS e Traffic Shaping por porta.
- O QoS deve possibilitar a definição de tráfego com banda garantida.
- O QoS deve possibilitar a definição de tráfego com banda máxima.
- O QoS deve possibilitar a definição de fila de prioridade.
- Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.
-

- Suportar marcação de pacotes Diffserv, inclusive por aplicação.
- Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping.
- Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes.

5.14 FILTRO DE CONTEÚDO

- Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc).
- Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos.
- Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos.

Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

5.15 GEOLOCALIZAÇÃO

- Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados.
- Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.
- Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.

5.16 1VPN IPSec

- Suportar VPN Site-to-Site e Cliente-To-Site.
- Suportar IPSec VPN.
- Suportar SSL VPN.
- A VPN IPSEc deve suportar 3DES.
- A VPN IPSEc deve suportar Autenticação MD5 e SHA-1.
- A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14.
- A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2).
- A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard).
- A VPN IPSEc deve suportar Autenticação via certificado IKE PKI.
- Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall.
- Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting.

- A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB.
- A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente.
- Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies.
- Atribuição de DNS nos clientes remotos de VPN.
- Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL.
- Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local.
 - Suportar leitura e verificação de CRL (certificate revocation list).
 - Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL.
 - Deve permitir que a conexão com a VPN seja estabelecida da seguinte forma: Antes do usuário autenticar na estação.
 - Deve permitir que a conexão com a VPN seja estabelecida da seguinte forma: Após autenticação do usuário na estação.
 - Deve permitir que a conexão com a VPN seja estabelecida da seguinte forma: Sob demanda do usuário.
 - Deverá manter uma conexão segura com o portal durante a sessão.
 - O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bits), Windows 8 (32 e 64 bits), Windows 10 (32 e 64 bits) e Mac OS X (v10.10 ou superior).

• **DOS LOCAIS DE PRESTAÇÃO DO SERVIÇO**

Órgão deverá disponibilizar a relação dos endereços e velocidades que deverão ser entregues na solução.

7. DOS PRAZOS DE EXECUÇÃO DOS SERVIÇOS

7.1 ELABORAÇÃO DO PLANO DE IMPLANTAÇÃO

- A CONTRATADA deverá apresentar um Plano de Implantação em no máximo 10 (dez) dias corridos a partir da assinatura do Contrato.
- A execução do Plano de Implantação somente poderá ser iniciada após a sua aprovação pela CONTRATANTE.

- O detalhamento do Plano de Implantação deverá conter no mínimo:
- Cronograma com macro atividades a serem desenvolvidas para a implantação de todos os serviços previstos neste Termo de Referência. O cronograma deverá conter as seguintes informações:
 - Identificação dos responsáveis das atividades.
 - Duração das atividades.
 - Sequenciamento das atividades.
- Projeto com topologias (física e lógica) da rede, elementos envolvidos, localização dos POPs, faixas de endereçamento IP, detalhamento da gerência, bem como a arquitetura do serviço, incluindo a estratégia de roteamento.

8. DA INSTALAÇÃO DOS SERVIÇOS

- A CONTRATADA terá até trinta (30) dias corridos após a assinatura do contrato para instalar os serviços especificados no Edital e Termo de Referência.
- A instalação do circuito e CPE somente será considerada concluída após a aprovação, pelo Gestor do Contrato, que ocorrerá em até 5 (cinco) dias corridos após notificação da CONTRATADA.
- Todos os equipamentos deverão suportar alimentação com tensão de 110/220 Volts (corrente alternada) bifásica com frequência de 60 Hz.

9. DO GERENCIAMENTO DA IMPLANTAÇÃO

- Disponibilizar e alocar 1 (um) profissional que será responsável pelo gerenciamento das atividades do projeto de implantação, por parte da CONTRATADA.
- Obter informações e esclarecimentos necessários para que possa elaborar o Plano de Implantação do Serviço. Serão abordados e discutidos os seguintes pontos:
 - a) Instalação dos circuitos.
 - b) Datas e horários de restrição para implantação.
 - c) Requisitos de infraestrutura necessários para a instalação dos equipamentos.
 - d) Requisitos para a elaboração e entrega do Plano de Implantação do Serviço.
 - e) Serviços que deverão ser configurados na implantação.
 - f) Demais assuntos de interesse correlatos à implantação dos serviços.
 - Apresentar ao Gestor do Contrato do CONTRANTE o(s) profissional(is) que atuará(ão) como preposto(s) da empresa para assuntos relativos à execução contratual, e informar ao CONTRANTE o nome completo e o CPF deste(s) preposto(s).

10. CENTRAL DE ATENDIMENTO E SUPORTE TÉCNICO

- A fim de manter os serviços em funcionamento adequado aos parâmetros contratuais, a CONTRATADA deverá:
 - Possuir um Centro de Operações de Rede (Network Operations Center – NOC) disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, responsável por monitorar o funcionamento dos serviços e realizar as ações corretivas necessárias para restabelecer a normalidade dos serviços.
- Possuir uma equipe especializada (SOC - Security Operation Center), disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, responsável pelo monitoramento, detecção e mitigação de ataques, realizando as ações corretivas necessárias para garantir o bom funcionamento dos serviços.
- Possuir uma equipe especializada (SOC - Security Operation Center), disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, responsável pelo monitoramento, detecção e mitigação de ataques, realizando as ações corretivas necessárias para garantir o bom funcionamento dos serviços.
- A CONTRATADA deverá disponibilizar à CONTRATANTE uma Central de Atendimento Técnico, acessível via chamada telefônica gratuita (0800), disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, responsável por prestar suporte técnico, receber chamados de serviços e prestar informações acerca do andamento destes.
- O limite de atuação da CONTRATADA para fins de manutenção, reparo e configuração será a porta LAN de seus roteadores ou switches, de forma a garantir os níveis de serviço contratados.
- Enviar à CONTRATANTE, por e-mail, notificações de abertura, andamento e fechamento de chamados, realização de manutenção preventiva ou corretiva e fatos relevantes para a prestação e utilização dos serviços.
- Enviar à CONTRATANTE, por e-mail, uma lista de recorrência (“escalation list”) contendo os nomes, números de telefone e endereços de e-mail das pessoas que devem ser acionadas em caso de problemas no atendimento técnico. A lista de recorrência deverá ser mantida atualizada e sua versão mais recente deverá ser enviada à CONTRATANTE sempre que houver alteração.

- A CONTRATADA deverá iniciar o atendimento no prazo máximo de 1 (uma) hora, contada a partir da data e hora do chamado.
- Todo acesso às instalações da CONTRATANTE por pessoal técnico da CONTRATADA, ou de seu preposto, deverá ser previamente agendado.
 - Manutenções e/ou intervenções programadas nos serviços, quando necessárias, mesmo no caso daquelas que não impliquem inoperância dos serviços contratados ou alteração nas suas características, que necessitem a presença do técnico da CONTRATADA, deverão ser autorizadas pela CONTRATANTE.
 - Qualquer manutenção e/ou intervenção de caráter emergencial para solução de falhas, inoperâncias e/ou indisponibilidades, verificadas na rede, deverá ser agendada e acordada previamente com a CONTRATANTE.

11. PORTAL DE GERENCIAMENTO E ACOMPANHAMENTO DOS SERVIÇOS

- A CONTRATADA deverá disponibilizar um Portal WEB de gerência, possibilitando a visualização online dos serviços prestados, como também realizar o registro e acompanhamento dos chamados.
- **Consulta e visualização online:** O Portal deverá apresentar informações relativas aos ativos de rede utilizados com as seguintes funcionalidades:
 - a) Alertas em caso de falhas e anormalidade dos circuitos.
 - b) Topologia da rede, incluindo roteadores e circuitos, com a visualização do status de todos os elementos.
 - c) Visualização da utilização de banda dos circuitos, de forma diária, semanal e mensal, com a opção de consulta de dados históricos de até 3 (três) meses.
 - d) Visualização do consumo de CPU e memória dos roteadores.
 - e) Indicação da taxa de perda de pacotes, latência e disponibilidade nos circuitos.
 - f) Inventário dos roteadores contendo a configuração física de cada equipamento (interfaces, memória, cpu, etc). modelo e fabricante. endereços IPs e máscaras.
- **Registro e acompanhamento dos chamados:**

Permitir o acompanhamento dos registros de problemas e das ações executadas para a recuperação dos serviços, relativos à pelo menos aos últimos 90 (noventa) dias, incluindo as seguintes informações:

 - Identificação do registro (número de chamado).
 - Data e hora de abertura do chamado (registro).
 - Descrição do problema.
 - Identificação do reclamante (nome e telefone).
 - Data e hora de conclusão do atendimento (fechamento do chamado).
 - Ações realizadas para a solução do problema.

12. GERENCIAMENTO PROATIVO

A CONTRATADA deverá prover o gerenciamento proativo, com funcionamento 24 horas por dia, 7 (sete) dias na semana, incluindo sábados, domingos e feriados. Entende-se por gerenciamento proativo a capacidade da CONTRATADA de detectar falhas ocorridas nos circuitos (serviços e equipamentos) de forma autônoma e independentemente de notificação por parte da CONTRATANTE. Da mesma forma autônoma a CONTRATADA deve dar início aos procedimentos de correção de falhas e em seguida informar a CONTRATANTE sobre o evento. A CONTRATADA deverá notificar a CONTRATANTE através de telefones e e-mails definidos pela CONTRATANTE no prazo máximo de 25 minutos após a identificação do incidente.

- Gerência exclusiva de relacionamento para acompanhamento, apresentação da evolução e gestão da rede, que fará mensalmente o agendamento e apresentação dos relatórios, através de videoconferência ou por e-mail.
- Atividades realizadas pela equipe responsável pelo gerenciamento proativo:
 - a) Gerenciamento individualizado da rede.
 - b) Relatórios mensais sobre a performance da rede.
 - c) Relatório Gráfico de indisponibilidade.
 - d) Relatório de tráfego de qualidade.
 - e) Relatório de Consumo de Banda.
 - f) Relatório de Eventos ocorridos.
 - g) Relatório de Disponibilidade dos serviços.
 - h) Gerenciamento de desempenho proativo.

13. DISPONIBILIDADE

- Índice de Disponibilidade:
- Os circuitos de comunicação deverão estar disponíveis 24 horas por dia, todos os dias do ano.
- A CONTRATADA deverá garantir disponibilidade mensal de no mínimo, 99,5% para cada circuito fornecido à CONTRATANTE, calculada da seguinte forma:

$$\text{DMA} = \frac{[(43200 - \text{TTICM}) / 43200] \times 100}{}$$

Onde:

TTICM: Tempo Total de Interrupção do Circuito (em minutos) no Mês.

DMA(%): Disponibilidade Mensal Atingida

- Para efeito de cálculo de TTICM, será considerado o período em minutos entre o primeiro minuto do primeiro dia e o último minuto do último dia do calendário do mês a que se refere a fatura.
- O serviço será considerado indisponível quando não for possível a conexão entre o equipamento da CONTRATANTE e o da CONTRATADA, a partir do registro do chamado técnico na Central de Atendimento da CONTRATADA, sendo considerado disponível após o fechamento do chamado técnico, com a devida anuência da CONTRATANTE, na Central de atendimento da CONTRATADA.
- Entende-se como início do atendimento a primeira mensagem trocada pela CONTRATANTE com a CONTRATADA informando a ocorrência ou início da ligação efetuada a central de atendimento da CONTRATADA independentemente do atendimento do operador.
- O prazo máximo de recuperação dos circuitos será 2 (duas) horas, todos os dias do mês, inclusive sábados, domingos e feriados.
- As indisponibilidades informadas pela gerência e supervisão da CONTRATADA, bem como os registros na Central de Atendimento da CONTRATADA serão validadas pelos sistemas de gerência e supervisão da CONTRATANTE.
- No caso de interrupção programada por necessidade da CONTRATANTE, a mesma não afetará o índice de disponibilidade da CONTRATADA.
- As interrupções programadas solicitadas pela CONTRATANTE serão previamente combinadas com a CONTRATADA.

14. DESCONTO POR INTERRUPÇÃO:

- Para cada interrupção do circuito que for comprovadamente de responsabilidade da CONTRATADA, será calculado um desconto referente ao tempo de interrupção desse circuito, cujo valor apurado será ressarcido à CONTRATANTE na Nota Fiscal/Fatura dos serviços com vencimento no mês seguinte ao da apuração.
- O valor do desconto será obtido a partir do seguinte cálculo:

$$VD = (VC / 43200) \times n$$

Onde:

VD = Valor do Desconto

VC = Valor mensal pago pelo circuito ativo

n = Quantidade de minutos em que o serviço ficou interrompido.

- **NÍVEIS MÍNIMOS DE SERVIÇO**

A CONTRATADA deverá fornecer o serviço com os seguintes níveis mínimos de disponibilidade, latência e taxa máxima de erro, os quais são utilizados para mensurar o desempenho e a qualidade dos circuitos:

Métrica	Nível Mínimo de Serviço
Disponibilidade do circuito IP	$\geq 99,5\%$
Latência	$\leq 1\text{ms}$
Perda de pacotes	$\leq 2\%$

DA VINCULAÇÃO À PROPOSTA E TERMO DE REFERÊNCIA

A CONTRATADA deverá ainda executar os serviços conforme especificações constantes no Termo de Referência do Processo Seletivo em referência e da proposta apresentada, que passam a integrar o presente contrato.

QUADRO 04 – DOS VALORES

CONDIÇÕES DE PAGAMENTO: Os serviços serão pagos de forma mensal.

VALOR MENSAL: R\$ XXX

VALOR TOTAL DA CONTRATAÇÃO: A contratação se refere a um valor total de xxx considerando o tempo previsto do contrato de 12 (doze) meses podendo este valor variar para mais ou para menos desde que devidamente justificável.

QUADRO 05 – CONTEÚDO DA NOTA FISCAL

CONTRATO DE GESTÃO Nº 1095/2018 –SEL

CONTRATO DE NA PRESTAÇÃO DE SERVIÇOS DE INTERNET

PERÍODO DE COMPETÊNCIA

SERVIÇO PRESTADO NO HOSPITAL MUNICIPAL DE APARECIDA DE GOIÂNIA – HMAP

As partes, devidamente qualificadas no **Quadro 01**, resolvem de comum acordo celebrar o presente instrumento nos seguintes termos e condições.

CLÁUSULA 1ª

A **CONTRATADA** obriga-se a prestação dos serviços discriminados e nas condições estabelecidas no **Quadro 03**, obrigando-se a **CONTRATANTE** a efetuar o pagamento dos serviços nos valores convencionados no **Quadro 04**. Tudo nos termos do termo de referência e da proposta da **CONTRATADA**, que são parte integrante do presente instrumento de ajuste.

CLÁUSULA 2ª

São obrigações da **CONTRATANTE**:

- a) Efetuar o pagamento no prazo estabelecido, observando-se a totalidade ou parcialidade dos serviços prestados.
- b) Prestar as informações necessárias para o melhor cumprimento deste Contrato.
- c) Exigir a observação das normas emanadas pelos órgãos de fiscalização e controle.
- d) Glosar do valor contratado eventuais prejuízos causados pela **CONTRATADA**, empregados e prepostos, de qualquer natureza, bem como valores decorrentes de passivos trabalhistas e fiscais gerados e não adimplidos pela **CONTRATADA**.

2.2 A CONTRATANTE deverá aplicar, em caso de inexecução total ou parcial das obrigações inerentes à **CONTRATADA**:

- I. Advertência;
- II. Multa no valor 10% do valor mensal do contrato ou valor do bloco (se for o caso).
- III. Suspensão temporária da participação em outros processos seletivos no máximo de 06 (seis) meses, desde que já tenha havido aplicação da sanção prevista no inciso I por pelo menos duas vezes.

2.3. Será garantida a prévia defesa

CLÁUSULA 3ª

São obrigações da **CONTRATADA**:

- a) Prestar serviços, dentro dos padrões de qualidade e eficiência exigidos para o serviço e nos dispositivos legais e convencionais impostos.
- b) Respeitar, por si e por seus prepostos, as normas atinentes ao funcionamento da unidade e aquelas relativas ao objeto do presente Contrato.
- c) Não transferir a terceiros, por qualquer forma, nem mesmo parcialmente, o objeto do presente instrumento, nem subcontratar quaisquer das prestações a que está obrigada. **Salvo mediante anuência expressa da Contratante quanto aos termos do ajuste.**
- d) Promover a cobrança dos valores decorrentes do presente contrato somente após o respectivo vencimento e da demonstração do repasse dos valores por parte do Poder Público subscritor do Contrato de Gestão.
- e) Responder por qualquer prejuízo que seus empregados ou prepostos causarem ao patrimônio da unidade ou a terceiros, decorrente de ação ou omissão culposa ou dolosa, procedendo imediatamente os reparos ou indenizações cabíveis e assumindo o ônus decorrente.
- f) Manter no curso do contrato a sua regularidade fiscal e qualificação técnica exigível para o desempenho do objeto contratual
- g) Manter o mais absoluto sigilo e confidencialidade no tocante aos serviços, documentos, pesquisas, entrevistas e demais informações apuradas ou de que tome conhecimento durante a relação contratual.
- h) Sanar eventuais irregularidades ou correções apontadas pela CONTRATANTE quanto à apresentação de relatórios e/ou de cada etapa dos serviços.
- i) Providenciar a emissão de notas fiscal de acordo com os termos contratados, **até o dia 25** do mês da efetiva prestação do serviço, no qual deverá vir instruído com os seguintes documentos, sob pena de retenção do pagamento até regularização: 1 - Certidões de Regularidades Fiscais Federais (Conjunta, CRF e Previdenciária), 2 - Municipal (ISSQN), 3 - Estadual (ICMS), 4 - Trabalhista (TST), 5 - comprovante de recolhimento do INSS e empregados, 6 – comprovante de recolhimento do FGTS dos empregados, 7 – registro de frequência dos empregados e dos sócios caso esses sejam executores da prestação de serviços, 8 – comprovante de quitação da folha de pagamento do mês trabalhado e de referência à nota fiscal emitida, 9 – relatório de produção ou relatório de serviços prestados (papel timbrado da CONTRATADA, assinatura do sócio ou representante legal).
- j) Impedir o acesso à unidade de pessoa que não seja membro de seu corpo técnico com o fim de trabalhar, estagiar ou realizar qualquer atividade similar.
- k) Prestar esclarecimentos no prazo designado pela CONTRATANTE em relação a qualquer procedimento de sua responsabilidade e subordinar-se às sindicâncias instauradas para averiguação de qualquer fato que tenha participado ou tenha conhecimento.
- l) Acatar as glosas, sem prejuízos de advertências, caso os serviços estejam em desacordo com o contratado.
- m) Cumprir de forma integral e satisfatória tudo o que consta no Termo de Referência, bem como a proposta apresentada no certame.

PARÁGRAFO ÚNICO – A perda da regularidade fiscal e/ou trabalhista no curso deste contrato, ensejará a retenção dos pagamentos até que a situação seja regularizada.

CLÁUSULA 4ª

Os serviços prestados pela **CONTRATADA** serão pagos mensalmente e de acordo com o convencionado no **Quadro 04**.

§ 1ª – Não serão efetuados quaisquer pagamentos enquanto perdurar pendência de liquidação de obrigações impostas à **CONTRATADA** ou inadimplência contratual.

§ 2ª – Os pagamentos serão realizados unicamente por meio de depósito bancário, não sendo aceito pagamentos das faturas ou boletos bancários.

§ 3ª – O pagamento será efetuado em até 30 (trinta) dias, contados a partir do aceite da Nota Fiscal correspondente, desde que tenha havido o repasse do **Contrato de Gestão n .1095/2018 -SEL** referente ao mês da efetiva prestação de serviços por parte da Município de Aparecida de Goiânia por intermédio do Fundo Municipal de Saúde, e estará condicionado ao cumprimento integral dos serviços

§ 4ª –As Notas Fiscais deverão especificar em seu descritivo o conteúdo demonstrado no **Quadro 05** sob pena de retenção do pagamento até regularização.

§ 5ª – Do pagamento efetuado a empresa contratada serão calculados e deduzidas as retenções tributárias correspondentes conforme o tipo de serviço e o local onde esta sendo prestado.

§ 6ª – Para o caso específico do ISSQN caberá à **CONTRATADA** observar a legislação do município da prestação dos serviços.

CLÁUSULA 5ª

O contrato poderá ser reajustado ou aditivado a qualquer tempo, em razão da necessidade e sua devida comprovação justificada ou conveniência de continuação da prestação dos serviços, a partir de negociação acordada entre as partes, devidamente justificada mediante aditivo expresso.

PARÁGRAFO PRIMEIRO: Os índices de reajuste serão previstos no Termo de Referência, e na inércia da previsão será adotado o índice IGPM ou quando não aplicável será aquele que seja mais benéfico à CONTRATANTE. Os índices só poderão ser concedidos somente após 12 (doze) meses de vigência.

PARÁGRAFO SEGUNDO: Nas hipóteses de aditivos qualitativos e quantitativos serão obedecidas as seguintes regras:

- a) **Manutenção da natureza do objeto do contrato;**
- b) **Manutenção das mesmas condições contratuais.**

CLÁUSULA 6ª

O fiscal do Contrato designado pela **CONTRATANTE**, atestará a aceitação da entrega do serviço prestado e promoverá o aceite da nota fiscal observados os requisitos estabelecidos neste contrato, inclusive em relação ao cumprimento das metas e serviços contratados.

CLÁUSULA 7ª

Constituem motivos de rescisão unilateral pela **CONTRATANTE**:

- a) O cumprimento parcial ou o não cumprimento dos serviços contratados e ou fornecimento parcial dos produtos adquiridos.
- b) A desobediência de cláusulas contratuais, especificações e prazos pela CONTRATADA, ou a lentidão do seu cumprimento.
- c) Atraso injustificado no início dos serviços.
- d) Paralisação dos serviços.
- e) O cometimento de falhas na execução do objeto do contrato.
- f) Término do Contrato de Gestão, sem direito a qualquer indenização a **CONTRATADA**.
- g) Ineficiência na execução do objeto contratual.

PARÁGRAFO PRIMEIRO - Nos casos em que haja descumprimento total ou parcial do objeto deste contrato a

CONTRATANTE notificará a CONTRATADA para apresentar justificativa ou sanar as deficiências no prazo máximo de 02 (dois) dias úteis, sob pena de não o fazendo o contrato ser rescindido de plano, independentemente de qualquer outra notificação.

PARÁGRAFO SEGUNDO – Garantida a defesa prévia da CONTRATADA, a CONTRATANTE poderá, além de outras medidas tendentes a regularização do contrato:

- a) Aplicar advertência;
- b) Suspender a execução contratual;
- c) Rescindir o contrato;
- d) Impedir mediante justificativa a CONTRATANTE de participar de novos processos seletivos por 06 (seis) meses.

CLÁUSULA 8ª

Poderão **AMBAS AS PARTES** sem justo motivo rescindir o presente contrato notificando com antecedência de **30 (trinta) dias**.

PARÁGRAFO PRIMEIRO: Este contrato será obrigatoriamente rescindido em caso de término do contrato de gestão.

PARÁGRAFO SEGUNDO: Caso a CONTRATANTE dispense os serviços a serem prestados durante os 30 (trinta) dias referenciados no caput, a CONTRATADA somente terá direito ao pagamento indenizatório dos referidos dias desde efetivamente preste os serviços de acordo com a manifestação do fiscal do contrato.

CLÁUSULA 9ª

A **CONTRATADA** por si e por seus sócios, administradores, gestores, representantes legais, empregados, prepostos e subcontratados (“Colaboradores”), se compromete a adotar os mais altos padrões éticos de conduta na condução dos seus negócios e não pagar, prometer ou autorizar o pagamento de qualquer valor ou oferecer qualquer tipo de vantagem indevida direta ou indiretamente, a qualquer Funcionário Público ou a terceira pessoa, bem como garante que não emprega e não empregará, direta ou mediante contrato de serviços ou qualquer outro instrumento, trabalho escravo, trabalho infantil.

CLÁUSULA 10ª

A **CONTRATADA** declara, sob as penas da lei, que não esteve envolvida com qualquer alegação de crime de lavagem de dinheiro, delito financeiro, financiamento de atividades ilícitas ou atos contra a Administração Pública, incluindo, mas não se limitando a corrupção, fraude em licitações, suborno ou corrupção e que durante a prestação dos serviços ora avençado, cumprirá com todas as leis aplicáveis à natureza dos serviços contratados, em especial a Lei de Improbidade Administrativa e Lei Brasileira Anticorrupção.

CLÁUSULA 11ª

Havendo inadimplência no repasse financeiro do Contrato de Gestão em referência pelo o ente Público, que inviabilize alguma atividade do contrato temporariamente, será permitida a **SUSPENSÃO** temporária e por prazo indeterminado do presente contrato, a critério do CONTRATANTE, sem direito a qualquer indenização reparatória.

PARÁGRAFO ÚNICO: A Suspensão deve ser expressamente comunicada à outra parte, com exposição dos motivos que a ensejaram, estabelecendo as partes que a simples correspondência, mediante recibo, ou envio por e-mail é suficiente para tanto.

CLÁUSULA 12ª

Fica acordado entre as partes que qualquer documentação administrativa ou judicial somente terá validade se encaminhada para o seguinte endereço: **Rua Av. Areião, Qd. 17, Lt. 23, CEP: 74820-370, Setor Pedro Ludovico, Goiânia – Goiás.**

CLÁUSULA 13ª

As partes se comprometem a agir de modo leal, responsável e probo, atuando com boa-fé para repelir quaisquer ações intencionalmente desleais, injustas, desonestas, prejudiciais, fraudulentas ou ilegais, sempre ancorados nas ações de transparência pública.

CLÁUSULA 14ª

Para dirimir as questões oriundas do presente contrato é competente o Foro da Comarca de Goiânia (GO).

Para firmeza e como prova de haverem entre si, justos e avençados, e depois de lido e achado conforme, as partes assinam o presente Contrato, em 03 (três) vias de igual teor e forma.

Goiânia (GO), ____ de _____ de 2019.

CONTRATANTE	CONTRATADA
<p>_____</p> <p>ESTÊVÃO COSTA DALTRO</p> <p>SUPERINTENDENTE</p> <p>INSTITUTO BRASILEIRO DE GESTÃO HOSPITALAR- IBGH</p>	<p>_____</p> <p>xxx</p>