**TERMO DO CONTRATO DE PRESTAÇÃO DE SERVIÇO – CONTRATO Nº CRT.0021/2022, RELATIVO À PRESTAÇÃO DE SERVIÇOS DE INSTALAÇÃO, MANUTENÇÃO, SUPORTE TÉCNICO E IMPLEMENTAÇÃO DE SOLUÇÃO DE SEGURANÇA E CONTROLE DE ACESSO A REDE DE COMPUTADORES ATRAVÉS DE APPLIANCE DE CONTROLE UNIFICADO (FIREWALL), QUE ENTRE SI FIRMAM O CONSELHO REGIONAL DE FARMÁCIA DO ESTADO DE SÃO PAULO – CRF-SP E A EMPRESA ASSISNET SERVIÇOS DE INFORMÁTICA LTDA.**

O **CONSELHO REGIONAL DE FARMÁCIA DO ESTADO DE SÃO PAULO (CRF-SP)**, Autarquia instituída pela Lei Federal nº 3.820, de 11 de novembro de 1960, inscrita no CNPJ/MF sob o nº 60.975.075/0001-10, com sede na Rua Capote Valente, 487, Jardim América, São Paulo/SP, CEP 05.409-001, neste ato representado por seu Presidente, Dr. Marcelo Polacow Bisson, brasileiro, [redacted], farmacêutico, portador da cédula de identidade RG n° [redacted], inscrito no CPF/MF sob o n° [redacted] e no CRF-SP sob n° 13.573, e por sua Diretora Tesoureira, Dra. Danyelle Cristine Marini, brasileira, [redacted], farmacêutica, portadora da cédula de identidade RG n° [redacted], inscrita no CPF/MF sob o n° [redacted] e no CRF-SP sob n° 25.937, doravante simplesmente denominado **CONTRATANTE**, e do outro lado a empresa **ASSISNET SERVIÇOS DE INFORMÁTICA LTDA**, inscrita no CNPJ/MF sob o nº 73.558.934/0001-17, com sede na Avenida Marques de São Vicente, 446, 19º andar, conjunto 1.904, Barra Funda, São Paulo/SP, CEP 01.139-000, representada por seu sócio, Sr. José Roberto Consani, brasileiro, [redacted], empresário, portador da cédula de identidade RG nº [redacted] inscrito no CPF/MF sob o nº [redacted], residente e domiciliado na [redacted], adiante denominada **CONTRATADA**, têm certo e ajustado o presente contrato, o qual será regido pelas cláusulas e condições a seguir descritas, com inteira submissão às disposições legais que regem a espécie, especialmente à Lei nº 8.666, de 21 de junho de 1993.

Este contrato foi precedido de licitação, na modalidade **PREGÃO**, observados os dispositivos da Lei nº 10.520, de 17 de julho de 2002, do Decreto nº 3.555, de 8 de agosto de 2000, Decreto nº 5.450, de 31 de maio de 2005, Decreto nº 10.024, de 20 de setembro de 2019, e subsidiariamente, pela Lei nº 8.666, de 21 de junho de 1993, vinculando-se ao Processo Administrativo nº 039/2022 e Pregão Eletrônico nº 033/2022.

## 1. DO OBJETO

1.1. O presente contrato tem por objeto a contratação de empresa especializada na prestação de serviços, instalação, manutenção, suporte técnico e implementação de solução de segurança e controle de acesso a rede de computadores através de appliance de controle unificado (firewall), para o Conselho Regional de Farmácia do Estado de São Paulo – CRF-SP, conforme condições, quantidades e exigências estabelecidas neste contrato.

1.1.1. ITEM 01 – Demais serviços a serem prestados após a homologação, conforme descrito no contrato, incluindo a manutenção e suporte técnico da solução de segurança e controle de acesso a rede de computadores através de appliance de controle unificado (firewall).

1.1.2. ITEM 02 – Serviço de implantação (instalação, configuração, implementação etc) que possibilite a homologação da solução ofertada.

## 2. DESCRIÇÃO DETALHADA DO OBJETO

2.1. Disponibilização de Solução de Segurança em Firewall contemplando:

2.1.1. Disponibilização de Solução de Segurança em Firewall com as especificações técnicas mínimas a seguir e em High Availability (HA), durante o período do contrato;

2.1.2. Eventuais acessórios ou equipamentos necessários para o funcionamento da Solução de Segurança, como cabos, conectores, suportes, fixadores e demais componentes para o correto funcionamento do item acima, deverão ser disponibilizados pela contratada durante todo o período do contrato;

2.1.3. Deverá acompanhar todo licenciamento necessário para acesso, consulta, update e upgrade a base de conhecimento e assinaturas de ameaças do fabricante da solução para as funcionalidades mínimas

Escaneie a imagem para verificar a autenticidade do documento

de antivírus de gateway, Anti-Spyware de gateway, IPS (Intrusion Prevention system), filtro de conteúdo, geração de relatórios, entre outras funcionalidades durante o período do contrato.

2.2. Serviços continuados da solução pelo período de 30 meses sendo disponibilizado por profissional certificado que deverá observar:

2.2.1. Monitoramento de funcionamento da solução;

2.2.2. Monitoramento de consumo de recursos da solução (memória, processador e outras funcionalidades);

2.2.3. Monitoramento de conectividade dos links de internet conectados à Solução;

2.2.4. Alteração de políticas de acesso, controle de funcionalidades, IPS e filtro de conteúdo.

2.2.5. Diagnóstico de possíveis ataques;

2.2.6. Validação das atualizações de assinatura;

2.2.7. Validação da sincronização do Cluster HA;

2.2.8. Verificação das políticas de load balance com alteração caso necessário;

2.2.9. Configuração de rotas avançadas de acordo com a demanda do cliente;

2.2.10. Implementação de novas VPNs (client-to-site e site-to-site);

2.2.11. Suporte técnico 24x7.

2.3. GERAÇÃO DE RELATÓRIOS:

2.3.1. Utilização de banda de internet por link;

2.3.2. Consumo de banda por top users;

2.3.3. Consumo de tráfego web geral;

2.3.4. Consumo de tráfego web por usuários;

2.3.5. Consumo de tráfego web por serviços;

2.3.6. Sites mais acessados por usuários (segmentado por URL);

2.3.7. Lista de sites acessados segmentados por usuário;

2.3.8. Consumo de banda por e-mail;

2.3.9. Consumo de banda por VPN;

2.3.10. Lista de ataques;

2.3.11. Listas de tentativas de invasão por vírus;

2.3.12. Listas de tentativas de invasão por spyware.

2.3.13. Os relatórios com o histórico de acesso à internet deverão permanecer acessíveis por pelo menos 12 meses e armazenados nos equipamentos da contratada.

2.4. IMPLANTAÇÃO ÚNICA A SER EXECUTADA NO INÍCIO DO CONTRATO.

2.4.1. Definição das políticas de segurança junto ao cliente;

Escaneie a imagem para verificar a autenticidade do documento

2.4.2. Instalação física dos appliances;

2.4.3. Configuração do Cluster HA;

2.4.4. Instalação do sistema de gerenciamento e relatórios;

2.4.5. Configuração das políticas de Failover dos links de internet;

2.4.6. Configuração da integração da solução ao sistema de autenticação Active Directory do cliente;

2.4.7. Aplicação das políticas de segurança;

2.4.8. Implementação de VPN (client-to-site e site-to-site);

2.4.9. Repasse de conhecimento na operação básica da ferramenta de administração para equipe de até 5 pessoas.

2.5. REQUISITOS MÍNIMOS

2.5.1. Desempenho em modo Threat Prevention (Proteção Anti-Malware, IPS e Controle de Aplicação habilitados) mínimo de 3.5 Gbps ou superior.

2.5.2. Desempenho em modo de Inspeção (decriptografia e criptografia) de tráfego criptografado (SSL/TLS) mínimo de 850 Mbps. Os desempenhos solicitados devem ser comprovados por documento de domínio público do fabricante. Não serão aceitas declarações ou cartas de fabricantes para atendimento deste item.

2.5.3. Desempenho mínimo de 3.8 Gbps de IPS.

2.5.4. Suporte mínimo de 2.000.000 conexões simultâneas/concorrentes no modo SPI.

2.5.5. Suporte mínimo de 22.000 novas conexões por segundo.

2.5.6. Deve possuir armazenamento interno de no mínimo 128 GB e suportar expansão de armazenamento interno para até 256GB.

2.5.7. Deve possuir fonte de alimentação com chaveamento automático de 100-240 VAC.

2.5.8. Deve possuir 24 interfaces 1 GbE padrão RJ-45.

2.5.9. Deve possuir 6 interfaces 10GbE SFP+ e 4 interfaces 1GbE SFP.

2.5.10. Deve possuir 1 do tipo 1 GbE RJ-45 dedicada para gerenciamento do equipamento.

2.5.11. Deve possuir 2 interfaces USB 3.0 com suporte a tecnologias LTE 3G/4G e 5G.

2.5.12. A VPN Client-to-Site IPsec deve ser licenciada para, no mínimo, 50 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 1000 usuários simultâneos, com aquisição de licença complementar.

2.5.13. A VPN SSL deve ser licenciada para, no mínimo, 2 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 500 usuários simultâneos, com aquisição de licença complementar.

2.5.14. Deve suportar 2800 túneis de VPN tipo Site-to-Site padrão IPSEC simultâneos.

2.5.15. Deve suportar, no mínimo, 2.1 Gbps de desempenho de VPN IPSEC.

Escaneie a imagem para verificar a autenticidade do documento

2.5.16. Os desempenhos apontados devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste contrato. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, o fornecedor será considerado inabilitado. Todos os custos oriundos do teste de bancada serão custeados pelo fornecedor/vendedor do certame.

2.5.17. O fornecimento da solução e de seus licenciamentos devem ser entregues através de empresa credenciada e autorizada pelo fabricante. Isto deve ser comprovado através de carta de reconhecimento assinada pelo representante legal do fabricante no Brasil.

2.5.18. O Equipamento deverá ser homologado pela ANATEL.

2.5.19. Não serão aceitas cartas ou declarações de fabricantes para atendimento aos valores de desempenho solicitados.

2.5.20. O licenciamento para todos os serviços deverá ser de no mínimo 30 meses.

2.5.21. A garantia e suporte da solução deverá ser de no mínimo 30 meses.

2.6. CARACTERÍSTICAS GERAIS

2.6.1. A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall. O termo Next Generation Firewall doravante será empregado como NGFW ou simplesmente FIREWALL.

2.6.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, prevenção de ataques zero-day, filtro de URL, identificação de usuários e controle granular de permissões.

2.6.3. Para proteção do ambiente contra-ataques, o dispositivo de proteção deve possuir módulos de IPS, Antivírus e Anti-Spyware (para bloqueio de arquivos maliciosos), integrados ao próprio appliance de NGFW.

2.6.4. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.

2.6.5. Define-se o termo “appliance” como sendo um equipamento dotado de processamento, memória e outros recursos tecnológicos exclusivos para um determinado serviço.

2.6.6. Não serão aceitas soluções baseadas em PC's (personal computers) de uso geral, assim como, soluções de “appliance” que utilizam hardware e software de fabricantes diferentes.

2.7. CARACTERÍSTICAS DIVERSAS

2.7.1. Deve implementar controle do tráfego para os protocolos TCP, UDP, ICMP, e serviços como FTP, DNS, P2P entre outros, baseados nos endereços de origem e destino.

2.7.2. Implementar recurso de NAT (network address translation) tipo one-to-one, one-to-many, many-to-many, many-to-one, porta TCP de conexão (NAPT) e NAT Traversal em VPN IPSec (NAT-T) e NAT dentro do túnel IPSec.

2.7.3. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico.

2.7.4. Deve possuir proteção anti-spoofing.

2.7.5. Suportar protocolos de roteamento RIP, RIPng, OSPF, OSPFv3 e BGP;

2.7.6. Suportar Equal Cost Multi-Path (ECMP) no mínimo para roteamento estático e protocolo OSPF.

Escaneie a imagem para verificar a autenticidade do documento

2.7.7. Suporte a Policy-Based Routing (PBR), com a capacidade de roteamento no mínimo, mas não limitado a: endereço de origem, endereço de destino, serviço e aplicação.

2.7.8. A solução deverá implementar tecnologia de SD-WAN (Software Defined WAN).

2.7.9. Capacidade de agregar no mínimo 4 (quatro) circuitos WAN distintos em um único canal lógico onde seja possível criar controles de caminho automático baseado em políticas, com habilidade de selecionar o melhor caminho, no mínimo, através dos seguintes parâmetros simultâneos:

2.7.9.1. Latência;

2.7.9.2. Jitter;

2.7.9.3. Perda de pacotes.

2.7.10. O administrador da solução deverá ter a capacidade de configurar o canal lógico de SD-WAN para encaminhar tráfego simultaneamente por todos os links pertencentes a esse canal lógico.

2.7.11. A comutação do SD-WAN deve ocorrer de maneira dinâmica e automática baseada nas políticas previamente aplicadas.

2.7.12. A solução de SD-WAN deve permitir encaminhamento de tráfego com base em assinaturas de aplicações conhecidas (DPI), como Office 365, Facebook e Youtube, bem como aplicações associadas como Facebook Messenger e Office 365 Outlook.

2.7.13. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.

2.7.14. Deve suportar modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.

2.7.15. Implementar proxy transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes.

2.7.16. Possuir servidor de DHCP (Dynamic Host Configuration Protocol) interno com capacidade de alocação de endereçamento IP para as estações conectadas às interfaces do firewall e via VPN.

2.7.17. Deve suportar DHCP relay.

2.7.18. Possibilitar a aplicação de regras de firewall e IPS por IP e grupo de usuários, permitindo a definição de regras para determinado horário ou período (dia da semana e hora) com matriz de horários que possibilite o bloqueio de serviços em horários específicos, tendo o início e fim das conexões vinculadas a essa matriz de horários.

2.7.19. Deve permitir a utilização de regras de Anti-Vírus, Anti-Spyware, IPS e filtro de conteúdo web por segmentos de rede. Todos os serviços devem ser suportados no mesmo segmento de rede, VLAN ou zona de segurança.

2.7.20. Possuir capacidade de inspecionar e bloquear em tempo real aplicativos e transferências de arquivos de softwares p2p (peer-to-peer) incluindo, no mínimo, Kazaa, Limewire, Morpheus e Napster e de comunicadores instantâneos (instant messengers) incluindo, no mínimo, ICQ, WhatsApp, Google Talk, Skype e IRC, para usuários da rede, individualmente ou em grupo.

2.7.21. Deve ter suporte à proteção e identificação de hosts possivelmente infectados com “botnets”. A solução ofertada deve permitir ao administrador a possibilidade de apenas registrar e identificar as máquinas possivelmente contaminadas, além de ter a possibilidade de habilitar e analisar todas as conexões que passam por este dispositivo de segurança, bem como ativar tal funcionalidade especificando análise por regra de firewall, permitindo assim maior granularidade da gestão e do recurso.

2.7.22. Possuir assinaturas específicas, ou implementar mecanismo interno no appliance, para mitigação de ataques DoS (denial-of-service) e DDoS devidamente licenciados.

Escaneie a imagem para verificar a autenticidade do documento

2.7.23. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc.

2.7.24. Detectar e bloquear a origem de portscans.

2.7.25. Deve permitir o bloqueio de ataques.

2.7.26. Deve permitir o bloqueio de exploits conhecidos.

2.7.27. O gateway Anti-Vírus deve suportar a análise de pelo menos os protocolos HTTP, FTP, IMAP e SMTP.

2.7.28. Deve ter a capacidade de analisar tráfegos criptografados HTTPS/SSL, que deverá ser decriptografado de forma transparente à aplicação.

2.7.29. Implementar DSCP (Differentiated Services Code Points).

2.7.30. Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP, SIP, RTP, RTSP e H323, mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para acessos de dentro para fora quanto de fora para dentro da rede.

2.7.31. Implementar controle e gerenciamento de banda para a tecnologia VoIP (Voice OverIP) sobre diferentes segmentos de rede com inspeção profunda de segurança sobre este serviço.

2.7.32. Implementar mecanismo de sincronismo de horário através do protocolo NTP.

2.7.33. Possuir suporte ao protocolo SNMP versões 2 e 3.

2.7.34. Possuir suporte a log via syslog.

2.7.35. Possuir suporte aos protocolos de roteamento RIP, OSPF e BGP. As configurações de RIP e OSPF devem ser configuradas através da interface gráfica.

2.7.36. O fabricante ou a solução devem possuir certificado ICSA (International Computer Security Association) para FIREWALL, ou CC (Common Criteria). Será aceito certificado equivalente ao ICSA, emitido por órgãos nacionais com competência para tal, desde que nos moldes deste, ou seja, certificado baseado na versão ou release atual do firewall, com manutenção recorrente deste certificado a cada mudança de versão, ou após determinado período de tempo, e baseado em normas nacionais e internacionais de segurança da informação.

2.7.37. Visando estabelecer efetividade de segurança dos firewalls de nova geração e assegurar que o fornecedor tenha uma solução já testada e comprovada por um órgão independente de mercado, o fabricante da solução deverá ser avaliado e certificado pelo NetSecOPEN, além de ser avaliado e citado pelo Gartner MQ (Magic Quadrant for Network Firewalls) nos relatórios de 2022 ou mais recentes.

2.7.38. Reconhecer aplicações como, no mínimo, peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos e e-mail.

2.7.39. Para tráfego criptografado SSL/TLS, deve de-criptografar pacotes possibilitando a leitura de payload dos pacotes para checagem de assinaturas de aplicações conhecidas pelo fabricante.

2.7.40. Controle, inspeção e decriptografia de SSL/TLS por política para tráfego de entrada (Inbound) ou Saída (Outbound) com suporte a no mínimo, SSLv23, SSLv3, TLS 1.0, TLS 1.1, TLS 1.2 e TLS 1.3.

2.8. CARACTERÍSTICAS DE VPN

Escaneie a imagem para verificar a autenticidade do documento

Escaneie a imagem para verificar a autenticidade do documento

2.8.1. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site, com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.

2.8.2. Suportar algoritmos de criptografia 3DES, AES 128 e AES 256.

2.8.3. Suportar algoritmos Hash no mínimo SHA-1, SHA-256 e SHA-384.

2.8.4. Diffie-Hellman: Grupo 2 (1024 bits), Grupo 5 (1536 bits) e Grupo 14 (2048 bits.

2.8.5. Deverá suportar algoritmo Internet Key Exchange (IKE) v1 e v2.

2.8.6. Autenticação via de tuneis IPSec via certificado digital para VPNs Site-to-Site e Client-to-Site.

2.8.7. A solução deve suportar VPNs L2TP, incluindo suporte para Apple iOS e Android.

2.8.8. Solução deve suportar VPNs baseadas em políticas, e VPNs baseadas em roteamento estático e/ou dinâmico.

2.8.9. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo Site-to-Site com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.

2.8.10. Solução deve incluir a capacidade de estabelecer VPNs com outros firewalls que utilizam IP públicos dinâmicos.

2.8.11. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do circuito primário.

2.8.12. Permitir criação de políticas de roteamento estático utilizando IPs de origem, destino, serviços e a própria VPN como parte encaminhadora deste tráfego, sendo este visto pela regra de roteamento como uma interface simples de rede para encaminhamento do tráfego.

2.8.13. Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet.

2.8.14. Implementar os esquemas de troca de chaves manual, IKE e IKEv2 por Pré-Shared Key, certificados digitais e XAUTH client authentication.

2.8.15. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do primário.

2.8.16. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

2.9. ALTA DISPONIBILIDADE

2.9.1. Deve ser fornecida uma solução que contemple no mínimo 02 (dois) appliances de NGFW com gerenciamento unificado, novos e sem uso anterior, funcionando em alta disponibilidade. A solução ofertada deverá estar em linha de produção, sem previsão de encerramento de fabricação, na data de entrega da proposta. O licenciamento deverá ser fornecido em sua versão mais atualizada.

2.9.2. A solução deve ser entregue operando em alta disponibilidade no modo Ativo/Standby, com as implementações de Failover.

2.9.3. Não serão permitidas soluções de cluster (HA) que façam com que os equipamentos se reiniciem após qualquer modificação de parâmetro/configuração realizada pelo administrador.

2.9.4. A solução deve ter capacidade de fazer monitoramento físico das interfaces dos membros do cluster.

2.9.5. A solução deve operar em alta disponibilidade implementando monitoramento lógico de um host na rede, e possibilitar failover.

2.9.6. A solução deve permitir o uso de endereço MAC virtual para evitar problemas de expiração de tabela ARP em caso de Failover.

2.9.7. A solução deve possibilitar a sincronização de todas as configurações realizadas no nó principal do cluster incluído, mas não limitado a objetos, regras, rotas, VPNs e políticas de segurança.

2.9.8. A solução deve permitir visualizar no nó principal, o status da comunicação entre os parceiros do cluster, status de sincronização das configurações, status atual do equipamento redundante.

2.10. CONTROLE DE AMEAÇAS

2.10.1. Para as ameaças de dia-zero, a solução deve ter a habilidade de prevenir o ataque antes de qualquer assinatura ser criada. Deve possuir módulo de Anti-Vírus e Anti-Bot integrado ao próprio appliance de segurança.

2.10.2. A solução de Anti-Virus integrada deve ter capacidade de analisar arquivos maiores que 1GB.

2.10.3. A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliances através de assinaturas.

2.10.4. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego.

2.10.5. Implementar funcionalidade de detecção e bloqueio de “call-backs”.

2.10.6. A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede.

2.10.7. A solução Anti-bot deve possuir mecanismo de detecção que inclua reputação de endereço IP.

2.10.8. Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS.

2.10.9. Implementar interface CLI segura através do protocolo SSH.

2.10.10. Possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado à plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, FTP, CIFS e TCP Stream.

2.10.11. A solução deve permitir criar regras de exceção de acordo com a proteção.

2.10.12. Deve possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts, ou incidentes referentes a vírus e Bots;

2.10.13. Permitir o bloqueio de malwares (vírus, worms, spyware e etc).

2.10.14. A solução deve ser capaz de proteger contra ataques a DNS.

2.10.15. A solução deverá ser gerenciada a partir de uma console centralizada com políticas granulares.

2.10.16. A solução deve ser capaz de prevenir acesso a websites maliciosos.

2.10.17. A solução deve ser capaz de realizar inspeção de tráfego SSL/TLS e SSH.

2.10.18. A solução deverá receber atualizações de um serviço baseado em cloud.

2.10.19. A solução deverá ser capaz de bloquear a entrada de arquivos maliciosos.

Escaneie a imagem para verificar a autenticidade do documento

2.10.20. A solução Anti-Vírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS.

2.10.21. A solução deve suportar funcionalidade de Geo-IP, ou seja, a capacidade de identificar, isolar e controlar tráfego baseado na localização (origem e/ou destino), incluindo a capacidade de configuração de listas customizadas para esta mesma finalidade

2.10.22. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio appliance de firewall, onde sua console de gerência deverá residir na mesma console centralizada dos appliances de segurança, com suporte a pelo menos 3.000 assinaturas;

2.10.23. A solução de IPS deverá possuir os seguintes mecanismos de detecção: assinaturas e trabalhar em conjunto com o controle de aplicações;

2.10.24. A solução de IPS deve fazer a inspeção de todo o pacote, independentemente do tamanho;

2.10.25. A solução de IPS deve fazer a inspeção de todo o tráfego de forma bidirecional, analisando qualquer tamanho de pacote sem degradar a performance do equipamento solicitada neste contrato;

2.10.26. Possuir capacidade de remontagem de pacotes para identificação de ataques;

2.10.27. O mecanismo de inspeção deve receber e implementar em tempo real atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance;

2.10.28. Para cada proteção de segurança, deve ser possível consultar informações no site do fabricante.

2.10.29. A ferramenta de log deve possuir a capacidade de criar uma regra de exceção a partir do log visualizado na gerência centralizada;

2.10.30. As regras de exceção devem possuir: origem, destino e serviço;

2.10.31. A solução deve ser capaz de inspecionar tráfego HTTPS.

2.10.32. Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;

2.10.33. Detecção de anomalias;

2.10.34. A solução de IPS deve possuir política capaz de definir o modo de operação (bloqueio ou detecção);

2.10.35. O módulo de IPS deve possuir assinaturas voltadas para ambientes de servidores de SMTP, Web e DNS;

2.10.36. O mecanismo de inspeção deve receber e implementar em tempo real atualizações de novas assinaturas sem a necessidade de reiniciar o appliance;

2.10.37. Para cada proteção, ou para todas as proteções suportadas, deve incluir a opção de adicionar exceções baseado na origem e destino;

2.10.38. A solução deve ser capaz de detectar e bloquear ataques nas camadas de rede e aplicação, protegendo pelo menos os seguintes serviços: Aplicações web, serviços de e-mail, DNS, FTP, SQL Injection, ataques a sistemas operacionais e VOIP;

2.10.39. Deve incluir proteção contra worms;

2.10.40. Deve incluir uma tela de visualização situacional a fim de monitorar graficamente a quantidade de alertas de diferentes severidades e a evolução ao logo do tempo dispondo o sumário quantitativo das ameaças analisadas.

2.10.41. A solução deve possuir esquema de atualização de assinaturas através de um clique;

Escaneie a imagem para verificar a autenticidade do documento

2.10.42. Atualização de modo offline, onde poder ser baixado na base do fabricante e posteriormente fazer o upload do arquivo na solução;

2.10.43. A solução deve suportar importar certificados de servidor para inspeções de tráfego seguro HTTP (HTTPS) de entrada. Depois de importar esses certificados, a solução deve permitir o IPS para Inspeção segura HTTP (HTTPS);

2.10.44. A solução deverá ser capaz de inspecionar e proteger apenas hosts internos;

2.10.45. A solução deverá possuir proteções para sistemas SCADA;

2.10.46. A solução deverá permitir que o administrador bloqueie facilmente o tráfego de entrada e/ou saída com base em países, sem a necessidade de gerir manualmente os ranges de endereços IP dos países que deseja bloquear.

2.11. PROTEÇÃO CONTRA ATAQUES AVANÇADOS

2.11.1. A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT, com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de “call-backs”.

2.11.2. Suportar os protocolos HTTP assim como inspeção de tráfego criptografado através de HTTPS.

2.11.3. A solução deve ser capaz de inspecionar o tráfego criptografado SSL/TLS e SSH.

2.11.4. Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle.

2.11.5. Implementar mecanismo de bloqueio de vazamento não intencional de dados oriundos de máquinas existentes no ambiente LAN em tempo real.

2.11.6. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF com até 10MB.

2.11.7. Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows e Android.

2.11.8. Conter ameaças de dia zero permitindo ao usuário final o recebimento dos arquivos livres de malware.

2.11.9. A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas.

2.11.10. A solução deve possuir nuvem de inteligência proprietária do fabricante, onde este seja responsável por atualizar toda a base de segurança dos appliance através de assinaturas.

2.11.11. Implementar a visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados.

2.11.12. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e quaisquer outros mecanismos de redirecionamento de tráfego;

2.11.13. Conter ameaças avançadas de dia zero.

2.11.14. Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador.

2.11.15. Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos;

Escaneie a imagem para verificar a autenticidade do documento

2.11.16. Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos.

2.11.17. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx) e Android APKs no ambiente controlado.

2.11.18. Implementar a análise de arquivos executáveis, DLLs e ZIP no ambiente controlado.

2.11.19. Possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, FTP, IMAP e CIFS.

2.11.20. Mitigar ameaças de dia zero de forma transparente para o usuário final.

2.11.21. Mitigar ameaças de dia zero através de tecnologias de emulação e código de registro.

2.11.22. Implementar mecanismo de pesquisa por diferentes intervalos de tempo.

2.11.23. Mitigar ameaças de dia zero via tráfego de internet.

2.11.24. Permitir a contenção de ameaças de dia zero sem a alteração da infraestrutura de segurança.

2.11.25. Mitigar ameaças de dia zero que possam burlar o sistema operacional emulado.

2.11.26. A solução deve permitir a criação de listas brancas (whitelist) baseadas no MD5 do arquivo.

2.11.27. Mitigar ameaças de dia zero antes da execução e evasão de qualquer código malicioso.

2.11.28. Conter e mitigar exploits avançados.

2.11.29. A análise em nuvem ou local deve prover informações sobre as ações do malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo malware, gerar assinaturas de Anti-Vírus e Anti-Spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo malware e prover Informações sobre o usuário infectado (seu endereço IP e seu login de rede).

2.11.30. Suporte a submissão manual de arquivos para análise através do serviço de Sandbox.

2.12. CARACTERÍSTICAS DE FILTRO DE CONTEÚDO WEB

2.12.1. Possuir filtro de conteúdo integrado ao NGFW para classificação de páginas web com, no mínimo, 50 (cinquenta) categorias distintas, com mecanismo de atualização e consulta automáticas.

2.12.2. 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.

2.12.3. Devem ser fornecidas licenças de filtro de conteúdo para cada equipamento e quantidade de usuários ilimitada, provendo atualização automática e em tempo real através da categorização contínua de novos sites da Internet, sem custo adicional, por todo o período de vigência da garantia e do contrato de manutenção e suporte técnico.

2.12.4. Permitir a customização de página de bloqueio.

2.12.5. Controle de conteúdo filtrado por categorias de sites com base de dados continuamente atualizada pelo fabricante.

2.12.6. Deve permitir submissão de novos sites para categorização.

2.12.7. Permitir a classificação dinâmica de sites web, URLs e domínios.

Escaneie a imagem para verificar a autenticidade do documento

2.12.8. Permitir a associação de grupos de usuários a diferentes regras de filtragem de sites web, definindo quais categorias deverão ser bloqueadas ou permitidas para cada grupo de usuários, podendo ainda adicionar ou retirar acesso a domínios específicos da Internet.

2.12.9. Permitir a definição de quais zonas de segurança terão aplicadas as regras de filtragem de web.

2.12.10. Permitir aplicar a política de filtro de conteúdo baseada em horário do dia, bem como dia da semana.

2.13. CARACTERÍSTICAS DE AUTENTICAÇÃO

2.13.1. Prover autenticação de usuários para os serviços Telnet, FTP, HTTP e HTTPS, utilizando as bases de dados de usuários e grupos de servidores Windows e Unix, de forma simultânea.

2.13.2. Permitir a autenticação dos usuários utilizando servidores LDAP, AD, RADIUS, Tacacs+, Single Sign On e API.

2.13.3. Permitir o cadastro manual dos usuários e grupos diretamente no NGFW por meio da interface de gerência remota do equipamento.

2.13.4. Permitir a integração com qualquer autoridade certificadora emissora de certificados X.509 que siga o padrão de PKI descrito na RFC 2459, inclusive verificando os certificados expirados/revogados, emitidos periodicamente pelas autoridades certificadoras, os quais devem ser obtidos automaticamente pelo NGFW.

2.13.5. Permitir o controle de acesso por usuário, para plataformas Microsoft Windows de forma transparente, para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado sem a instalação de softwares adicionais nas estações de trabalho e sem configuração adicional no browser.

2.13.6. 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 NGFW.

2.13.7. Permitir aos usuários o uso de seu perfil independentemente do endereço IP da máquina que o usuário esteja utilizando.

2.13.8. Permitir a atribuição de perfil por faixa de endereço IP nos casos em que a autenticação não seja requerida.

2.13.9. Suportar a criação de túneis seguros sobre IP (IPSEC tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet

2.14. CARACTERÍSTICAS DE ADMINISTRAÇÃO

2.14.1. Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o NGFW, cada um responsável por determinadas tarefas da administração.

2.14.2. Possuir mecanismo para aplicar remotamente, pela interface gráfica, correções e atualizações para o NGFW.

2.14.3. Possuir mecanismo para realizar remotamente, através de interface gráfica, cópias de segurança (backup) e restauração de configurações e sistema operacional.

2.14.4. Possuir mecanismo para agendamento realização das cópias de segurança (backups) de configuração.

2.14.5. Possuir mecanismo para exportar as configurações através de FTP, HTTPs ou SFTP.

Escaneie a imagem para verificar a autenticidade do documento

2.14.6. A solução deve permitir ao administrador aplicar ajustes rápidos das melhores práticas de segurança no dispositivo com apenas um clique, possibilitando implementar as melhores práticas recomendadas pelo fabricante.

2.14.7. Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do NGFW e a remoção de qualquer uma destas sessões ou conexões.

2.14.8. Permitir a visualização, em forma gráfica, do percentual do uso de CPU e quantidade de tráfego de rede em todas as interfaces do NGFW em tempo real.

2.14.9. Permitir a visualização, em tempo real, dos serviços com maior tráfego e os endereços IP mais acessados.

2.14.10. Deve suportar minimamente dois tipos de negação de tráfego nas políticas de firewall: Descarte sem notificação do bloqueio ao usuário (discard), descarte com notificação do bloqueio ao usuário (drop), descarte com opção de envio de "ICMP Unreachable" para máquina de origem do tráfego, "TCP-Reset" para o cliente, "TCP-Reset" para o servidor ou para os dois lados da conexão.

2.14.11. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps, URLs acessadas e ameaças identificadas.

2.14.12. Ser capaz de visualizar, de forma direta no appliance e em tempo real estado do processamento do produto e volume/desempenho de dados utilizado pela rede de computadores conectada ao equipamento.

2.14.13. Possibilitar a geração de relatório de ameaças com avaliação e gerenciamento de riscos e informações detalhadas sobre o ambiente, ajudando a identificar explorações de vulnerabilidades, intrusões e outras ameaças. Deve permitir a emissão deste relatório em formato PDF.

2.14.14. Ser capaz de visualizar, de forma direta no appliance e em tempo real, a largura de banda utilizada por política, por protocolo TCP/UDP IPV4 e IPV6.

2.14.15. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as conexões estabelecidas, com possibilidade de aplicar filtros na visualização.

2.14.16. Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML ou PDF: relatório de acessos realizados a sites e protocolos por usuários específicos durante determinado período, máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (considerando a existência do filtro de conteúdo Web). O histórico de acesso à internet deverá permanecer acessível por pelo menos 12 meses e armazenado nos equipamentos da contratada.

2.14.17. Permitir habilitar auditoria de configurações no equipamento, possibilitando o rastreio das configurações aplicadas no produto.

2.14.18. Ser capaz de implementar a funcionalidade de "Zero-Touch", permitindo que o equipamento se provisione autônoma e automaticamente no sistema de gestão centralizada.

2.14.19. A solução deve possuir mecanismo de gerenciamento através de aplicativo móvel, com disponibilidade para os sistemas operacionais IOS e Android.

2.14.20. O aplicativo móvel deve possibilitar conexão ao dispositivo via protocolo HTTPS e conexão USB.

2.14.21. O gerenciamento via aplicativo móvel deve permitir visualização de status de consumo de banda, CPU, conexões ativas dos dispositivos e topologia do NGFW.

2.14.22. O aplicativo móvel deve permitir visualização de status das ameaças observadas e bloqueadas pelas funcionalidades de segurança de NGFW.

Escaneie a imagem para verificar a autenticidade do documento

2.14.23. O aplicativo móvel deve permitir visualização dos últimos logs gerados no NGFW.

2.14.24. O aplicativo móvel deve permitir diagnósticos simples na solução, como testes ICMP e verificação DNS.

2.14.25. O aplicativo móvel deve permitir configurar interfaces, objetos e políticas de acesso, além de exportar configurações.

2.14.26. A contratada deverá comprovar que possui em seu quadro de funcionários, pelo menos (3) três Profissionais Técnicos Certificados pelo fabricante da solução, na execução dos serviços de instalação, manutenção e treinamento.

2.14.27. A contratante deverá ter acesso administrativo (leitura e gravação) na solução com intuito de modificações e intervenções em questões emergenciais. Por definição "padrão" a contratante sempre fará abertura de chamados técnicos para intervenção nos equipamentos da contratada. Atrelado ao mencionado, deverá ser feito repasse de conhecimento para pelo menos 05 usuários referente a administração básica da ferramenta para as questões de acessos emergenciais.

2.15. ACORDO DE NÍVEL DE SERVIÇO

2.15.1. O objetivo deste Acordo de Nível de Serviço (ANS) ou Service Level Agreement (SLA) é definir as responsabilidades e dependências entre a contratada e o CRF-SP para os serviços contratados.

2.15.2. Os acordos operacionais previstos neste documento não devem ter precedência nem limitar as respectivas obrigações e responsabilidades já descritas no contrato feito entre o CRF-SP e a contratada.

2.15.3. Este SLA descreve como o CRF-SP e a contratada irão tratar seu relacionamento, para assegurar que os serviços serão corretamente entregues. Define os compromissos requeridos para a entrega dos serviços contratados.

2.16. SEVERIDADE

2.16.1. Os níveis abaixo devem ser observados para classificação de severidade na abertura de chamados ao Suporte Técnico, devendo ser registrados no momento do atendimento.

| SEVERIDADE | DESCRIÇÃO | TEMPO MÁXIMO PARA INÍCIO DO ATENDIMENTO |
|---|---|---|
| Emergencial | Falha no sistema, fora de operação, interrompido. | 1 hora |
| Mau Funcionamento | Falha intermitente em serviços suportados que torne o ambiente lento ou em pequenos grupos a operação está afetada, mas sem interrupção. Ajustes de configuração para liberação de acesso a sites restritos ou downloads de arquivos cuja extensões estejam bloqueadas. | 2 horas |
| Atividade Remota Programada | Realização de manutenção preventiva, atualizações e atividades agendadas. | 12 horas |

2.16.2. A Contratada permitirá que um técnico da equipe do CRF-SP possa realizar ajustes das permissões quanto aos acessos a sites e arquivos bloqueados aos usuários cujo objetivo é agilizar o atendimento a esse tipo de demanda. O CRF-SP ficará obrigado a comunicar a contratada quaisquer alterações que realizar na solução.

Escaneie a imagem para verificar a autenticidade do documento

2.16.3. Os prazos acima relacionados serão computados a partir do momento de abertura do chamado pelo funcionário do CRF-SP a central de suporte da contratada.

2.16.4. A contratada deverá prestar o serviço de suporte nas modalidades Web ou telefônica, em idioma português do Brasil.

2.16.5. A contratada deverá manter o serviço de suporte técnico disponível para abertura e acompanhamento de chamados em tempo integral 24x7 (vinte e quatro horas por dia, sete dias por semana, todos os dias do ano, inclusive sábados, domingos e feriados).

2.16.6. A contratada deverá garantir que o CRF-SP efetue um número ilimitado de chamados de suporte durante a vigência do contrato para suprir suas necessidades de utilização, sem ônus adicional para o CRF-SP.

2.16.7. A contratada deverá fornecer ao CRF-SP um número de telefone que possibilite ligações para o suporte técnico, para fins de abertura e acompanhamento de chamados. A contratada deverá fornecer ao CRF-SP acesso a pelo menos 3 (três) pessoas autorizadas para abertura e acompanhamento de chamados de suporte.

2.16.8. Na abertura de cada chamado técnico deverá ser emitido um registro contendo informações detalhadas do chamado.

2.16.9. Uma vez feito o contato por este número de telefone, a contratada terá os prazos estabelecidos nos termos deste Acordo de Nível de Serviços para dar uma solução à ocorrência, conforme seu grau de severidade.

2.17. REQUISITOS DE QUALIFICAÇÃO TÉCNICA

2.17.1. Como comprovação de atendimento dos requisitos de qualificação técnica, na data de assinatura do contrato, a Contratada deverá:

2.17.1.1. Apresentar declaração de que a mesma possui autorização e capacitação técnica do fabricante para fornecimento, instalação e configuração da solução de segurança.

2.17.1.2. Comprovar, obrigatoriamente, que possui em seu quadro de funcionários, pelo menos 02 (dois) técnicos certificados pelo fabricante do equipamento proposto, na execução dos serviços de instalação, manutenção e treinamento.

2.18. DA ENTREGA

2.18.1. O prazo total para entrega da solução é de até 60 (sessenta) dias corridos, contados da assinatura do contrato, sendo assim distribuídos:

2.18.1.1. Levantamento das informações: até 4 (quatro) dias;

2.18.1.2. Entrega do plano de implantação: até 5 (cinco) dias após a etapa anterior;

2.18.1.3. Entrega de todos os componentes da solução: até 30 (trinta) dias após a etapa anterior;

2.18.1.4. Instalação física de componentes: até 4 (quatro) dias após a etapa anterior;

2.18.1.5. Instalação lógica e testes: até 5 (cinco) dias após a etapa anterior;

2.18.1.6. Acompanhamento operacional do ambiente pela contratada: até 10 (dez) dias após a etapa anterior;

2.18.1.7. Emissão do termo de homologação da solução: até 2 (dois) dias.

2.18.2. Poderá ser aceita prorrogação, se solicitado com justificativa formal, com até 10 (dez) dias do vencimento do primeiro prazo, após análise da área técnica.

Escaneie a imagem para verificar a autenticidade do documento

2.18.3. O início do pagamento será realizado após a emissão do termo de homologação, tendo como data de início da prestação de serviços / ativação (item 01) o dia 21/02/2023, evitando paralização dos serviços e cobrança cumulativa com o atual contrato.

2.18.4. Os serviços deverão ser executados nas dependências da sede do CRF-SP localizado no seguinte endereço: Conselho Regional de Farmácia do Estado de São Paulo (Sede) Rua Capote Valente, 487, Jardim América, São Paulo, SP, CEP 05.409-001.

## 3. DAS OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATANTE

3.1. Além das obrigações resultantes da observância da legislação vigente, são obrigações do Contratante:

3.1.1. Exercer a fiscalização dos serviços através de servidores especialmente designados, verificando se no desenvolvimento dos trabalhos, estão sendo cumpridos os serviços e especificações previstas no edital, no termo de referência, na proposta e no contrato, de forma satisfatória, e documentando as ocorrências;

3.1.2. Comunicar à Contratada, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;

3.1.3. Prestar à Contratada e a seus representantes e funcionários, todas as informações e esclarecimentos que eventualmente venham a ser solicitados.

3.1.4. Convocar a Contratada para reuniões presenciais ou por meio de videoconferência, sempre que necessário.

3.1.5. Manter equipe interna à disposição da Contratada para acompanhamento, participação em reuniões, fornecimento de informações e esclarecimentos quanto às diretrizes do trabalho;

3.1.6. Encaminhar a liberação de pagamento das faturas da prestação de serviços aprovadas, correspondentes aos serviços efetivamente prestados pela Contratada, no prazo pactuado, mediante as notas fiscais/faturas, devidamente atestadas, comunicando à Contratada, por escrito e tempestivamente, qualquer mudança de Administração e endereço de cobrança.

3.1.7. Solicitar a substituição de qualquer profissional integrante das equipes de trabalho cuja atuação, permanência ou comportamento sejam julgados inadequados, prejudiciais, inconvenientes ou insatisfatórios pelo CRF-SP.

3.1.8. Manifestar-se formalmente em todos os atos relativos à execução do contrato, em especial quanto à aplicação de sanções e alterações do mesmo.

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

## 4. DAS OBRIGAÇÕES E RESPONSABILIDADES DO CONTRATADA

4.1. A Contratada deve cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:

4.1.1. Não transferir a outrem, no todo ou em parte, o contrato, sem prévia e expressa anuência do Contratante;

4.1.2. Fornecer o objeto contratado, conforme especificado, sempre da melhor qualidade, bem como, a solucionar qualquer defeito que ocorra, resultante de má qualidade;

4.1.3. Assumir inteira responsabilidade pela execução dos serviços contratados e efetuá-los de acordo com as especificações constantes da proposta de preços, as disposições do instrumento convocatório e seus anexos, a boa técnica, as legislações e normas pertinente;

Escaneie a imagem para verificar a autenticidade do documento

4.1.4. Cumprir com as condições e prazos contidos no presente contrato;

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

4.1.6. Substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste contrato, o objeto com avarias ou defeitos;

4.1.7. Providenciar a imediata correção das deficiências apontadas pelo Contratante, quanto à execução dos serviços contratados

4.1.8. Ressarcir os eventuais prejuízos causados ao órgão e/ou terceiros, provocados por ineficiência ou irregularidades cometidas na execução dos serviços contratados;

4.1.9. Responsabilizar-se por todas as despesas diretas ou indiretas, tais como salários, transportes, encargos sociais, fiscais, trabalhistas, previdenciários e de ordem de classe, indenizações e quaisquer outras despesas que forem devidas aos seus empregados ou prepostos, no desempenho dos serviços contratados;

4.1.10. Responsável pelos danos causados diretamente ao CRF-SP ou a terceiros, decorrentes de sua culpa ou dolo na execução do contrato, não excluindo ou reduzindo essa responsabilidade a fiscalização dos serviços pelo CRF-SP;

4.1.11. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

4.1.12. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições que culminaram em sua habilitação e qualificação na fase da licitação, mantendo-se devidamente regularizada e apta à contratação com entidades públicas, devendo manter em situação regular e com prazo de validade em vigor os seguintes documentos, que podem ser solicitados a qualquer tempo pelo Contratante.

i - Regularidade Trabalhista (Certidão Negativa de Débito Trabalhista ou Certidão Positiva de Débitos Trabalhistas com Efeito de Negativa);

ii - Regularidade Fiscal Federal (Receita Federal do Brasil – Certidão conjunta/FGTS e INSS); e

iii - Regularidade Fiscal Estadual/Municipal (Receita Estadual/Distrital e Municipal).

4.1.13. Não apresentar, tanto para o CNPJ da Contratada, como para o CPF do sócio majoritário, sanção que impeça a contratação com entidades públicas registradas no:

i - SICAF;

ii - Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) da Corregedoria Geral da União (CGU);

iii - Cadastro Nacional de Condenações Cíveis por Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça – CNJ;

iv - Cadastro de Licitantes inidôneos do Tribunal de Contas da União - TCU.

4.1.14. Designar formalmente preposto para representá-la nas tratativas relativas ao contrato e responsável pelo recebimento e acompanhamento de reclamações ou providências decorrentes da má execução dos serviços, devendo disponibilizar número telefônico fixo e/ou móvel e endereço de e-mail para formalização das demandas. O preposto deverá estar disponível para atendimento das demandas da Contratada em dias úteis e durante o horário comercial;

Escaneie a imagem para verificar a autenticidade do documento

4.1.15. Prestar os esclarecimentos desejados, bem como comunicar imediatamente ao Contratante, quaisquer fatos ou anormalidades que por ventura possam prejudicar o bom andamento ou o resultado final dos serviços.

4.1.16. Comparecer, sempre que convocada, presencialmente na sede do Contratante ou via videoconferência, por meio de pessoa devidamente credenciada, no prazo máximo de 48 (quarenta e oito) horas, para exame e esclarecimentos de quaisquer problemas relacionados com os serviços contratados;

4.1.17. Substituir qualquer profissional integrante das equipes de trabalho cuja atuação, permanência ou comportamento sejam julgados inadequados, prejudiciais, inconvenientes ou insatisfatórios pelo CRF-SP;

4.1.18. Informar formalmente ao Contratante quaisquer alterações dos dados cadastrais, incluindo a de preposto e dados de contatos.

4.1.19. Manifestar-se formalmente em todos os atos relativos à execução do contrato, em especial quanto à aplicação de sanções e alterações do mesmo.

4.1.20. Aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem em até 25% (vinte e cinco por cento), do valor inicial atualizado do contrato, sendo limitado em conformidade com o artigo 65, parágrafo 1º da Lei nº 8.666/1993, entendendo–se como contrato todos os instrumentos mencionados no artigo 62, do mesmo diploma legal.

4.2. Do Sigilo, Da Segurança e Do Tratamento das Operações e Dados Pessoais

4.2.1. A Contratada deverá manter sigilo absoluto sobre quaisquer dados pessoais ou sensíveis, informações, documentos, sejam tais informações tangíveis ou não, orais ou escritas, bem como imagens ou vídeos, armazenados em meio físico, mídia eletrônica ou ainda qualquer outro meio, que a ela venham ser confiados ou que venha ter acesso em razão do contrato, não podendo, sob qualquer pretexto, revelá-los, divulgá-los, reproduzi-los ou deles dar conhecimento a quaisquer terceiros estranhos a este contrato. A manutenção deste sigilo perdurará por 100 (cem) anos, no mínimo, após o término dos serviços contratados, em observância ao artigo 31, §1º, da Lei nº 12.527/2011. Caso se verifique a quebra de sigilo das informações disponibilizadas pelo CRF-SP, serão aplicadas as penalidades previstas na Lei n° 8.666/1993 e no contrato, sem prejuízo das sanções penais cabíveis contidas na Lei nº 13.709/2018 e da comunicação à Autoridade Nacional de Proteção de Dados.

4.2.2. A Contratada deverá fornecer no prazo de 15 dias úteis ao gestor do contrato todas as informações relacionadas ao tratamento de dados, isto é, a todo e qualquer ato que abranja a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle, modificação, comunicação, transferência, difusão ou extração, incluindo eventuais cessões a terceiros, dos dados dos empregados da autarquia, de forma que o Contratante analise a adequação e a necessidade, além de outros princípios contidos na Lei nº 13.709/2018.

4.2.3. Caso o Contratante ou qualquer dos seus empregados entenda que há inobservância aos princípios e diretrizes contidos na Lei nº 13.709/2018, determinará a readequação ou restrição dos dados dos seus empregados, no prazo de 05 dias úteis, sob pena de aplicação das sanções contidas no presente contrato, sem prejuízo de comunicação à Autoridade Nacional de Proteção de Dados.

4.2.4. A Contratada será responsável, seja a título de dolo ou culpa, por qualquer vazamento dos dados dos empregados da autarquia a que der causa, nos termos da Lei nº 13.709/2018 e do Código Civil.

4.2.5. A Contratada deverá disponibilizar ao gestor do contrato, no ato da assinatura deste contrato, as informações e o contato dos CONTROLADOR, OPERADOR E ENCARREGADO DE DADOS, para fins de eventuais adequações aos ditames da Lei Geral de Proteção de Dados, a pedido do Contratante.

4.2.6. Toda e qualquer adequação deverá ser atendida no prazo de 05 dias úteis, sob pena de aplicação das sanções contidas neste contrato, sem prejuízo de outras previstas na Lei nº 13.709/2018, além da

Escaneie a imagem para verificar a autenticidade do documento

comunicação à Autoridade Nacional de Proteção de Dados.

## 5. DA SUBCONTRATAÇÃO

5.1. É expressamente vedada a subcontratação total do objeto deste contrato, sob pena de rescisão contratual.

5.1.1. Será permitida a subcontratação parcial, mediante autorização prévia do Contratante, a quem incumbe avaliar se a subcontratada cumpre os requisitos de qualificação técnica necessária para a execução do objeto.

5.2. Em qualquer hipótese de subcontratação, permanece a responsabilidade integral da Contratada pela perfeita execução contratual, cabendo-lhe realizar a supervisão e coordenação das atividades da subcontratada, bem como responder perante a Contratante pelo rigoroso cumprimento das obrigações contratuais correspondentes ao objeto da subcontratação.

## 6. DA ALTERAÇÃO SUBJETIVA

6.1. É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

## 7. DO CONTROLE E FISCALIZAÇÃO DA EXECUÇÃO

7.1. Não obstante a contratada seja a única e exclusiva responsável pela execução de todos os serviços, ao CRF-SP é reservado o direito de, sem que de qualquer forma restrinja a plenitude dessa responsabilidade, exercer a mais ampla e completa fiscalização sobre os serviços, por funcionário indicado, podendo para isso:

7.1.1. Acompanhar os serviços que serão executados pela Contratada, em qualquer de suas fases, sem prévia comunicação.

7.1.2. Promover as diligências necessárias de forma a acompanhar a execução do contrato;

7.1.3. Tomar a decisão final em todos e quaisquer assuntos relativos ao objeto contratado, levando-se em conta a experiência, opiniões e sugestões da Contratada;

7.1.4. Observar para que durante toda a vigência do contrato, seja mantida a compatibilidade com as obrigações assumidas, as condições de habilitação e qualificações exigidas na contratação.

7.1.5. Executar mensalmente a medição dos serviços, descontando-se do valor devido, o equivalente aos serviços não prestado ou aqueles em desacordo com o contratado e por motivos imputáveis à Contratada, sem prejuízo das demais sanções disciplinares em contrato.

7.2. É assegurada ao Contratante a faculdade de exigir, a qualquer tempo, da Contratada, documentação que comprove o correto e tempestivo pagamento de todos os encargos previdenciários, trabalhistas, fiscais e comerciais decorrentes da execução deste contrato.

7.3. A fiscalização e acompanhamento dos serviços prestados pela Contratada serão feitos pelo Departamento de Tecnologia da Informação, que reclamará junto ao representante ou preposto indicado a regularização das eventuais falhas ou irregularidades que forem verificadas, comunicando à autoridade superior aquelas que ultrapassarem a sua competência, tudo sem prejuízo das penalidades que se mostrarem cabíveis.

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

7.4.1. O recebimento de material será realizado em conformidade com o estabelecido nas Seção I e II do Capítulo IV da Portaria CRF-SP nº 01, de 19 de janeiro de 2021.

Escaneie a imagem para verificar a autenticidade do documento

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

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

## 8. DOS RECURSOS ORÇAMENTÁRIOS

8.1. O crédito orçamentário para atender as despesas decorrentes desta contratação está consignado no orçamento para o exercício 2022 e correrá à conta de:

8.1.1. Serviço de Manutenção e Atualização de Software – Elemento de despesa: 6.2.2.1.1.01.04.04.005.008.

8.2. Sempre que a vigência do contrato ultrapassar a vigência dos respectivos créditos orçamentários, será providenciada dotação orçamentária própria para cobertura do período subsequente.

## 9. DA VIGÊNCIA

9.1. O presente contrato de prestação de serviços por tempo determinado terá vigência pelo **período de 30 (trinta) meses**, **com início em 01 de dezembro de 2022 e término em 31 de maio de 2025**, podendo ser prorrogado em conformidade com o artigo 57, inciso II da Lei nº 8.666/1993.

## 10. DO PAGAMENTO

10.1. O Contratante pagará à Contratada os valores a seguir dispostos:

10.1.1. Item 01 – Demais serviços a serem prestados após a homologação, conforme descrito no contrato, incluindo a manutenção e suporte técnico da solução de segurança e controle de acesso a rede de computadores através de appliance de controle unificado (firewall) – **Valor Mensal: R$ 10.993,50 (dez mil e novecentos e noventa e três reais e cinquenta centavos).**

10.1.2. Item 02 – Serviço de implantação (instalação, configuração, implementação etc) que possibilite a homologação da solução ofertada – **Valor total (parcela única): R$ 5.195,00 (cinco mil e cento e noventa e cinco reais).**

10.2. O pagamento será realizado após a completa execução dos serviços e/ou entrega dos itens, no prazo máximo de até 21 (vinte e um) dias, contados a partir do recebimento da nota fiscal ou fatura, creditada em conta bancária da Contratada, mediante atesto do departamento gestor do contrato.

10.2.1. Caso seja devolvida por qualquer irregularidade quanto ao atesto ou documental/fiscal novo prazo de 21 (vinte e um) dias será contado a partir de sua reapresentação, sem qualquer ônus para o Contratante, independentemente da data de vencimento.

10.3. A nota fiscal poderá ser substituída por fatura ou documento equivalente, observada a legislação aplicável.

10.4. No campo para descrição na nota fiscal a Contratada deverá informar os dados bancário para depósito, fazendo constar o banco, número da agência e conta corrente ou poupança, caso a Contratada opte por esta forma de pagamento.

10.4.1. Em caso de pagamento via boleto, a empresa deverá observar as retenções previstas nos subitens abaixo.

10.5. Para emissão da nota fiscal, a Contratada deverá observar a legislação fiscal vigente e suas alterações subsequentes, especialmente a Instrução Normativa nº 1.234/2012 da Receita Federal, e suas alterações, que dispõe sobre a retenção de tributos e contribuições nos pagamentos efetuados pelas pessoas jurídicas que

Escaneie a imagem para verificar a autenticidade do documento

menciona a outras pessoas jurídicas pelo fornecimento de bens e serviços (http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=37200&visao=anotado), devendo fazer constar no campo próprio da nota fiscal os percentuais de descontos e retenções.

10.5.1. Caso a empresa seja optante pelo Regime Especial Unificado de Arrecadação de Tributos e Contribuições devidos pelas Microempresas e Empresas de Pequeno Porte (Simples Nacional), de que trata o artigo 12 da Lei Complementar nº 123/2006, em relação às suas receitas próprias, deverão, juntamente com a nota fiscal para pagamento, apresentar devidamente preenchido o Anexo IV da instrução Normativa a que se refere o item anterior.

10.6. Além do disposto no subitem acima, a Contratada também deverá observar a Lei Complementar nº 116/2003, relativa ao Imposto Sobre Serviços de Qualquer Natureza (ISS), bem como observar os regulamentos do município correspondente no qual a empresa é prestadora de serviços, bem como no município do estabelecimento tomador dos serviços (ou seja, do município da unidade contratante) para que as notas fiscais sejam devidamente escrituradas e o recolhimento ocorra em conformidade às disposições legais, considerando o prazo constante do item 10.1, devendo o mesmo considerar também o vencimento do recolhimento do referido imposto e fazer o percentual correspondente constar do campo próprio da nota fiscal.

10.6.1. No caso de prestação de serviços, sujeitos à retenção de ISS, a nota fiscal que não for entregue ao Contratante dentro do próprio mês da prestação, deve ser entregue até o 1º (primeiro) dia útil do mês subsequente, sob pena de arcar com os ônus decorrentes, conforme disposto no subitem abaixo.

10.6.2. Caso a Contratada não observe o prazo para recolhimento do ISS e o término da contagem do prazo disposto no subitem acima ultrapasse o prazo para recolhimento do mesmo, o valor de possíveis penalidades, multas e afins, serão abatidos do valor líquido a ser pago à empresa, não sendo o Contratante onerado com tais custos de forma alguma.

10.7. A nota fiscal ou fatura deverá estar obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao 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 8.666/1993.

10.7.1. Constatando-se, junto ao SICAF, a situação de irregularidade da Contratada, deverão ser tomadas as providências previstas no do art. 31 da Instrução Normativa nº 3, de 26 de abril de 2018.

10.8. 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 a Contratante.

10.9. A nota fiscal ou fatura deverá ser entregue no Departamento de Licitações e Contratos do CRF-SP, localizado na Rua Capote Valente, 487 – 3º andar – Jardim América – CEP: 05.409-001 – São Paulo – SP, nos dias úteis, no horário das 08h30 horas às 17h30, impreterivelmente, podendo ser recusado a entrega caso não seja cumprido o horário determinado.

10.9.1. No caso da emissão e do envio de Nota Fiscal Eletrônica, deverão ser utilizados os seguintes endereços eletrônicos:

a) Departamento de Licitações e Contratos - licitacoes@crfsp.org.br; e

b) Departamento de Tecnologia da Informação: suporte@crfsp.org.br

10.10. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP, sendo:
EM = Encargos moratórios;
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = Valor da parcela a ser paga.

Escaneie a imagem para verificar a autenticidade do documento

I = Índice de compensação financeira = 0,00016438, assim apurado:

| | | |
|---|---|---|
| I = (TX) | I = ( 6 / 100 ) / 365 | I = 0,00016438<br>TX = Percentual da taxa anual = 6% |

10.11. O Contratante efetuará o pagamento o objeto contratado somente a Contratada, vedada sua negociação com terceiros.

10.12. Caso ocorra, serão abatidos do valor da Nota Fiscal ou Fatura devido à Contratada, os custos com deslocamentos, hospedagens e afins, de advogado e preposto do Contratante para defesa em ações trabalhistas diversas, propostas por funcionários da Contratada.

10.12.1. Somente não será aplicada à Contratada a providência descrita no subitem acima caso elabore a respectiva defesa ou medida judicial cabível, mediante substabelecimento, submetendo-a obrigatoriamente ao crivo do Contratante.

10.13. O CRF-SP é considerado consumidor final e, portanto, deverá a Contratada obedecer ao fixado no artigo. 155, § 2º, inciso VII, da Constituição Federal do Brasil.

## 11. DO REAJUSTE

11.1. Os preços são fixos e irreajustáveis no prazo de um ano contado da data limite para a apresentação das propostas.

11.1.1. Dentro do prazo de vigência do contrato e mediante solicitação da contratada, os preços contratados poderão sofrer reajuste após o interregno de um ano, aplicando-se o índice IPCA/IBGE exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

11.2. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

11.3. No caso de atraso ou não divulgação do índice de reajustamento, o Contratante pagará à Contratada a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo. Fica a Contratada obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.

11.4. Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.

11.5. Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.

11.6. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

11.7. O reajuste será realizado por apostilamento.

## 12. DA GARANTIA DE EXECUÇÃO

12.1. A Contratada, no prazo de 05 (cinco) dias úteis, após a assinatura do Termo de Contrato ou aceite do instrumento equivalente, prestará garantia equivalente a 5% (cinco por cento) do valor do contrato, que será liberada de acordo com as condições previstas neste contrato, conforme disposto no art. 56 da Lei nº 8.666/1993, desde que cumpridas as obrigações contratuais.

12.2. Caberá a Contratada optar por uma das seguintes modalidades de garantia:

12.2.1. **CAUÇÃO EM DINHEIRO OU EM TÍTULOS DA DÍVIDA PÚBLICA**, devendo estes ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda;

Escaneie a imagem para verificar a autenticidade do documento

12.2.2. **SEGURO-GARANTIA**, contendo:

12.2.2.1. Apólice em que o Contratante deverá ser indicado como beneficiário;

12.2.2.2. Prazo de validade, que deverá corresponder ao período de vigência do contrato, acrescido de 3 (três) meses, devendo ser tempestivamente renovado se estendida ou prorrogada essa vigência;

12.2.2.3. Cláusula que assegure o pagamento, independente de interpelação judicial, caso a Contratada não cumpra as obrigações decorrentes da execução do contrato.

12.2.3. **FIANÇA BANCÁRIA**, contendo:

12.2.3.1. Prazo de validade, que deverá corresponder ao período de vigência do contrato, acrescido de 03 (três) meses, devendo ser tempestivamente renovada se estendida ou prorrogada a vigência do contrato;

12.2.3.2. Expressa afirmação do fiador de que, como devedor solidário, fará o pagamento ao CRF-SP, independentemente de interpelação judicial, caso o afiançado não cumpra as obrigações decorrentes da execução do contrato;

12.2.3.3. Renúncia expressa do fiador ao benefício de ordem e aos direitos previstos nos artigos 827 e 838 do Código Civil.

12.3. A garantia em dinheiro deverá ser efetuada em favor da Contratante, conforme dados bancários a seguir descrito:

Favorecido: Conselho Regional de Farmácia do Estado de São Paulo – CRF-SP
CNPJ: 60.975.075/0001-10
001 – Banco do Brasil S/A
Agência nº 1897-X – Conta Corrente nº 300.671-9

12.3.1. Uma vez realizada a transação, deverá ser enviado o respectivo comprovante para o o endereço eletrônico licitacoes@crfsp.org.br.

12.4. Caso a garantia oferecida pela Contratada evidencie qualquer impropriedade ou incorreção em seu teor ou origem, ou se for utilizada no pagamento de quaisquer obrigações, incluindo a indenização de terceiros, a Contratante poderá, a qualquer tempo, exigir sua regularização ou substituição no prazo máximo e improrrogável de 5 (cinco) dias úteis, contados do recebimento da referida notificação.

12.5. A falta de atendimento à convocação para regularização ou substituição da garantia na forma e prazo especificados no subitem anterior sujeitará a Contratada às seguintes consequências:

a) retenção dos pagamentos que lhe sejam devidos, para recomposição da garantia, na modalidade caução em dinheiro; ou

b) caracterização de inexecução contratual, ensejando a consequente aplicação das penalidades previstas neste contrato e, ainda, a rescisão do ajuste com fundamento no artigo 78 da Lei nº 8.666/1993.

12.6. Caberá à Administração decidir motivadamente entre a retenção de pagamentos para recomposição da garantia ou a caracterização da inexecução contratual.

12.7. A Contratante poderá utilizar a garantia, a qualquer momento, para se ressarcir das despesas decorrentes de quaisquer obrigações inadimplidas da Contratada.

12.7.1. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

12.7.1.1. Prejuízos advindos do não cumprimento do objeto do contrato;

Escaneie a imagem para verificar a autenticidade do documento

12.7.1.2. Prejuízos diretos causados à Administração decorrentes de culpa ou dolo durante a execução do contrato;

12.7.1.3. Multas moratórias e punitivas aplicadas pela Administração à Contratada; e

12.7.1.4. Obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela Contratada, quando couber.

12.8. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item anterior, observada a legislação que rege a matéria.

12.9. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser readequada ou renovada nas mesmas condições.

12.10. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a Contratada obriga-se a fazer a respectiva reposição no prazo máximo de 05 (cinco) dias úteis, contados da data em que for notificada.

12.10.1. Em caso da não reposição da garantia pela Contratada, fica autorizada ao Contratante reter os pagamentos devidos até o cumprimento do subitem acima.

12.11. A Contratante executará a garantia na forma prevista na legislação que rege a matéria.

12.12. A garantia prestada pelo Contratado será liberada ou restituída após a execução do contrato e, quando em dinheiro, atualizada monetariamente (artigo 56, §4º da Lei nº 8666/93).

12.13. A devolução da garantia não isenta a Contratada das responsabilidades previstas no artigo 618 do Código Civil Brasileiro.

## 13. DO REAJUSTE

13.1. Os preços são fixos e irreajustáveis no prazo de um ano contado da data limite para a apresentação das propostas.

13.1.1. Dentro do prazo de vigência do contrato e mediante solicitação da contratada, os preços contratados poderão sofrer reajuste após o interregno de um ano, aplicando-se o índice IPCA/IBGE exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

13.2. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

13.3. No caso de atraso ou não divulgação do índice de reajustamento, o Contratante pagará à Contratada a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo. Fica a Contratada obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.

13.4. Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.

13.5. Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.

13.6. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

13.7. O reajuste será realizado por apostilamento.

## 14. DA RESCISÃO CONTRATUAL

14.1. O presente contrato poderá ser rescindido de pleno direito, conforme disposições e motivos previstos nos artigos 77, 78, 79 e 80 da Lei n° 8.666/1993, ou quaisquer outros motivos devidamente justificados.

Escaneie a imagem para verificar a autenticidade do documento

14.2. No caso de rescisão por ato unilateral e escrito da Administração (artigo 79, inciso I, da Lei n° 8.666/1993), a intenção será comunicada com antecedência de, no mínimo, 30 (trinta) dias corridos.

## 15. DA ALTERAÇÃO

15.1. Este contrato poderá ser alterado em qualquer das hipóteses previstas no artigo 65 da Lei nº 8.666/1993.

## 16. DAS SANÇÕES ADMINISTRATIVAS

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

16.1.1. Não assinar o termo de contrato ou aceitar/retirar o instrumento equivalente, quando convocado dentro do prazo de validade da proposta;

16.1.2. Não assinar a ata de registro de preços, quando cabível;

16.1.3. Apresentar documentação falsa;

16.1.4. Deixar de entregar os documentos exigidos no certame;

16.1.5. Ensejar o retardamento da execução do objeto;

16.1.6. Não mantiver a proposta;

16.1.7. Cometer fraude fiscal;

16.1.8. Comportar-se de modo inidôneo;

16.2. No que couber, as infrações capituladas na Lei 10.520/2002, prévias à formalização da contratação, serão apenadas com o impedimento de licitar e o descredenciamento do SICAF pelo prazo de até 5 anos.

16.3. Pela inexecução total ou parcial do objeto da contratação, a Administração pode aplicar à Contratada as seguintes sanções:

16.3.1. **Advertência por escrito**, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado;

16.3.2. **Multa**

16.3.2.1. Multa moratória de 1% (um por cento), por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias;

16.3.2.2. Multa moratória de 0,5% (cinco décimos por cento) do valor total do contrato por dia de atraso na apresentação da garantia (seja para reforço ou por ocasião de prorrogação), observado o máximo de 5% (cinco por cento). O atraso superior a 10 (dez) dias autorizará a Contratante, com base no juízo de conveniência e oportunidade, a decidir sopre a rescisão ou manutenção do contrato;

16.3.2.3. Multa compensatória de 15% (quinze por cento) sobre o valor total do contrato, no caso de inexecução parcial do objeto;

16.3.2.4. Multa compensatória de 30% (tinta por cento) sobre o valor total do contrato, no caso de inexecução total do objeto;

16.3.2.5. As penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si.

16.3.3. **Suspensão temporária** de participação em licitação e impedimento de contratar com a Conselho Regional de Farmácia do Estado de São Paulo – CRF-SP, por prazo não superior a dois anos;

Escaneie a imagem para verificar a autenticidade do documento

16.3.4. **Impedimento de licitar** e contratar com a União com o consequente descredenciamento no SICAF pelo prazo de até cinco anos;

16.3.4.1. A Sanção de impedimento de licitar e contratar prevista neste subitem também é aplicável em quaisquer das hipóteses previstas como infração administrativa no subitem 13.1 deste contrato.

16.3.5. **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 a Contratante pelos prejuízos causados;

16.4. As sanções previstas nos subitens 16.3.1, 16.3.3, 16.3.4 e 16.3.5 poderão ser aplicadas à Contratada juntamente com as de multa, descontando-a dos pagamentos a serem efetuados.

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

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

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

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

16.1. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto na Portaria CRF-SP nº 04, de 2021 (http://www.crfsp.org.br/legisla%C3%A7%C3%A3o/crf-sp/portarias.html?layout=edit&id=11680), Lei nº 8.666/1993, e subsidiariamente na Lei nº 9.784/1999.

16.2. As multas devidas e/ou prejuízos causados à Contratante serão deduzidos do valor líquido, após a liquidação das obrigações tributárias, de qualquer fatura ou crédito existente no CRF-SP, em favor da Contratada.

16.2.1. Caso a Contratante determine, a multa deverá ser recolhida no prazo máximo de 10 (dez) dias corridos, a contar da data do recebimento da comunicação enviada pela autoridade competente.

16.3. Caso a multa seja superior ao crédito eventualmente existente, a diferença será cobrada administrativamente ou judicialmente.

16.4. 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.

16.5. Se, durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização - PAR.

16.6. A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.

16.7. O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Federal resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

Escaneie a imagem para verificar a autenticidade do documento

16.8. Em caso de aplicação de penalidade, a Contratada será notificada e será concedido o prazo de 05 (cinco) dias úteis para apresentação de defesa prévia. Em caso de manutenção da penalidade imposta, a empresa será notificada e facultado novo prazo de 05 (cinco) dias úteis para interposição de recurso.

16.8.1. As razões e eventuais contrarrazões deverão ser protocoladas, em via original, no horário das 08h30 às 17h30, em dias úteis, no Departamento de Atendimento, localizado na Rua Capote Valente, 487 – térreo – Jardim América – CEP: 05.409-001 – São Paulo – SP.

16.8.2. A apresentação de defesa prévia e/ou interposição de recurso poderá ser realizada através do endereço eletrônico licitacoes@crfsp.org.br, desde que atendido o seu prazo original, previsto no item 16.13, e que os documentos em vias originais sejam protocolados em até 05 (cinco) dias úteis, contados da data em que se encerraria o prazo da defesa prévia e/ou do recurso.

16.8.2.1. O descumprimento do subitem acima acarretará na intempestividade da defesa/recurso, exceto se os documentos apresentados por meio eletrônico, contiverem assinatura por meio de plataforma eletrônica, ou outro meio eletrônico, com ou sem a utilização de certificado digital emitida no padrão estabelecido pela ICP-Brasil, nos termos do Decreto nº 8.539/2015.

16.8.3. Quem fizer uso de sistema de transmissão torna-se responsável pela qualidade e fidelidade do material transmitido, e pelo seu protocolo conforme estabelecido no subitem acima.

16.9. As penalidades serão obrigatoriamente registradas no SICAF.

## 17. DAS ORIENTAÇÕES ANTICORRUPÇÃO

17.1. Na execução do presente contrato é vedado ao CONTRATANTE e a Contratada e/ou a empregado seu, e/ou a preposto seu, e/ou a gestor seu:

a) Prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público ou a quem quer que seja, ou a terceira pessoa a ele relacionada;

b) Criar, de modo fraudulento ou irregular, pessoa jurídica para celebrar o presente contrato;

c) Obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações do presente contrato, sem autorização em lei, no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais;

d) Manipular ou fraudar o equilíbrio econômico-financeiro do presente contrato; ou

e) De qualquer maneira fraudar o presente contrato; assim como realizar quaisquer ações ou omissões que constituam prática ilegal ou de corrupção, nos termos da Lei nº 12.846/2013 (conforme alterada), do Decreto nº 8.420/2015 (conforme alterado), do U.S. Foreign Corrupt Practices Act de 1977 (conforme alterado) ou de quaisquer outras leis ou regulamentos aplicáveis ("Leis Anticorrupção"), ainda que não relacionadas com o presente contrato.

17.2. Para a execução deste contrato, nenhuma das partes poderá oferecer, dar ou se comprometer a dar a quem quer que seja, ou aceitar ou se comprometer a aceitar de quem quer que seja, tanto por conta própria quanto por intermédio de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou não financeiras ou benefícios de qualquer espécie que constituam prática ilegal ou de corrupção, seja de forma direta ou indireta quanto ao objeto deste contrato, ou de outra forma a ele não relacionada, devendo garantir, ainda, que seus prepostos e colaboradores ajam da mesma forma.

## 18. DA PUBLICIDADE DO CONTRATO

18.1. As partes aqui descritas possuem ciência e desde já concordam que a minuta deste instrumento será divulgada no Portal da Transparência do Conselho Regional de Farmácia do Estado de São Paulo, observadas as disposições da Lei Geral de Proteção de Dados (LGPD) - Lei nº 13.709, de 14 de agosto de 2018.

Escaneie a imagem para verificar a autenticidade do documento

## 19. FORO

19.1. Fica eleito o foro da subseção judiciária de São Paulo (Justiça Federal), como único e competente para processar qualquer questão oriunda deste contrato, com renúncia expressa de qualquer outro por mais privilegiado que seja.

E por estarem assim justos e contratados, assinam o presente instrumento em 02 (duas) vias de igual teor e forma, para um só e único fim, juntamente com as testemunhas presentes ao ato.

São Paulo, 25 de novembro de 2022.

Pelo CONTRATANTE:

**Assinado eletronicamente**

**Dr. Marcelo Polacow Bisson**
Presidente

**Assinado eletronicamente**

**Dra. Danyelle Cristine Marini**
Diretora Tesoureira

Pela CONTRATADA:

**Assinado eletronicamente**

**Sr. José Roberto Consani**
Representante Legal

**Testemunha**

Nome: **Elizabeth Adaniya**

Assinatura: **Assinado eletronicamente**

**Testemunha**

Nome: **Moisés Carlos Simão**

Assinatura: **Assinado eletronicamente**

| ELABORADO E CONFERIDO POR: | CONFERIDO E APROVADO POR: | CONFERIDO E APROVADO POR: |
|---|---|---|
| **Assinado eletronicamente** | **Assinado eletronicamente** | **Assinado eletronicamente** |
| **Alexandre Pires Omena**<br>Departamento de Licitações e Contratos | **André Luis Gomes Duarte**<br>Departamento de Tecnologia da Informação | **Leandro Funchal Pescuma**<br>**OAB/SP 315.339**<br>Consultoria Jurídica |

Escaneie a imagem para verificar a autenticidade do documento

# Página de assinaturas

Assinado eletronicamente

**Alexandre Omena**
CRF-SP
Signatário

Assinado eletronicamente

**Andre Duarte**
Conselho Regional de Farmacia de Sã...
Signatário

Assinado eletronicamente

**Leandro Pescuma**
[redacted]
Signatário

Assinado eletronicamente

**Elizabeth Adaniya**
CRF-SP
Signatário

Assinado eletronicamente

**José Consani**
[redacted]
Signatário

Assinado eletronicamente

**Moisés Simão**
[redacted]
Signatário

Assinado eletronicamente

**Marcelo Bisson**
[redacted]
Signatário

Assinado eletronicamente

**Danyelle Marini**
[redacted]
Signatário

## HISTÓRICO

**25 nov 2022**

15:45:01 **Alexandre Pires Omena** criou este documento. (Empresa: CRF-SP, E-mail: alexandre.omena@crfsp.org.br, CPF: [redacted])

**25 nov 2022** 15:45:04 **Alexandre Pires Omena** *(Empresa: CRF-SP, E-mail: alexandre.omena@crfsp.org.br, CPF:* [redacted]) visualizou este documento por meio do IP 200.229.234.2 localizado em São Paulo - Sao Paulo - Brazil.

**25 nov 2022** 15:45:09 **Alexandre Pires Omena** *(Empresa: CRF-SP, E-mail: alexandre.omena@crfsp.org.br, CPF:* [redacted]) assinou este documento por meio do IP 200.229.234.2 localizado em São Paulo - Sao Paulo - Brazil.

**25 nov 2022** 15:45:44 **Andre Luis Gomes Duarte** *(Empresa: Conselho Regional de Farmacia de São Paulo, E-mail: andre.duarte@crfsp.org.br, CPF:* [redacted]) visualizou este documento por meio do IP 200.229.234.2 localizado em São Paulo - Sao Paulo - Brazil.

**25 nov 2022** 15:45:53 **Andre Luis Gomes Duarte** *(Empresa: Conselho Regional de Farmacia de São Paulo, E-mail: andre.duarte@crfsp.org.br, CPF:* [redacted]) assinou este documento por meio do IP 200.229.234.2 localizado em São Paulo - Sao Paulo - Brazil.

**25 nov 2022** 15:48:11 **Leandro Funchal Pescuma** *(E-mail: leandro.pescuma@crfsp.org.br, CPF:* [redacted]) visualizou este documento por meio do IP 200.229.234.2 localizado em São Paulo - Sao Paulo - Brazil.

**25 nov 2022** 15:48:15 **Leandro Funchal Pescuma** *(E-mail: leandro.pescuma@crfsp.org.br, CPF:* [redacted]) assinou este documento por meio do IP 200.229.234.2 localizado em São Paulo - Sao Paulo - Brazil.

**28 nov 2022** 08:37:51 **Elizabeth Adaniya** *(Empresa: CRF-SP, E-mail: elizabeth.adaniya@crfsp.org.br, CPF:* [redacted]) visualizou este documento por meio do IP 200.229.234.2 localizado em São Paulo - Sao Paulo - Brazil.

**28 nov 2022** 08:49:16 **Elizabeth Adaniya** *(Empresa: CRF-SP, E-mail: elizabeth.adaniya@crfsp.org.br, CPF:* [redacted]) assinou este documento por meio do IP 200.229.234.2 localizado em São Paulo - Sao Paulo - Brazil.

**25 nov 2022** 16:13:26 **José Roberto Consani** *(E-mail: consani@assisnetsolucoes.com.br, CPF:* [redacted]) visualizou este documento por meio do IP 187.35.252.166 localizado em São Paulo - Sao Paulo - Brazil.

**25 nov 2022** 16:15:55 **José Roberto Consani** *(E-mail: consani@assisnetsolucoes.com.br, CPF:* [redacted]) assinou este documento por meio do IP 187.35.252.166 localizado em São Paulo - Sao Paulo - Brazil.

**25 nov 2022** 15:47:00 **Moisés Carlos Simão** *(E-mail: moises.simao@assisnetsolucoes.com.br, CPF:* [redacted]) visualizou este documento por meio do IP 200.49.50.130 localizado em Rio de Janeiro - Rio de Janeiro - Brazil.

**25 nov 2022** 15:47:21 **Moisés Carlos Simão** *(E-mail: moises.simao@assisnetsolucoes.com.br, CPF:* [redacted]) assinou este documento por meio do IP 200.49.50.130 localizado em Rio de Janeiro - Rio de Janeiro - Brazil.

**29 nov 2022** 14:38:33 **Marcelo Polacow Bisson** *(E-mail: marcelo.polacow@crfsp.org.br, CPF:* [redacted]) visualizou este documento por meio do IP 200.229.234.2 localizado em São Paulo - Sao Paulo - Brazil.

**29 nov 2022** 14:38:45 **Marcelo Polacow Bisson** *(E-mail: marcelo.polacow@crfsp.org.br, CPF:* [redacted]) assinou este documento por meio do IP 200.229.234.2 localizado em São Paulo - Sao Paulo - Brazil.

**28 nov 2022** 19:43:10 **Danyelle Cristine Marini** *(E-mail: danyelle.marini@crfsp.org.br, CPF:* [redacted]) visualizou este documento por meio do IP 179.247.141.151 localizado em São Carlos - Sao Paulo - Brazil.

**28 nov 2022** 19:43:13 **Danyelle Cristine Marini** *(E-mail: danyelle.marini@crfsp.org.br, CPF:* [redacted]) assinou este documento por meio do IP 179.247.141.151 localizado em São Carlos - Sao Paulo - Brazil.