INDÚSTRIA DE MATERIAL BÉLICO DO BRASIL
Vinculada ao Ministério da Defesa por intermédio do Comando do Exército

CONTRATO Nº 11/2022-UA IMBEL

O ORIGINAL DESTE CONTRATO ENCONTRA-SE ARQUIVADO NA SALCP/UA IMBEL

PROCESSO ADMINISTRATIVO N° 128/2022-UA IMBEL
REFERÊNCIA: PREGÃO ELETRÔNICO SRP N° 04/2022-UA IMBEL
VALOR GLOBAL: R$ 335.350,00
VIGÊNCIA: 23/06/2022 A 22/06/2023

CONTRATO CELEBRADO ENTRE A INDÚSTRIA DE MATERIAL BÉLICO DO BRASIL - SEDE E A EMPRESA STRATEGIO SISTEMAS SERVIÇOS E INFORMÁTICA LTDA PARA AQUISIÇÃO DE MATERIAIS PERMANENTES DE INFORMÁTICA.

A **INDÚSTRIA DE MATERIAL BÉLICO DO BRASIL - IMBEL,** Empresa Pública Federal, vinculada ao Ministério da Defesa, por intermédio do Comando do Exército, constituída pela Lei nº 6.227, de 14/07/1975, com seu Estatuto Social aprovado pela Assembleia Geral Extraordinária nº 04/2020, realizada em 14/12/2020, registrado perante a Junta Comercial, Industrial e Serviços do Distrito Federal - JUCISDF, em 15/01/2021, conforme NIRE 53500000275 e sob nº 1646051, publicado no Diário Oficial da União - DOU, Seção I, página 23 a 28, de 19/01/2021, arquivado e publicado na JUCISDF sob nº 1650189, em 27/01/2021, regida pela Lei nº 13.303, de 30/06/2016, Lei nº 6.404, de 15/12/1976, Decreto nº 8.945, de 27/12/2016, e demais legislações aplicáveis, classificada como Empresa Pública Dependente, nos termos do art. 2º, III, da Lei Complementar nº 101, de 04/05/2000 e da Portaria nº 289, de 29/05/2008, da Secretaria do Tesouro Nacional - STN, publicada no DOU, Seção I, de 30/05/2008, com capital integralmente

subscrito pela **UNIÃO**, inscrita no CNPJ/ME sob n° 00.444.232/0001-39, com **SEDE** e foro na cidade de Brasília - Distrito Federal, localizada no Quartel General do Exército, Bloco "H", 3° Pavimento, Setor Militar Urbano - SMU, Brasília - Distrito Federal, CEP: 70630-901, denominada **CONTRATANTE** ou simplesmente **IMBEL**, neste ato representada, na forma do seu Estatuto, pelo Sr. **E.X.C.**, Ordenador de Despesas, brasileiro, casado, portador da Carteira de Identidade nº **568** SSP/DF, inscrito no CPF nº ***.178.581-**, que no final assina, e, de outro lado, a Empresa **STRATEGIO SISTEMAS SERVIÇOS E INFORMÁTICA LTDA**, pessoa jurídica de direito privado, inscrita no CNPJ/ME nº 00.473.342/0001-29, sediada à Avenida Perimetral, 175, Vila Abajá, Goiânia-GO, CEP 74550-425, neste ato representada pelo Sr. **W.L.DE.M.M.**, Diretor de Soluções, brasileiro, casado, portador da Carteira de Identidade nº **694**-DGPC/GO, inscrito no CPF n° ***.944.761-**, denominada **CONTRATADA,** consoante o que consta o Processo Administrativo nº 128/2022-UA **IMBEL**, referente Pregão Eletrônico SRP nº 4/2022-UA **IMBEL**, resolvem celebrar o presente Contrato, que será regido pelo Edital, Termo de Referência e pela proposta da **CONTRATADA**, no que couber, independentemente de suas expressas transcrições, pelo Decreto nº 8.945/2016, de 27 de dezembro de 2016, pela Lei nº 13.303/2016, pelo Regulamento de Licitações e Contratos da **IMBEL**, aprovado na 305ª Reunião do Conselho de Administração da **IMBEL**, ocorrida em 22/05/2018, conforme Resolução nº 06/2018-CA-**IMBEL**, de 22/05/2018, e pelas cláusulas e condições a seguir dispostas:

CLÁUSULA PRIMEIRA - DO OBJETO E DA SUA ESPECIFICAÇÃO TÉCNICA

1. DO OBJETO

Fornecimento de firewall, modelos sonicwall tz670, sistema de gerenciamento centralizado Network Security Manager, VPN SSL, Sonicwall Analytics e Solução Wireless SONICWAVE 231C. Contemplando serviços de instalação, migração, configuração, garantia e suporte técnico, conforme condições, quantidades e exigências estabelecidas no Termo de Referência.

1.1. ESPECIFICAÇÕES TÉCNICAS

1.1.1. A Atualização da Solução de Firewall para a **IMBEL** consiste no seguinte:

1.1.1.1. Atualização dos atuais equipamentos por meio de Substituição por outros superiores, conforme descritos neste Termo de Referência;

1.1.1.2. Fornecimento de serviços de suporte técnico para solução de eventuais problemas de funcionamento dos equipamentos dos firewalls pelo período de Garantia contratado, incluindo substituições de hardwares quando necessário durante a vigência da Garantia;

1.1.1.3. Fornecimento, ativação e manutenção dos requisitos de segurança nos firewalls, conforme descritos neste Termo de Referência, pelo período de Garantia contratado; e

1.1.1.4. Diante dos procedimentos legais para desfazimento de Patrimônios Públicos a Contratada ao concordar em participar do Certame, tacitamente já concorda que os equipamentos substituídos serão oportunamente incluídos ao processo administrativo de desfazimento de bens, o que impedirá a retirada dos antigos equipamentos da **IMBEL**.

1.1.2. Fornecimento dos Serviços de instalação dos novos equipamentos, configuração, migração de todos os objetos e regras de firewall, configuração entre firewall concentrador e firewalls de pequeno porte, enfim, todos os serviços para a efetiva migração da solução de firewall, sistema de gerenciamento centralizado NSM, Sofware Analitics e rede Wireless da **IMBEL**, até alcançar plena estabilidade operacional.

1.1.3. A retirada dos atuais equipamentos do modo operacional se dará somente com a efetiva instalação e estabilização dos serviços ativos nos novos equipamentos.

1.1.4. A substituição deverá ser por equipamentos novos, podendo ser da mesma família de produção, porém, de modelos superiores, de lançamento no mercado em data mais recente dos atuais equipamentos.

1.1.5. Os novos equipamentos deverão estar em linha de produção quando da entrega dos equipamentos para fins de substituição.

1.1.6. Deverá possuir recursos técnicos e desempenho de processamento equivalente ou superior aos atuais equipamentos.

1.1.7. Na descrição a seguir consta os modelos de referência mínimo aceitável, em termos de performance e capacidade de processamento, para fins de substituição:

1.2. REQUISITOS MÍNIMOS TZ670 – GRUPO 1 - ITEM 01, 02 e 04

1.2.1. DESCRIÇÃO TÉCNICA

1.2.1.1. Desempenho em modo Threat Prevention (Proteção Anti-Malware, IPS e Controle de Aplicação habilitados) mínimo de 2.5 Gbps ou superior;

1.2.1.2. Desempenho em modo de Inspeção (decriptografia e criptografia) de tráfego criptografado (SSL/TLS) mínimo de 790 Mbps;

1.2.1.3. Os desempenhos solicitados devem ser comprovados por documento de domínio público do fabricante;

1.2.1.4. Não serão aceitas declarações ou cartas de fabricantes para atendimento deste item;

1.2.1.5. Desempenho mínimo de 3.0 Gbps de IPS;

1.2.1.6. Suporte mínimo de 1.450.000 conexões simultâneas/concorrentes;

1.2.1.7. Suporte mínimo de 25.000 novas conexões por segundo;

1.2.1.8. Deve possuir armazenamento interno de 32 GB e suportar expansão de armazenamento interno para até 256GB; e

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

1.2.1.10. Deve possuir 8 interfaces 1 GbE padrão RJ-45 e 2 interfaces de 10GbE SFP+;

1.2.1.11. Deve possuir 1 interface do tipo console ou similar;

1.2.1.12. Deve possuir 1 interface USB 3.0 com suporte a tecnologias LTE 3G/4G e 5G;

1.2.1.13. O fornecimento dos produtos e 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;

1.2.1.14. O Equipamento deverá ser homologado pela ANATEL; e

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

1.2.2. CARACTERÍSTICAS GERAIS

1.2.2.1. 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;

1.2.2.2. 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;

1.2.2.3. 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, por um período de 60 meses;

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

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

1.2.2.6. A atualização das assinaturas deverá ocorrer de forma automática sem há necessidade de intervenção humana; e

1.2.2.7. 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.

1.2.3. CARACTERÍSTICAS DIVERSAS

1.2.3.1. 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;

1.2.3.2. 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 tunel IPSec;

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

1.2.3.4. Deve possuir proteção anti-spoofing;

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

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

1.2.3.7. 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;

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

1.2.3.9. 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: (Latência, Jitter e Perda de pacotes);

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

1.2.3.11. A solução de SD-WAN deve permitir encaminhamento de trafego 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;

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

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

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

1.2.3.15. 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;

1.2.3.16. Deve suportar DHCP relay;

1.2.3.17. 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;

1.2.3.18. Deve permitir a utilização de regras de Antivírus, 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;

1.2.3.19. 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;

1.2.3.20. Deve ter suporte à proteção e identificação de hosts possivelmente infectados com "botnets";

1.2.3.21. 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;

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

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

1.2.3.24. Detectar e bloquear a origem de portscans;

1.2.3.25. Deve permitir o bloqueio de ataques;

1.2.3.26. Deve permitir o bloqueio de exploits conhecidos;

1.2.3.27. O gateway Antivírus deve suportar a análise de pelo menos os protocolos HTTP, FTP, IMAP e SMTP;

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

1.2.3.29. Implementar DSCP (Differentiated Services Code Points);

1.2.3.30. 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;

1.2.3.31. 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;

1.2.3.32. Implementar mecanismo de sincronismo de horário através do protocolo NTP;

1.2.3.33. Possuir suporte ao protocolo SNMP versões 2 e 3;

1.2.3.34. Possuir suporte a log via syslog;

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

1.2.3.36. O fabricante ou o produto deve possuir certificado ICSA (International Computer

1.2.3.37. Security Association) para FIREWALL, ou CC (Common Criteria);

1.2.3.38. 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;

1.2.3.39. 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 2019 ou mais recentes;

1.2.3.40. 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;

1.2.3.41. 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; e

1.2.3.42. Controle, inspeção e de-criptografia 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.

1.2.4. CARACTERÍSTICAS DE VPN

1.2.4.1. A VPN SSL deve ser licenciada para, no mínimo, 150 usuários simultâneos;

1.2.4.2. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 200 usuários simultâneos, com aquisição de licença complementar;

1.2.4.3. Deve suportar 250 túneis de VPN tipo Site-to-Site padrão IPSEC simultâneos;

1.2.4.4. Deve suportar, no mínimo, 2 Gbps de desempenho de VPN IPSEC;

1.2.4.5. 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 edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, o fornecedor será considerado inabilitados;

1.2.4.6. Todos os custos oriundos do teste de bancada serão custeados pelo fornecedor/vendedor do certame;

1.2.4.7. 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;

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

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

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

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

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

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

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

1.2.4.15. 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;

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

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

1.2.4.18. 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;

1.2.4.19. 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;

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

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

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

1.2.4.23. A VPN deve permitir que os usuários façam autenticação utilizando no mínimo dois fatores de autenticação, 2FA (two factors authentication).

1.2.5. ALTA DISPONIBILIDADE

1.2.5.1. Devem ser fornecidos 02 (dois) appliances de NGFW do mesmo modelo com gerenciamento unificado, novos e sem uso anterior, funcionando em alta disponibilidade, cobertos pela garantia e suporte de 60 meses;

1.2.5.2. O modelo ofertado deverá estar em linha de produção, sem previsão de encerramento de fabricação, na data de entrega da proposta;

1.2.5.3. O software deverá ser fornecido em sua versão mais atualizada;

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

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

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

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

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

1.2.5.9. A solução deve possibilitar a sincronização de todas as configurações realizadas na caixa principal do cluster incluído, mas não limitado a objetos, regras, rotas, VPNs e políticas de segurança; e

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

1.2.6. CONTROLE DE AMEAÇAS

1.2.6.1. 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 Antivírus e Anti-Bot integrado ao próprio appliance de segurança;

1.2.6.2. A solução de Antivírus integrada deve ter capacidade de analisar arquivos maiores que 1Gbps;

1.2.6.3. 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;

1.2.6.4. 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;

1.2.6.5. Implementar funcionalidade de detecção e bloqueio de "call-backs";

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

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

1.2.6.8. Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS;

1.2.6.9. Implementar interface CLI segura através do protocolo SSH;

1.2.6.10. Possuir Antivírus 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;

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

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

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

1.2.6.14. A solução deve ser capaz de proteger contra-ataques a DNS;

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

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

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

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

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

1.2.6.20. A solução Antivírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS;

1.2.6.21. 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); e

1.2.6.22. Incluindo a capacidade de configuração de listas customizadas para esta mesma finalidade.

1.2.7. <u>PROTEÇÃO CONTRA ATAQUES AVANÇADOS</u>

1.2.7.1. 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";

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

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

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

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

1.2.7.6. 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;

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

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

1.2.7.9. 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;

1.2.7.10.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;

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

1.2.7.12. 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;

1.2.7.13. Conter ameaças avançadas de dia zero;

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

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

1.2.7.16. 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;

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

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

1.2.7.19. Possuir Antivírus 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;

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

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

1.2.7.22. Implementar mecanismo de pesquisa por diferentes intervalos de tempo;

1.2.7.23. Mitigar ameaças de dia zero via tráfego de internet;

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

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

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

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

1.2.7.28. Conter e mitigar exploits avançados;

1.2.7.29.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 Antivírus 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);

1.2.7.30. Suporte a submissão manual de arquivos para análise através do serviço de Sandbox; e

1.2.7.31. 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.

1.2.8. CARACTERÍSTICAS DE FILTRO DE CONTEÚDO WEB

1.2.8.1. 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;

1.2.8.2. 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;

1.2.8.3. 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;

1.2.8.4. Permitir a customização de página de bloqueio;

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

1.2.8.6. Deve permitir submissão de novos sites para categorização;

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

1.2.8.8. 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;

1.2.8.9. Permitir a definição de quais zonas de segurança terão aplicadas as regras de filtragem de web; e

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

1.2.9. CARACTERÍSTICAS DE AUTENTICAÇÃO

1.2.9.1. 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;

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

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

1.2.9.4. 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;

1.2.9.5. 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;

1.2.9.6. 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;

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

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

1.2.9.9. 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.

1.2.10. CARACTERÍSTICAS DE ADMINISTRAÇÃO

1.2.10.1. 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;

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

1.2.10.3. A solução deve permitir que os administradores façam autenticação no console utilizando no mínimo dois fatores de autenticação, 2FA (two factors authentication);

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

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

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

1.2.10.7. 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;

1.2.10.8. 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;

1.2.10.9. 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;

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

1.2.10.11. 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

1.2.10.12. Unreachable" para máquina de origem do tráfego, "TCP-Reset" para o cliente, "TCP-Reset" para o servidor ou para os dois lados da conexão;

1.2.10.13. 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;

1.2.10.14. 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;

1.2.10.15. 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;

1.2.10.16. Deve permitir a emissão deste relatório em formato PDF;

1.2.10.17. 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;

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

1.2.10.18. Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML: 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);

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

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

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

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

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

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

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

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

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

1.2.11. GARANTIA E SUPORTE

1.2.11.1. A garantia de funcionamento do hardware será do Fabricante, pelo período de 60 (sessenta) meses contada a partir da ativação do produto, sem prejuízo de qualquer política de garantia adicional oferecido;

1.2.11.2. O atendimento será em regime 24x7, na modalidade on-site, e serão prestados pelo fabricante ou empresa fornecedora da solução;

1.2.11.3. O prazo máximo para que se inicie o atendimento técnico será de 04 (quatro) horas corridas, contado a partir do momento em que for realizado o chamado técnico devidamente formalizado. Entende-se por início do atendimento técnico inclusive contato telefônico para identificação do tipo de ocorrência afim de preparação de peças adequadas e demais procedimentos técnicos;

1.2.11.4. O prazo máximo para que seja realizado o reparo ou substituição do equipamento será de até 15 (quinze) dias úteis, contado a partir do início do atendimento do chamado;

1.2.11.5. A manutenção corretiva, que se fará sempre que necessária ou solicitada pela **CONTRATANTE**, compreende o diagnóstico, assistência técnica e solução de problemas, bem como a substituição de componentes que apresentarem defeitos ou avarias, ou seja, quaisquer serviços que se fizerem necessários para deixar os equipamentos em perfeito estado de funcionamento;

1.2.11.6. Na manutenção corretiva, após a sua realização, deverão ser feitos testes com os equipamentos, acompanhando o seu funcionamento, pelo técnico em conjunto com o usuário, havendo a obrigatoriedade da assinatura de ambos no documento, ao final dos trabalhos;

1.2.11.7. Na substituição de algum componente ou periférico, devido à manutenção, este deverá ser compatível com os softwares envolvidos, e com as demais partes do equipamento, não podendo ser, em hipótese alguma, de configuração inferior à do substituído;

1.2.11.8. Suporte Técnico ao Software deve estar disponível por meio telefônico pelo período de 60 (sessenta) meses até a renovação da licença, contada a partir da entrega do software, sem prejuízo de qualquer política de garantia adicional oferecido pelo fabricante;

1.2.11.9. O suporte técnico telefônico será em regime 24x7 (vinte e quatro horas por sete dias da semana) através de atendimento remoto e via telefone;

1.2.11.10. Abertura de chamados de atendimento via telefone (0800 ou número local), e-mail e web do Fabricante.

1.2.11.11. Os tipos de chamados (ao Suporte Técnico) a serem abertos e registrados no sistema de atendimento serão:

1.2.11.11.1. Emergência – Falha no sistema (Segurança), fora de operação;

1.2.11.11.2. O início do atendimento "emergencial" não poderá ultrapassar o prazo de 2 (duas) horas, contado a partir da abertura do chamado;

1.2.11.11.3. Mau Funcionamento - Falha intermitente em serviços suportados que torne o ambiente lento ou em pequenos grupos a operação está afetada, mas sem interrupção;

1.2.11.11.4. O início do atendimento "Mau Funcionamento" não poderá ultrapassar o prazo de 4 (quatro) horas, contado a partir da abertura do chamado; e

1.2.11.11.5. Atividade Programada - para a realização de Manutenção e atualização de firmware; e

1.2.11.11.6. O início do atendimento "Atividade Programada" não poderá ultrapassar o prazo de 2 (duas) horas, contado a partir da abertura do chamado, fora do horário comercial.

1.2.11.12. Entende-se por início do atendimento o primeiro contato, após a abertura formal do chamado, feito pela equipe de suporte da **CONTRATADA** com a equipe da **CONTRATANTE** para tratar do problema reportado, devidamente registrado no sistema;

1.2.11.13. Nas situações em que for detectado e/ou comprovado um problema de firmware (bug) no equipamento de Segurança, o prazo de atendimento será fornecido diretamente pela engenharia do fabricante com apoio continuo e intermediação do chamado pela contratada. O SLA para a resolução do problema neste caso não poderá ser superior a 30 dias úteis a partir da data da confirmação deste problema;

1.2.11.14. A assistência técnica da garantia consiste na reparação das eventuais falhas dos equipamentos, mediante ao diagnóstico do software e substituição do equipamento defeituoso de acordo com os manuais e normas técnicas específicas para os equipamentos.

1.2.11.15. A **CONTRATADA** deverá prover os serviços de suporte, no nível 1, tendo capacitação para analisar problemas de configuração, parametrização, interoperabilidade e incompatibilidade do equipamento adquirido, e a Integração do mesmo com o ambiente do **CONTRATANTE**. Entende-se por:

1.2.11.15.1. Nível 1 - os serviços executados pela **CONTRATADA** por profissionais certificados pelo fabricante do produto ofertado; e

1.2.11.15.2. Nível 2 – os serviços prestados pelo fabricante, por profissionais certificados ao produto ofertado, via internet, por e-mail ou banco de conhecimento, ou ainda via telefone gratuito (0800) por intermédio da **CONTRATADA**.

1.2.11.16. O prazo para o atendimento será contado a partir da solicitação efetuada pelo **CONTRATANTE**, e não poderá ultrapassar os prazos descritos abaixo:

1.2.11.17. Prazo máximo de 3 (três) dias corridos para diagnóstico contados a partir do dia subsequente ao da abertura do chamado, para equipamentos instalados no **CONTRATANTE** localizadas nas capitais, caso o diagnóstico identifique problemas em software, após identificação 7 dias de solução a partir do dia subsequente. Em caso de diagnóstico de problemas de hardware a solução deverá ser de 15 dias úteis para substituição do equipamento defeituoso;

1.2.11.18. Entende-se por término do atendimento a disponibilidade do equipamento para uso em perfeitas condições de funcionamento no local onde está instalado, estando condicionado à aprovação do **CONTRATANTE**, através do setor competente;

1.2.11.19. Caso o equipamento não possa ser reparado dentro dos prazos previstos e antes de findar os prazos ali estabelecidos, a **CONTRATADA** deverá formalizar pedido de prorrogação, desde que disponibilizado previamente equipamento de backup, equivalente ou de configuração superior, cujas razões expostas serão examinadas pelo **CONTRATANTE**, que decidirá pela dilação do prazo ou aplicação das penalidades previstas no contrato;

1.2.11.20. Decorridos os prazos estipulados, sem o devido atendimento, fica o **CONTRATANTE** autorizado a contratar serviços emergenciais de suporte técnico e repassar os custos para a **CONTRATADA**;

1.2.11.21. Os serviços de assistência técnica deverão ser prestados pelo próprio fabricante ou empresa por ele designada, devendo esta ser autorizada pelo fabricante para manutenção dos equipamentos ofertados;

1.2.11.22. A **CONTRATADA** deverá trabalhar, ininterruptamente, na solução dos problemas até que a solução esteja novamente operando em regime normal de produção. Caso a solução do problema reportado exija a presença de analista da **CONTRATADA** nas dependências do **CONTRATANTE**, mesmo fora do horário comercial, este deverá ficar dedicado à resolução do problema até que ele esteja resolvido;

1.2.11.23. A **CONTRATADA** deverá informar ao **CONTRATANTE** o número do telefone para fins de esclarecimento de dúvidas relativas aos itens contratados, assim como para orientação e acompanhamento da solução de problemas quando não for demandada a presença de um técnico, a critério do **CONTRATANTE**;

1.2.11.24. Deverá ser informada página na Internet, do fabricante do (s) software (s), onde estejam disponíveis, últimas versões do (s) software (s) e informações sobre correções e

reporte de problemas, sem restrições de acesso público ou via cadastramento de pessoas autorizadas para o acesso. A página deverá conter, ainda, documentação técnica detalhada do (s) software (s) ofertado (s);

1.2.11.25. Todas as solicitações feitas pelo **CONTRATANTE** deverão ser registradas pela **CONTRATADA** em sistema informatizado para acompanhamento e controle da execução dos serviços;

1.2.11.26. O acompanhamento da prestação de serviço deverá ser por meio de um número de protocolo fornecido pela **CONTRATADA**, no momento da abertura da solicitação; e

1.2.11.27. Caso os serviços de assistência técnica da garantia não possam ser executados nas dependências do **CONTRATANTE**, o equipamento avariado poderá ser removido para o Centro de Atendimento da **CONTRATADA**, mediante justificativa por escrito da **CONTRATADA** e aceito pelo **CONTRATANTE**, observando a seguinte exigência:

1.2.11.27.1. O equipamento somente poderá ser retirado com autorização expressa de saída do equipamento, emitida pelo **CONTRATANTE** e por pessoa ou empresa designada pela **CONTRATADA**;

1.2.11.27.2. A saída só poderá ser autorizada mediante substituição por outro equivalente ou de superior configuração, durante o período de reparo;

1.2.11.27.3. O equipamento retirado para reparo deverá ser devolvido no prazo de 03 (três) dias úteis contados a partir da sua retirada;

1.2.11.27.4. A devolução de qualquer equipamento retirado para reparo deverá ser comunicada por escrito ao **CONTRATANTE**;

1.2.11.27.5. A critério da **CONTRATADA**, o componente defeituoso poderá ser trocado por outro de mesma marca e modelo, mediante informação ao gestor contendo detalhamento a respeito do número de série do novo componente, para fins de regularização patrimonial. Cabe ao **CONTRATANTE** informar a opção pela troca à localidade responsável para a devida regularização;

1.2.11.27.6. A substituição por equipamento de configuração superior somente será aceita após prévia homologação e aceitação pelo **CONTRATANTE**;

1.2.11.27.7. Toda e qualquer substituição de peças e componentes, sem ônus para o **CONTRATANTE**, deverá ser acompanhada pelo gestor do Contrato, o qual autorizará a substituição das peças e componentes;

1.2.11.27.8. As peças e componentes substituídos deverão ser novos e originais;

1.2.11.27.9. Após a conclusão da manutenção de qualquer equipamento, a **CONTRATADA** deverá gerar documento relatando as substituições de peças e componentes, contendo a identificação do chamado técnico, a data e hora do início e término do atendimento;

1.2.11.27.10. A **CONTRATADA** deverá comunicar ao **CONTRATANTE**, por escrito, sempre que constatar condições inadequadas de funcionamento ou má utilização a que estejam submetidos os equipamentos fornecidos, fazendo constar à causa de inadequação e a ação devida para sua correção;

1.2.11.27.11. A **CONTRATADA** deverá substituir o equipamento já instalado, por um novo e de primeiro uso, na hipótese da soma dos períodos de paralisação do equipamento ultrapassar 15 (quinze) dias úteis, dentro de qualquer período do contrato de 60 meses; e

1.2.11.27.12. O **CONTRATANTE** poderá fazer quaisquer ajustes de configuração em quaisquer itens ofertados, para adequação ao ambiente onde está instalado.

1.3. SONICWALL ANALYTICS GRUPO 1 - ITEM 03

1.3.1. DESCRIÇÃO TÉCNICA

1.3.1.1. Poderá ser composto de appliance ou máquina virtual únicos ou composição de appliances ou maquinas virtuais, de forma a atender a todos os requisitos solicitados sem perda de funcionalidade. Em caso de appliance o hardware deve ser do mesmo fabricante do equipamento de firewall.

1.3.1.2. Caso a solução entregue utilize virtualização deverá ser compatível com os seguintes Hypervisors: VMware ESX i v.5.5 / v6.0 / v6.6 / v6.7. Microsoft Hyper-V Win 2016.

1.3.1.3. Caso seja fornecida em appliance, ao mínimo 16 GB de memória RAM.

1.3.1.4. Caso a solução seja fornecida em appliance, o armazenamento total em disco deverá ser de no mínimo 2 TB. Estes discos poderão ainda ser substituídos pela **CONTRATANTE** / **CONTRATADA** sem a paralisação parcial ou total do sistema.

1.3.1.5. A plataforma deve permitir sincronização de tempo baseada em NTP;

1.3.1.6. A plataforma de relatórios deve ser do mesmo fornecedor dos appliances/firewalls, de forma a garantir plena compatibilidade entre os elementos do sistema.

1.3.1.7. Disponibilizar gerência remota, com interface gráfica nativa por acesso através de browsers, sem a necessidade de instalação de aplicativos complementares nas máquinas que realizarem os acessos.

1.3.1.8. Deve suportar acesso seguro via HTTPS, possibilitando inclusive redirecionamento HTTP/HTTPS.

1.3.1.9. Deve suportar, minimamente, os seguintes navegadores web:

1.3.1.9.1. Mozilla Firefox 37.0 ou superior;

1.3.1.9.2. Google Chrome 42.0 ou superior;

1.3.1.9.3. Safari 14.x ou superior.

1.3.1.10. Permitir acesso simultâneo por múltiplos usuários.

1.3.1.11. Console de monitoramento de status e saúde da infraestrutura do serviço, que permita identificar potenciais problemas e indicadores para a resolução rápida e efetiva.

1.3.1.12. Console com informações sobre licenciamento e suporte da plataforma de relatórios.

1.3.1.13.A interface gráfica deverá possuir mecanismo que permita a gerência e emissão de relatórios de forma remota.

1.3.1.14.Módulo dedicado ao gerenciamento da plataforma de relatórios, com acesso a logs e gestão dos elementos que compõem a solução (memória, espaço em disco, CPU).

1.3.1.15. Indicadores gráficos de saúde dos componentes da solução (memória, espaço em disco, CPU).

1.3.1.16. Console apresentando inventário geral dos appliances conectados à plataforma de relatórios.

1.3.1.17. Console permitindo o agrupamento dos appliances/firewalls com visualização por Grupos (ex.: departamentos, regiões, tipos, versões, modelos).

1.3.1.18. Prover capacidade de importar/exportar as configurações conectividade dos appliances/firewalls para finalidade de backup.

1.3.1.19. Fornecer indicadores gráficos de status de conectividade com os appliances/firewalls.

1.3.1.20. Deve permitir atualização de firmware/software da plataforma diretamente pela interface de gerenciamento remoto.

1.3.1.21. Deve permitir criação e restauração de backups de configuração e dados do sistema diretamente através da interface de gerenciamento remoto.

1.3.1.22. Deve permitir o agendamento de backups.

1.3.1.23. Deve fornecer console de busca de logs, com critérios de pesquisa que incluam, mas não se restrinjam a: (Palavras e Combinação de palavras).

1.3.1.24. Deve listar usuários conectados à plataforma.

1.3.1.25. Deve permitir customizar características dos relatórios como: capa, logomarca.

1.3.1.26. Deve permitir o agendamento de envio automático de relatórios.

1.3.1.27. Deve permitir configuração do tempo de retenção de registros (logs) na plataforma, com mínimo estabelecido de 12 meses.

1.3.1.28.A plataforma de relatórios deve permitir o agrupamento de appliances/firewalls, possibilitando melhor visualização de acordo com a topologia de rede e distribuição dos dispositivos associados.

1.3.1.29. Também deve ser oferecer agrupamento de dispositivos à visibilidade do status de conectividade dos appliances associados à plataforma de relatórios, com alarmes indicativos de status de conexão.

1.3.1.30. Deve oferecer relatórios globais (agrupados) e individuais (por appliance/firewall), com indicadores consolidados que incluam, mas se limitem a:

1.3.1.31. Consumo de banda, informando:

1.3.1.31.1. Utilização histórica x tempo;

1.3.1.31.2. Origem das conexões;

1.3.1.31.3. Destino das conexões;

1.3.1.31.4. Serviços e/ou aplicações utilizadas;

1.3.1.31.5. Informação dos países de origem das conexões (Geo-localização); e

1.3.1.31.6. Informações dos países de destino das conexões (Geo-localização).

1.3.1.32. Aplicações utilizadas, informando:

1.3.1.32.1. Volume de dados utilizado;

1.3.1.32.2. Aplicações detectadas pelo appliance/firewall, indicando seu nível de risco para a rede/usuário;

1.3.1.32.3. Aplicações bloqueadas pelo appliance/firewall;

1.3.1.32.4. Categoria associada às aplicações detectadas e/ou bloqueadas; e

1.3.1.32.5. Originador da utilização da aplicação.

1.3.1.33. Atividade de usuários, informando:

1.3.1.33.1. Usuário;

1.3.1.33.2. IP associado ao usuário;

1.3.1.33.3. Endereço MAC do dispositivo utilizado para o acesso; e

1.3.1.33.4. Aplicação utilizada.

1.3.1.34. Filtro de navegação WEB, informando:

1.3.1.34.1. Categorias associadas aos sites/portais acessados;

1.3.1.34.2. Lista de sites/portais acessados;

1.3.1.34.3. Originadores das solicitações de navegação, contendo Usuário, endereço IP associado ao usuário, endereço MAC do dispositivo associado à navegação, tempo de navegação, volume de dados transferidos;

1.3.1.34.4. Informação dos países de origem das conexões (Geo-localização); e

1.3.1.34.5. Informações dos países de destino das conexões (Geo-localização).

1.3.1.35. Atividade de navegação WEB, informando:

1.3.1.35.1. Categorias associadas aos sites/portais acessados;

1.3.1.35.2. Lista de sites/portais acessados;

1.3.1.35.3. Originadores das solicitações de navegação, contendo Usuário, endereço IP associado ao usuário, endereço MAC do dispositivo associado à navegação, tempo de navegação, volume de dados transferidos;

1.3.1.35.4. Informação dos países de origem das conexões (Geo-localização); e

1.3.1.35.5. Informações dos países de destino das conexões (Geo-localização).

1.3.1.36. Utilização de VPN, informando:

1.3.1.36.1. Origem da conexão;

1.3.1.36.2. Serviços/aplicações utilizados através da conexão;

1.3.1.36.3. Registro de tempo (timestamp) das conexões;

1.3.1.36.4. Eventos de Intrusão (IPS), informando:

1.3.1.36.5. Eventos detectados;

1.3.1.36.6. Eventos bloqueados;

1.3.1.36.7. Alvos dos eventos (ataques);

1.3.1.36.8. Iniciadores da sessão que originou o evento;

1.3.1.36.9. Histórico temporal dos eventos;

1.3.1.36.10. Categorias associadas aos eventos;

1.3.1.36.11. Informação dos países de origem das conexões (Geo-localização); e

1.3.1.36.12. Informações dos países de destino das conexões (Geo-localização).

1.3.1.37. Eventos relacionados a Botnets, informando:

1.3.1.37.1. Eventos detectados;

1.3.1.37.2. Origem e destino das conexões;

1.3.1.37.3. Informação dos países de origem das conexões (Geo-localização);

1.3.1.37.4. Informações dos países de destino das conexões (Geo-localização);

1.3.1.37.5. Eventos relacionados a Vírus, Malware, Spyware, informando:

1.3.1.37.6. Vírus bloqueados;

1.3.1.37.7. Destino da máquina/usuário objeto do ataque;

1.3.1.37.8. Iniciador da conexão;

1.3.1.37.9. Registro temporal dos eventos;

1.3.1.37.10. Informação dos países de origem das conexões (Geo-localização);

1.3.1.37.11. Informações dos países de destino das conexões (Geo-localização.

1.3.1.38. Deve possibilitar customização dos relatórios, considerando os quesitos acima mencionados como variáveis selecionáveis, de forma a atender aos requisitos específicos do usuário.

1.3.1.39. Além de relatórios, a plataforma deve propiciar acesso e busca de informações nos registros/logs primários (syslogs) enviados pelos appliances/firewalls diretamente a partir da interface gráfica de acesso à plataforma.

1.3.1.40. A plataforma deve permitir o agendamento de envio automático de relatórios por e-mail.

1.3.1.41. A garantia de funcionamento deste item será do Fabricante, pelo período de 60 (sessenta) meses contada a partir da ativação da licença, sem prejuízo de qualquer política de garantia adicional oferecido.

1.4. SOFTWARE NETWORK SECURITY MANAGER - GRUPO 1 - ITEM 05

1.4.1. DESCRIÇÃO TÉCNICA

1.4.1.1. Poderá ser composto de appliance ou máquina virtual, de forma a atender a todos os requisitos solicitados sem perda de funcionalidade.

1.4.1.2. A solução deverá ser do mesmo fabricante do equipamento de firewall.

1.4.1.3. Deve ser separada do gateway de segurança e gerenciar políticas de segurança de todos os firewalls.

1.4.1.4. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança, possibilitando geração de relatórios analíticos e de forma centralizada de todos os dispositivos gerenciados.

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

1.4.1.6. A solução deve permitir controle granular do acesso dos administradores, utilizando controle de acesso do tipo RBAC (Role based access control), aumentando a segurança e integridade da plataforma.

1.4.1.7. A solução deve permitir que os administradores façam autenticação no console utilizando no mínimo dois fatores de autenticação, 2FA (two factors authentication).

1.4.1.8. A solução deve fornecer uma ferramenta de gestão centralizada capaz de reunir todos os equipamentos sob uma única interface gráfica, possibilitando o gerenciamento unificado de políticas e regras de todos os firewalls ofertados.

1.4.1.9. A solução deve fornecer uma ferramenta de gestão centralizada capaz de reunir todos os equipamentos sob uma única interface gráfica, possibilitando o gerenciamento unificado de políticas e regras de todos os firewalls ofertados.

1.4.1.10. A solução deve permitir tecnologia de “Zero touch” para os dispositivos de NGFW.

1.4.1.11. A solução deve possuir tela situacional com todo os inventario de firewalls gerenciados centralizadamente, informando no mínimo para o administrador, nome do Hostname do firewall, número de série, modelo, versão do firmware e status da conectividade do equipamento com a gerência em online ou off-line.

1.4.1.12. Deve ser possível visualizar a último horário de comunicação entre o firewall e a gerência, onde deve ser informado ao administrador, pela console, se a configuração do dispositivo está sincronizada ou não.

1.4.1.13. A solução deve oferecer as funcionalidades de backup de configurações dos equipamentos gerenciados, permitindo que o administrador possa agendar procedimentos de backup em dias ou horários específicos e exportá-los e acordo com o agendamento.

1.4.1.14. A solução deve oferecer as funcionalidades de backup e agendamento de arquivo com informações técnicas do dispositivo para utilização do suporte técnico do fabricante.

1.4.1.15. Deverá permitir atualizar o sistema operacional de múltiplos equipamentos gerenciados de uma única vez.

1.4.1.16. Deverá permitir atualizar o sistema operacional dos equipamentos gerenciados, onde deverá ser possível criar agendamento para a atualização.

1.4.1.17. Deve centralizar a administração de regras e políticas do (s) cluster (s), usando uma única interface de gerenciamento.

1.4.1.18. A solução deverá permitir seu gerenciamento por Web GUI utilizando protocolo HTTPS sem a necessidade de uso de cliente ou console do tipo aplicativo.

1.4.1.19. Deve manter um canal de comunicação segura, com encriptação baseada HTTPS, entre todos os componentes que fazem parte da solução de firewall, gerência.

1.4.1.20. A solução deverá permitir que a partir da console de gerência centralizada seja feito conexão no console de gerência local do firewall sem a necessidade do administrador utilizar endereço IP do dispositivo, URL ou FQDN.

1.4.1.21. A solução de gerência deve prover fácil administração na aplicação das políticas para os gateways, sendo capaz de realizar o processo de alteração de políticas e configuração de todos os firewalls em uma única sessão, evitando qualquer tipo de retrabalho de configuração e aplicação de regra.

1.4.1.22. A solução deve permitir a criação de modelos de configuração ou “Templates” para aplicá-los em grupos de dispositivos. Os modelos de configurações devem permitir visualização e edição para sua aplicação nos firewalls.

1.4.1.23. Os modelos de configuração ou “templates” devem suportar configurações de interfaces físicas ou virtuais.

1.4.1.24. A solução deve permitir a criação de grupos lógicos, para o agrupamento de dispositivos, com isso permitindo a aplicação de modelos de configuração a diversos equipamentos de uma única vez.

1.4.1.25. A solução deverá contar com tela situacional para a gestão de configurações e mudanças das políticas de segurança, onde deve permitir visualizar as alterações feitas pelos administradores, como exemplo, mas não limitado há: data e horário da aplicação das alterações, quantidade de dispositivos afetados pelas alterações, sumario da alteração, status de sucesso ou insucesso da alteração e comentários deixados pelo administrador durante a alteração das políticas.

1.4.1.26. Deverá suportar API (interface de programação de aplicativo) RESTFUL para criação de scripts personalizados para gerenciar e configurar e os equipamentos de acordo com a necessidade de customização do administrador.

1.4.1.27. Para cada alteração configurada nos firewalls, o sistema de gerenciamento centralizado deverá possibilitar a visualização e o download dos comandos enviados ao gateway, em formato de API, para o uso do administrador.

1.4.1.28. Deverá permitir visualizar a diferença nas mudanças antes que a configurações sejam implantadas.

1.4.1.29. De forma centralizada deve permitir gerenciar, mas não limitado há, políticas de firewall, NAT, rotas, PBR (Policy Based Routing), configuração de endereçamento IP das interfaces dos equipamentos, criação e administração de políticas de IPS, configuração de políticas de antivírus e anti-malware, configuração e criação de políticas de controle de URL, criação e configuração de políticas de controle de aplicações, criação e configuração de políticas de SANDBOX, criação e configuração de políticas de controle de banda, criação e configuração de objetos necessários para configuração das políticas especificadas acima, usando uma única interface de gerenciamento.

1.4.1.30. Deverá possibilitar a criação de políticas SD-WAN, baseando-se em parâmetros de latência, perda de pacote e jitter, para a tomada de decisão de encaminhamento de tráfego no firewall.

1.4.1.31. Registrar em log de auditoria as ações dos usuários administradores, registrando todas as alterações realizadas em uma política de segurança, permitindo a identificação do responsável pela mudança, o horário e a origem.

1.4.1.32. A solução deverá permitir o rastreamento e auditoria das alterações de políticas e configurações de no mínimo dos últimos 20 dias.

1.4.1.33. Para cada alteração de configuração a solução deverá confirmar a aplicação da política, possibilitando a adição de comentários nas políticas instaladas, para futuras consultas de auditoria.

1.4.1.34. Durante a alterações de políticas de segurança dos firewalls, deverá ser possível o agendamento para determinar o horário que as mudanças entrarão em vigor, proporcionando ao administrador aplicar políticas de segurança em horários com menor impacto para o ambiente.

1.4.1.35. Permitir a criação de janela de mudança podendo executar regras imediatamente ou criar um agendamento.

1.4.1.36. Deverá permitir que configurações realizadas pelos administradores da solução sejam validadas e aprovadas (workflow), por um colaborador responsável por aprovação e aplicação de políticas, esse processo de aprovação deve ser encaminhado de forma automatizada para o responsável da aprovação via e-mail ou console da solução, possibilitando mitigar erros de configuração e impactos negativos ao ambiente de segurança da informação do órgão.

1.4.1.37. A funcionalidade de Workflow deve permitir o administrador definir se o processo de aprovação por um usuário será completo ou parcial, para que possa ser definido se o processo de aprovação terá apenas um aprovador ou vários aprovadores.

1.4.1.38. A funcionalidade de Workflow deve permitir configurar, em dias, a validade dos pedidos de aprovação, caso o pedido de aprovação não seja aprovado no período configurado, essa mudança deve ser expirada e não efetivada.

1.4.1.39. A funcionalidade de Workflow deve permitir o administrador criar de grupos de aprovação com os aprovadores e e-mails que receberão a notificação de pendência de aprovação.

1.4.1.40. A Solução deverá permitir visualizar a topologia na qual determinado firewall está inserida.

1.4.1.41. A solução deverá permitir visualizar sumario com as informações referentes as principais ameaças protegidas pelos firewalls.

1.4.1.42. Deverá receber suportar logs do tipo Netflow, IPFIX ou Syslog, para a gerar reports.

1.4.1.43. A solução deverá prover relatórios com no mínimo histórico de 365 dias.

1.4.1.44. A solução deverá prover relatórios referente as atividades dos usuários.

1.4.1.45. A solução deverá prover relatórios referente ao uso de aplicações web, com no mínimo as seguintes informações, nome da aplicação, quantidade de conexões e percentual que a aplicação representa do tráfego da rede, quantidade de Megabytes trafegados, quantidades de bloqueios que existe para a Aplicação, nível de risco e categoria da aplicação.

1.4.1.46. A solução deverá prover relatórios referente ao consumo de rede dos usuários, com no mínimo as seguintes informações, nome do usuário, quantidade de conexões e percentual que tráfego do usuário representa na rede, quantidade de Megabytes trafegados, quantidades de bloqueios de tráfego para o usuário e quantidade de vírus/spyware/intrusões encontrado no tráfego dos usuários.

1.4.1.47. Caso o administrador não habilitado a funcionalidade de identificação do usuário, a solução deverá identificar as informações acima como usuário desconhecido.

1.4.1.48. A solução deverá prover relatórios referente ao consumo de rede por endereço IP, com no mínimo as seguintes informações, endereço IP, quantidade de conexões e percentual que tráfego que o IP representa na rede, quantidade de Megabytes trafegados, quantidades de bloqueios de tráfego para o endereço IP e quantidade de vírus/spyware/intrusões encontrado no tráfego.

1.4.1.49. A solução deverá prover relatórios referente aos acessos geográficos, com no mínimo as seguintes informações, país de origem/destino do tráfego, quantidade de conexões e percentual que tráfego que do país representa na rede, quantidade de Megabytes trafegados do todo, quantidade de Megabytes enviados e recebidos por país.

1.4.1.50. A solução deverá prover relatórios referente aos acessos web com no mínimo informações referentes as categorias acessadas, quantidade de conexões e percentual que cada categoria web representou no tráfego de rede.

1.4.1.51. A solução deverá permitir criar agendamentos para geração automática de relatórios no formato PDF, possibilitando o envio dos relatórios agendados via e-mail.

1.4.1.52. A solução deve possuir tela situacional com informações referente a geração dos relatórios agendados, informando se houve sucesso, falha ou se existe relatórios em progresso.

1.4.1.53. A solução deverá arquivar os relatórios gerados automaticamente, permitindo o administrador fazer o download em formato PDF. e

1.4.1.54. A garantia de funcionamento deste item será do Fabricante, pelo período de 60 (sessenta) meses contada a partir da ativação da licença, sem prejuízo de qualquer política de garantia adicional oferecido.

1.5. SOLUÇÃO WIRELESS SONICWAVE 231C OU MODELO SUPERIOR– GRUPO 1 - ITEM 06

1.5.1. DESCRIÇÃO TÉCNICA

1.5.1.1. Aquisição de equipamento Sonicwall Wireless Sonicwave 231C ou modelo SUPERIOR.

1.5.1.1. Possuir estrutura que permita a utilização do equipamento em locais internos, com fixação em teto.

1.5.1.2. Esse equipamento deve possuir total integração com o firewall, o firewall que fará o papel de controlador da rede Wireless.

1.5.1.3. Deverá acompanhar kit para fixação do Access point nas paredes ou teto.

1.5.1.4. Operar simultaneamente nas frequências de 2.4GHz e 5GHz, com rádios distintos.

1.5.1.5. Permitir a criação de – no mínimo – 8 SSID's – para cada rádio.

1.5.1.6. Permitir a configuração de Hidden SSID's (SSID's ocultos).

1.5.1.7. Suportar os padrões IEEE 802.11 a/b/g/n/ac.

1.5.1.8. Deverá suportar os padrões IEEE 802.11r (fast transition), IEEE 802.11k, IEEE 802.11v.

1.5.1.9. Operar com tecnologia do tipo "MIMO (Multiple Input/Multiple Output)" do tipo "multi-user", MU-MIMO.

1.5.1.10. Deverá possuir mecanismo de rádio com suporte à MU-MIMO 2x2.

1.5.1.11. Suportar no mínimo 128 usuários conectados por rádio.

1.5.1.12. Possuir antenas internas e integradas com padrão de irradiação omni-direcional.

1.5.1.13. Compatíveis com as frequências de rádio dos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n e IEEE 802.11AC.

1.5.1.14. Implementar, pelo menos, os seguintes padrões de segurança wireless:

1.5.1.14.1. Wi-Fi Protected Access (WPA) com algoritmo de criptografia TKIP (Temporal Key Integrity Protocol);

1.5.1.14.2. Wi-Fi Protected Access 2 (WPA2) com os seguintes algoritmos, Advanced Encryption Standard (WPA2-AES) e IEEE 802.11i; e

1.5.1.14.3. Deverá suportar Beamforming;

1.5.1.15. Possuir capacidade de selecionar automaticamente o canal de transmissão.

1.5.1.16. O equipamento deve ser capaz de implementar 802.11 Dynamic Frequency Selection (DFS).

1.5.1.17. A solução wireless deve implementar mecanismo que permita às estações se conectarem ao rádio com melhor throughput, ao invés do rádio com melhor sinal, através do padrão RRM (Radio Resource Management) IEEE 802.11k ou similar, evitando sobrecarga nos Pontos de Acesso.

1.5.1.18. Deverá ser fornecido com todas as licenças para funcionamento em MESH (WiFi Mesh).

1.5.1.19. Deve suportar mecanismo que identifique e associe clientes preferencialmente na banda de 5 GHz, deixando a banda de 2,4 GHz livre para dispositivos que trabalhem somente nesta frequência.

1.5.1.20. Possuir tecnologia “Airtime Fairness” permitindo melhor desempenho da rede wireless.

1.5.1.21. Permitir alimentação elétrica por meio de Power Over Ethernet (PoE), padrão 802.3at.

1.5.1.22. Os injetores PoE deverão ser fornecidos juntamente com os equipamentos AP.

1.5.1.23. Alternativamente, a **CONTRATADA** poderá fornecer um switch com alimentação PoE e com quantidade de portas suficientes para conectar e alimentar eletricamente os equipamentos AP objeto deste Edital.

1.5.1.24. Possuir capacidade de selecionar dinamicamente a frequência de operação (DFS).

1.5.1.25. Permitir o controle da potência de transmissão (Transmit Power Control - TPC).

1.5.1.26. Suportar padrão de criptografia WPA2 Personal e WPA2 Enterprise.

1.5.1.27. Possuir radio dedicado para detectar ataques do tipo “Rogue AP”, ou seja, detectar a existência em funcionamento de outros equipamentos AP cuja instalação/operação/sinal de rádio não tenha sido autorizado para uso.

1.5.1.28. Deve, juntamente com a solução de Controladora Wireless, detectar e gerar alarmes de interferências WiFi provenientes de dispositivos padrão IEEE 802.11.

1.5.1.29. Possuir funcionalidade de visualização de dispositivos conectados e histórico das conexões.

1.5.1.30. Permitir atualização de firmware através da controladora centralizada.

1.5.1.31. Possuir, no mínimo, 01 (uma) interface IEEE 802.3 10/100/1000 Mbps Base-T Ethernet, autosensing, com conector RJ-45, para conexão à rede local fixa.

1.5.1.32. Possuir interface USB dedicada para conexão de modens 3G/4G permitindo configurar uma saída de internet por esta conexão.

1.5.1.33. Implementar cliente DHCP, para configuração automática do seu endereço IP.

1.5.1.34. Deve suportar VLAN seguindo a norma IEEE 802.1q.

1.5.1.35. Deverá ser apresentado certificado válido de interoperabilidade fornecido pela Wi-Fi Alliance na categoria de Enterprise Access Point.

1.5.1.36. Possuir LEDs para a indicação do status: portas ethernets, rede wireless, e atividades do equipamento.

1.5.1.37. Deve suportar temperatura de operação entre 0°C a 40°C.

1.5.1.38. A garantia de funcionamento do hardware será do Fabricante, pelo período de 60 (sessenta) meses contada a partir da ativação do produto, sem prejuízo de qualquer política de garantia adicional oferecido.

1.6. SERVIÇO DE INSTALAÇÃO GRUPO 1 – ITEM 07

1.6.1. DESCRIÇÃO TÉCNICA

1.6.1.1. A realização do serviço deve ser planejada de acordo com disponibilidade de ambas as partes.

1.6.1.2. O planejamento anterior ao serviço deverá ser realizado de forma on-site nas dependências da **CONTRATANTE** Sede (Matriz) em Brasília.

1.6.1.3. A instalação física e configuração da solução de equipamentos e softwares Sonicwall, deverá ser realizado de forma on-site nas dependências da **CONTRATANTE** Sede (Matriz) em Brasília.

1.6.1.4. Deverá contemplar a instalação física do firewall, substituindo os atuais equipamentos pelos novos no rack.

1.6.1.5. Deverá contemplar instalação física dos Access Points na localidade designada pela **CONTRATANTE** e atualização de firmware do Appliance, se necessário. A **IMBEL** possui 09 Access Points em produção na SEDE, o serviço de instalação deve contemplar a substituição desses equipamentos.

1.6.1.6. A **CONTRATADA** deve exportar os arquivos de configuração do TZ600 e importar para o novo equipamento TZ670.

1.6.1.7. Deverá contemplar a instalação e configuração do SOFTWARE NETWORK SECURITY MANAGER e SOFTWARE ANALYTICS, integrando a comunicação com todos os equipamentos da Sonicwall na SEDE e Fábricas.

1.6.1.8. A solução Wireless deverá ser integrada ao Firewall, Software de Gerência centralizada e Software Analytics, garantindo seu pleno funcionamento. Conforme plano de instalação previamente estabelecido com a **CONTRATANTE**.

1.6.1.9. Deve configurar a autenticação dos usuários no firewall integrando a comunicação do Active Directory através do Single Sign On.

1.6.1.10. Neste documento devem conter a relação, descrição e quantidades dos produtos fornecidos, descrição da infraestrutura atual e desejada, detalhamento dos serviços que serão executados, premissas do projeto, locais e horários de execução dos serviços, condições de execução dos serviços, pontos de contato da **CONTRATADA** e **CONTRATANTE**, cronograma de execução do projeto em etapas, com responsáveis e data e início e fim (se aplicável), relação da documentação a ser entregue ao final da execução dos serviços, responsabilidade da **CONTRATADA**, plano de gerenciamento de mudanças, itens excluídos no projeto e termo de aceite.

1.6.1.11. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes.

1.6.1.12. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, devendo a **CONTRATADA** sugerir as configurações de acordo com normas técnicas e boas práticas, cabendo à **CONTRATANTE** a sua aceitação expressa ou recusa nos casos de não atendimento das condições estabelecidas.

1.6.1.13. Após a instalação, a solução deverá ser monitorada remotamente pelo prazo de 15 dias, observando as condições de funcionamento e performance dos equipamentos, sendo possível o troubleshooting em caso de problemas ou não conformidades na operação.

1.6.1.14. Durante as atividades realizadas na prestação do serviço, o técnico da **CONTRATADA** deverá demonstrar à equipe técnica de acompanhamento da **CONTRATANTE** como instalar e configurar os equipamentos e os softwares fornecidos (instalação assistida).

1.6.1.15. As atividades deverão ser realizadas, sempre que possível, dentro do horário comercial; Todas as atualizações de firmware ou qualquer outro software componentes da solução, para a versão mais atualizada disponível ou a última compatível com as demais soluções deste lote e considerada estável.

1.6.1.16.A implantação deverá abranger quaisquer funcionalidades suportadas pela solução as quais poderão fazer parte do escopo do projeto. Estas informações serão documentadas no termo de abertura do projeto a ser documentado pela **CONTRATADA** após alinhamento do escopo de trabalho entre **CONTRATADA** e **CONTRATANTE**.

1.6.1.17. Ao final da instalação, deverá ser realizado o repasse de configurações hands-on, de forma on-site nas dependências da **CONTRATANTE** apresentando as configurações realizadas. A **CONTRATANTE** disponibilizará o local adequado para a transferência do conhecimento e acesso a solução em produção.

1.6.1.18. Os serviços deverão ser realizados por pessoal técnico experiente e certificado pelo fabricante da solução. Em momento anterior à instalação, a **CONTRATANTE** poderá solicitar os comprovantes da qualificação profissional do (s) técnico (s) que executará (ão) os serviços, sendo direito da mesma a sua aceitação ou exigência de troca de profissional no caso de este não satisfazer às condições supramencionadas.

1.6.1.19. Ao término dos serviços deve ser criado um relatório detalhado contendo todos os itens configurados no projeto (relatório as-built), etapas de execução e toda informação pertinente para posterior continuidade e manutenção da solução instalada, como usuários e endereços de acesso, configurações realizadas e o resumo das configurações dos equipamentos.

1.6.1.20. Este relatório deve ser enviado com todas as informações em até 15 dias após a finalização dos serviços.

1.6.1.21. Nos valores cotados devem estar inclusas todas as despesas com deslocamento, alimentação e estadia para realização dos serviços (onsite) nos locais de presença da **CONTRATANTE**. Os funcionários da **CONTRATADA** deverão possuir todo o ferramental necessário ao exercício das suas atividades.

1.6.1.22.A **CONTRATADA** deverá garantir a confidencialidade das informações, dados e senhas compartilhadas da **CONTRATANTE**.

CLÁUSULA SEGUNDA - DO PRAZO DE ENTREGA DO OBJETO

O prazo de entrega e da prestação do serviço será de 30 (trinta) dias corridos a partir do dia útil imediato ao da assinatura deste contrato.

CLÁUSULA TERCEIRA - DA CONFIDENCIALIDADE

A **CONTRATADA** deverá respeitar e assegurar o sigilo relativamente às informações obtidas durante a execução dos serviços, não as divulgando, sob nenhuma circunstância, sem autorização expressa da **IMBEL**, salvo quando houver obrigação legal de fazê-lo.

CLÁUSULA QUARTA - DA FORMA DE PAGAMENTO

4.1. O pagamento pelos materiais entregues e os serviços efetivamente prestados, será efetuado em até 30 (trinta) dias após a entrega da Nota Fiscal/Fatura correspondente.

4.2. Na ocorrência de erros na(s) Nota(s) Fiscal(is) do(s) Serviço(s)/Fatura(s) ou situação que impeça a liquidação da despesa, aquela(s) será(ão) devolvidas(s) e o pagamento ficará pendente até que as medidas saneadoras sejam providenciadas pela **CONTRATADA**.

4.3. Na hipótese acima mencionada, a contagem do prazo para pagamento será iniciada após a correção dos erros identificados e reapresentação da(s) Nota(s) Fiscal(is) do(s) Serviço(s)/Fatura(s), não acarretando qualquer ônus para a **CONTRATANTE**.

4.4. O pagamento será efetuado em favor da **CONTRATADA** através de ordem bancária, devendo para isso ficar explicitado o nome da instituição financeira recebedora, agência, localidade, número da operação, quando for o caso, e número da conta corrente na qual deverá ser depositado o crédito, que ocorrerá após mediante a aceitação e atesto na(s) Nota(s) Fiscal(is) do(s) Serviço(s)/Fatura(s), pelo fiscal do contrato em até 3 (três) dias úteis.

4.5. Será realizada consulta "*ON LINE*" ao Sistema de Cadastro de Fornecedores - SICAF antes do pagamento a ser efetuado a **CONTRATADA**, para a verificação de sua situação, no que diz respeito às condições exigidas para contratação, cujo resultado será impresso e juntado aos autos processuais próprios.

4.6. Constada a não regularidade junto ao SICAF, a **CONTRATADA** será acionada para que no prazo de 5 (cinco) dias úteis regularize a sua situação, contados da data da notificação.

4.7. Não sendo regularizada a situação no prazo acima estabelecido, o contrato poderá ser rescindido e a **CONTRATADA** sujeita às multas estabelecidas.

4.8. Dos pagamentos devidos à **CONTRATADA** serão descontados os impostos e contribuições de acordo com os ditames estabelecidos na legislação de regência.

4.9. O pagamento somente será efetuado quando do recolhimento de eventuais multas que tenham sido impostos à **CONTRATADA** em decorrência de inadimplemento contratual.

4.10. A **IMBEL** reserva-se o direito de suspender o pagamento caso os serviços sejam entregues em desacordo com este contrato.

4.11. No caso de eventuais atrasos de pagamento provocados exclusivamente pela **IMBEL**, o valor devido deverá ser acrescido de atualização financeira e a sua apuração se fará desde a data do vencimento da fatura até a data do efetivo pagamento, em que os juros de mora serão calculados à taxa de 0,5% (meio por cento) ao mês, ou 6% (seis por cento) ao ano, mediante a aplicação da seguinte fórmula:

$$I = \frac{(\frac{TX}{100})}{365}$$

EM = I x N x VP, onde:

I = Índice de atualização financeira.

TX = Percentual da taxa de juros de mora anual.

EM = Encargos moratórios.

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento.

VP = Valor da parcela em atraso.

4.12. Em hipótese alguma será admitida antecipação do pagamento.

CLÁUSULA QUINTA - DO REGIME DE EXECUÇÃO

O objeto do presente contrato será executado pela **CONTRATADA** sob o regime de execução da forma indireta de empreitada por preço unitário.

CLÁUSULA SEXTA - DO VALOR DO CONTRATO

O valor global deste contrato, consoante o contido na proposta da **CONTRATADA**, é de R$ 335.350,00 (trezentos e trinta e cinco mil, trezentos e cinquenta reais).

CLÁUSULA SÉTIMA - DA DOTAÇÃO ORÇAMENTÁRIA

A despesa orçamentária para a execução do presente contrato correrá por conta da Natureza de Despesa 339040 / 449052, PI B1DAATSSTIC / B1DIINVSTIC, Fonte de recurso 0100 / 0150.

CLÁUSULA OITAVA - DO PRAZO PARA EXECUÇÃO DO CONTRATO E DA PUBLICAÇÃO

8.1. O prazo execução do contrato, será de 12 (doze) meses contados a partir do dia da sua assinatura, podendo ser prorrogado até o limite de 60 (sessenta) meses.

8.2. A não renovação deste contrato, não libera a **CONTRATADA** de prestar a Garantia e Suporte de 60 (sessenta) meses do Appliance Hiperconvergente do Servidor de Rede, conforme previsto neste contrato e no Termo de Referência.

8.3. A **IMBEL** providenciar a publicação resumida do contrato se houver, até o quinto dia útil do mês seguinte ao da sua assinatura de acordo com o § único do Art. 169 do Regulamento de Licitações e Contratos da **IMBEL**.

CLÁUSULA NONA - DO PREÇO POR ITEM

9.1. Nos preços cotados deverão estar inclusos todos os valores que os compõem, tais como impostos, taxas, frete e outros que incidam direta ou indiretamente no preço final.

9.2. Os preços a serem praticados neste contrato, são os constantes da tabela abaixo:

GRUPO	ITEM	ESPECIFICAÇÃO	UND	QUANT	VALOR UNIT.	VALOR TOTAL
1	01	Firewall, Aplicação: Segurança Rede Computadores, Modelo: Sonicwall Tz670, em cluster, Capacidade Armazenamento interno: Até 256 GB e demais especificações técnicas detalhadas neste TR.	Und	01	R$ 62,000,00	R$ 62.000,00
	02	Essential Protection Service Suite For TZ670, coberto pela garantia e suporte de 60 meses		01	R$ 73.000,00	R$ 73.000,00
	03	Sonicwall Analytics (Syslog) for TZ670/TZ670W Series, coberto pela garantia e suporte de 60 meses		01	R$ 7.000,00	R$ 7.000,00
	04	SSL-VPN for TZ670		150	R$ 115,00	R$ 17.250,00
	05	Software de gerenciamento Network Security Manager 06 nodes, com requisitos de segurança e serviços de suporte 24x7 coberto pela Garantia de 60 meses.		01	R$ 49.000,00	R$ 49.000,00
	06	Equipamento Wireless Sonicwave 231C ou modelo Superior, Padrão: 802.11 A/B/G/N/Ac, Frequência: 5 -2,4 GHZ, Aplicação: Conexão Sem Fio De Equipamentos Em Rede e demais especificações técnicas detalhadas neste TR.		09	R$ 11.900,00	R$ 107.100,00
	07	Serviço de Instalação Migração e Configuração para o TZ670, NSM, Analytics e Sonicwave.		01	R$ 20.000,00	R$ 20.000,00
VALOR GLOBAL						**R$ 335.350,00**

9.3. Desde já fica empenhado o valor de R$ 335.350,00 (trezentos e trinta e cinco mil, trezentos e cinquenta reais), referente as Notas de Empenhos n^{os} 2022NE000338, de 21/06/2022; 2022NE000332 e 2022NE000333, ambas de 20/06/2022.

CLÁUSULA DÉCIMA – DA LEGISLAÇÃO APLICÁVEL

Aplica-se à execução deste contrato, inclusive aos casos omissos, a Lei nº 13.303, de 2016, o Decreto nº 8.945 de 2016, a Lei Complementar nº 123, de 2006, a Lei nº 12.846, de 2013, o Regulamento de Licitações e Contratos da **IMBEL**, aprovado na 305ª Reunião do Conselho de Administração da **IMBEL**, ocorrida em 22/05/2018, conforme Resolução nº 06/2018-CA-**IMBEL**, de 22/05/2018, e as normas de direito civil acerca da matéria.

CLÁUSULA DÉCIMA PRIMEIRA DAS OBRIGAÇÕES E DIREITOS DA CONTRATADA

11.1. Executar os serviços e entregar o material de acordo com as especificações exigidas e da proposta apresentada, bem como de cumprir todos os requisitos de acordo com as condições gerais e prazos para a execução do objeto assentados no Termo de Referência.

11.2. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado, os serviços efetuados e os materiais em que se verificarem vícios, defeitos ou incorreções resultantes da execução dos serviços ou dos materiais entregues.

11.3. Responsabilizar-se pelos vícios e danos decorrentes da execução dos serviços contratados e entrega do material, de acordo com os artigos 14 e 17 a 11 do Código de Defesa do Consumidor (Lei nº 8.078/90), ficando a **CONTRATANTE** autorizada a descontar do pagamento devido à **CONTRATADA** o valor correspondente aos danos por ela sofridos.

11.4. Utilizar, somente, de empregados habilitados e com conhecimentos básicos acerca dos serviços a serem executados, em conformidade com as normas e determinações vigentes.

11.5. Assumir e responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e todas as demais previstas na legislação vigente, cuja inadimplência não transfere responsabilidade à **CONTRATANTE**, como também por quaisquer danos que eventualmente venham a ser causados por seus empregados no que se refere aos serviços e o material entregue executados para consecução do objeto licitado.

11.6. Relatar à **CONTRATANTE** toda e qualquer ocorrência de irregularidade verificada no decorrer da prestação dos serviços e da entrega do material, para fins de correção.

11.7. Manter em compatibilidade com as obrigações assumidas, todas as condições de habilitação e de qualificações previstas neste contrato e no edital.

11.8. Guardar sigilo sobre os dados cadastrais e todas as informações obtidas, sendo vedado, sob qualquer argumento, utilizá-las em benefício próprio, revelar, reproduzir ou delas dar conhecimento a terceiros, responsabilizando-se em caso de descumprimento, por eventuais perdas e danos, sujeitando-se às cominações legalmente estabelecidas.

11.9. Prestar todo e qualquer esclarecimento solicitado pela **IMBEL**, no que diz respeito ao objeto contratado.

11.10. Comunicar imediatamente à **CONTRATANTE**, por escrito, as dificuldades de qualquer ordem ou natureza que eventualmente surjam durante a execução do objeto.

11.11. Os serviços devem ser executados inobstante de contratempos internos enfrentados pela **CONTRATADA**.

11.12. Não serão aceitos atrasos ou interrupções que gerem prejuízo aos prazos estipulados, exceto por motivo de força maior devidamente comprovado pela **CONTRATADA**, conforme prescrito na legislação vigente.

11.13. A **CONTRATADA** deve observar, durante a execução de suas atribuições contratuais, o cumprimento das diretrizes e critérios de sustentabilidade ambiental, de acordo com o previsto no Art. 225 da Carta Magna de 1988, em conformidade com o Art. 27 da Lei nº 13.303/2016, da definição contida no inciso LXXVIII do Art. 17 e do prelecionado no Art. 24 do Regulamento de Licitações e Contratos da **IMBEL** de 2018.

11.14. Demais obrigações constantes deste contrato e no edital.

11.15. Respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas federais, a exemplo do Decreto nº 7983, de 8 de abril de 2013.

11.16. Cumprir das regras supramencionadas pela Administração por parte dos contratos pode ensejar a fiscalização do Tribunal de Contas da União e, após o devido processo legal, gerar as seguintes consequências:

11.16.1. assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da Lei, nos termos do Art. 71, Inciso IX da Constituição; ou

11.16.2. condenação dos agentes públicos responsáveis e da empresa **CONTRATADA** ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

11.17. Solicitar atestado de capacidade técnica pelos serviços prestados e materiais entregues.

11.18. Receber o pagamento pelos materiais entregues e os serviços prestados.

CLÁUSULA DÉCIMA SEGUNDA - DAS OBRIGAÇÕES E DIREITOS DO CONTRATANTE

12.1. Exigir o cumprimento de todas as obrigações assumidas pela **CONTRATADA**, de acordo com as cláusulas previstas neste instrumento e nos termos de sua proposta.

12.2. Notificar a **CONTRATADA**, por escrito, da ocorrência de eventuais imperfeições no curso da entrega do material ora contratados, fixando prazo para a sua correção.

12.3. Prestar as informações e os esclarecimentos que venham a ser solicitados pela **CONTRATADA** com relação ao objeto aqui tratado;

12.4. Proporcionar todas as condições para a execução do objeto, estabelecidas neste instrumento, permitindo, inclusive, o acesso aos técnicos, prepostos e/ou representantes da **CONTRATADA** às dependências da **CONTRATANTE**.

12.5. Rejeitar os materiais em desacordo com as condições estabelecidas em até 5 (cinco) dias úteis, contados a partir da entrega pela **CONTRATADA**, mediante Termo Circunstanciado celebrado entre os gestores dos entes signatários.

12.6. A **CONTRATANTE** somente deve considerar aceitos definitivamente os materiais entregues após o saneamento das irregularidades mencionadas no item anterior, o que deverá ser atestado, mediante atesto em termo circunstanciado celebrado entre os gestores dos entes signatários.

12.7. Fornecer Termos de Capacidade Técnica sempre que requeridos, desde que cumpridas as obrigações previstas.

12.8. Pagar à **CONTRATADA** o valor resultante da prestação dos serviços e entrega do material, nos prazos e nas condições aqui pactuados.

12.9. Proceder as retenções tributárias sobre o valor na Nota Fiscal/Fatura emitida pela **CONTRATADA**, sempre que devido.

12.10. Cumprir as demais obrigações previstas neste instrumento.

CLÁUSULA DÉCIMA TERCEIRA - DAS SANÇÕES ADMINISTRATIVAS E PENALIDADES

13.1. Comete condutas reprováveis e passíveis de sancionamento, nos termos da Lei nº 13.303/16 e dos artigos 188 a 193 do Regulamento de Licitações e Contratos da **IMBEL**, de 22 de maio de 2018, a **CONTRATADA** que:

13.1.1. não atender, sem a devida e tempestiva justificativa, à convocação da **IMBEL** para assinatura da ata de registro de preços.

13.1.2. apresentar documento falso em qualquer em qualquer procedimento licitatório ou processo administrativo instaurado pela **IMBEL**.

13.1.3. frustrar ou fraudar, mediante ajuste, combinação ou qualquer outro expediente o processo de contratação, caracterizando má-fé na relação contratual.

13.1.4. incorrer em inexecução da ata de registro de preços.

13.1.5. comportar-se de modo inidôneo.

13.2. Pela inexecução total ou parcial do objeto, a **IMBEL** pode aplicar à **CONTRATADA** as seguintes sanções:

13.2.1. Advertência - quando do ato praticado não acarretar prejuízo à **IMBEL**, suas instalações, seus integrantes, imagem, meio ambiente ou a terceiros, devendo ocorrer o registro do ato no SICAF.

13.2.2. multa de 10% (dez por cento) sobre o valor total do contrato, no caso de recusa injustificada para assinatura do contrato, da Ata de Registro de Preços, e do recebimento da Nota de Empenho.

13.2.3. multa de 0,3% (zero vírgula três por cento) em caso de atraso injustificado para assinatura da ata de registro de preços, por dia de atraso até o limite de 30 dias, sobre o valor total da ata, e

13.2.4. multa de 0,3% (zero vírgula três por cento) em caso de situação irregular de habilitação, por dia de atraso até o limite de 30 dias, sobre o valor total da Nota de Empenho.

13.2.5. multa de 0,3% (zero vírgula três por cento) em caso de atraso na entrega do material/serviço, por dia de atraso até o limite de 30 dias, sobre o valor total da Nota de Empenho.

13.2.6. multa de 10% (dez por cento) sobre o valor da Nota de Empenho por atraso na entrega do material e/ou prestação do serviço no prazo estipulado.

13.2.7. A multa aplicada deverá ser recolhida ao Tesouro Nacional por meio de GRU (guia de recolhimento da união), no prazo máximo de 20 (vinte) dias úteis, a contar do dia útil imediato ao recebimento da notificação enviada pela **IMBEL** e o recibo entregue na Divisão de Finanças da **IMBEL**.

13.2.8. No caso da multa aplica não for paga pela **CONTRATADA**, a mesma será descontada da garantia contratual e, caso o valor da garantia não cubra o valor da multa aplicada, sua diferença será descontada da fatura que por ventura a **IMBEL** tenha que pagar a **CONTRATADA**.

13.2.9. No caso do valor da garantia contratual e da fatura ainda não paga não cubra o valor da multa aplicada, a sua diferença será cobrada judicialmente a **CONTRATADA**.

13.3. Suspensão do direito de licitar e impedimento de contratar com a **IMBEL**, por até 2 (dois) anos, registro no SICAF e no CEIS, de acordo com o preconizado no artigo 23 da Lei nº 12.846/13, em virtude do cometimento de fraude fiscal; pela prática de atos ilícitos no intento de prejudicar os objetivos almejados pela **IMBEL**, por intermédio da ARP; pela manifesta demonstração de inidoneidade para contratar com a **IMBEL** em virtude do cometimento de atos ilícitos; bem como por falhar ou fraudar na execução do objeto.

13.4. As penalidades de multas decorrentes de fatos diversos serão consideradas independentes entre si e poderão ser aplicadas à **CONTRATADA** juntamente com as sanções previstas nos subitens 13.2.1; 13.3.

13.5. A aplicação de qualquer das penalidades acima elencadas realizar-se-á por intermédio de procedimento administrativo que garantirá à **CONTRATADA** o pleno direito ao exercício pleno da ampla defesa e do contraditório no prazo de 5 (cinco) dias úteis, a contar da data em que for notificada pela **IMBEL**.

13.6. Após o processo administrativo pertinente, as importâncias decorrentes das multas aplicadas e não recolhidas nos prazos estipulados nas notificações correspondentes, devem ser descontadas dos pagamentos eventualmente devidos pela **IMBEL**, ou ainda, conforme cada caso, judicialmente cobradas.

13.7. A autoridade competente, quando da aplicação das sanções, deve considerar a natureza e a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano gerado à **IMBEL**, observados os princípios da razoabilidade e da proporcionalidade.

13.8. As penalidades devem, obrigatoriamente, ser registradas no SICAF, nas situações e momentos para as quais foram estabelecidas, podendo ser aplicadas isolada ou cumulativamente a critério da **IMBEL** após a análise das circunstâncias que ensejaram sua aplicação.

13.9. Aplicam-se à **CONTRATADA** as normas de direito penal preconizadas entre os artigos 89 e 99 da Lei nº 8.666/93, conforme o disposto no Art. 41 da Lei nº 13.303/16 e no Art. 2º do Regulamento de Licitações e Contratos da **IMBEL**.

13.10. Concluída a instrução processual, a **CONTRATADA** será intimada para, se assim desejar, apresentar, apresentar razões finais num prazo de até 5 (cinco) dias úteis.

CLÁUSULA DÉCIMA QUARTA - DO CONTROLE, DA FISCALIZAÇÃO E GERENCIAMENTO DO CONTRATO

14.1. O acompanhamento e a fiscalização e o gerenciamento da execução contratual, bem como quanto à qualidade do material e a execução do serviço relacionados no objeto, fica a cargo do Fiscal do Contrato a ser designado para essa finalidade e, na falta deste, por substituto designado pela área demandante, a quem caberá, também, dirimir as dúvidas que surgirem durante a execução dos serviços.

14.2. O Fiscal do Contrato deve ter a experiência necessária para acompanhamento e controle durante a execução dos serviços provenientes do contrato.

14.3. A verificação da adequada prestação do serviço deve ser realizada conforme critérios preestabelecidos no Termo de Referência.

14.4. Não se admite que a própria **CONTRATADA** materialize a avaliação de desempenho e qualidade dos serviços por ela prestados.

14.5. O descumprimento total ou parcial das demais obrigações e responsabilidades assumidas pela **CONTRATADA** ensejará na aplicação das sanções administrativas previstas no **CONTRATO**, na legislação vigente e nos artigos 188 a 193 do Regulamento de Licitações e Contratos da **IMBEL**, em consonância com disposto entre os artigos 83 e 84 da Lei nº 13.303/16.

CLÁUSULA DÉCIMA QUINTA - DO RECEBIMENTO E DA ACEITAÇÃO DO OBJETO

15.1. O serviço e o material serão recebidos pelo Fiscal do Contrato da **IMBEL** no ato da entrega da Nota Fiscal por parte da **CONTRATADA**, após cumprido todas as exigências, para posterior verificação de sua conformidade com as especificações contidas no TR.

15.2. Os materiais e o serviço poderão ser rejeitados, totalmente ou parcialmente, quando estiverem em desacordo com as especificações constantes do Termo de Referência ou do Contrato, devendo ser corrigidos, refeitos ou substituídos no prazo fixado pelo Fiscal do contrato à custa da **CONTRATADA**, sem prejuízo da aplicação das demais penalidades provenientes do descumprimento contratual.

15.3. Após o prazo concedido pelo Fiscal do Contrato, os materiais e o serviço será novamente inspecionado para fins de aceitação e, caso ainda perdure alguma alteração será instaurado o devido processo administrativo contra a **CONTRATADA**, sem que isso a desobrigue de efetuar as correções ainda pendentes.

CLÁUSULA DÉCIMA SEXTA - DA INEXECUÇÃO E RESCISÃO

16.1. A inexecução total ou parcial do contrato poderá ensejar na sua rescisão, com a repercussão das consequências cabíveis.

16.2. Constituem razões para a rescisão contratual:

16.2.1. o descumprimento de obrigações contratuais.

16.2.2. a subcontratação total ou parcial do objeto, cessão ou transferência, total ou parcial, a quem não atenda aos pré-requisitos habilitatórios e sem prévia e expressa autorização da **IMBEL**.

16.2.3. a fusão, cisão, incorporação ou associação da **CONTRATADA** com outrem, quando não admitidas no Termo de Referência e se prévia e expressa autorização da **IMBEL**.

16.2.4. o desatendimento das determinações legais e regulares expedidas pelo Gestor ou Fiscal do Contrato.

16.2.5. o reiterado cometimento de faltas durante a execução contratual.

16.2.6. a dissolução da sociedade ou falecimento do **CONTRATADO**.

16.2.7. a decretação de falência ou insolvência civil do **CONTRATADO**.

16.2.8. a alteração social ou modificação da finalidade ou da estrutura da **CONTRATADA**, cuja repercussão possa prejudicar a consecução contratual.

16.2.9. razões de interesse da **IMBEL**, de alta relevância e amplo conhecimento, expressamente justificadas no processo administrativo.

16.2.10. o atraso nos pagamentos devidos pela **IMBEL**, provenientes de serviços ou fornecimentos, como também de parcelas destes, já recebidos ou executados, salvo nos casos de

calamidade pública, grave perturbação da ordem interna ou guerra, restando assegurado à **CONTRATADA** o direito de optar pela suspensão do cumprimento de suas obrigações até que seja normalizada a situação.

16.2.11. a falta de liberação, por parte da **IMBEL**, de área, local ou dos objetos e condições necessárias para a execução dos serviços nos prazos contratualmente especificados, bem como das informações prescritas no Termo de Referência.

16.2.12. a ocorrência de caso fortuito, força maior ou fato do príncipe, regularmente comprovada, desde que esteja caracterizado o vínculo impeditivo da execução contratual.

16.2.13. a suspensão dos direitos da **CONTRATADA** de contratar e licitar com a **IMBEL**.

16.2.14. o descumprimento, por parte da **CONTRATADA**, da proibição de trabalho noturno, perigoso ou insalubre a menores de 18 (dezoito) anos e de qualquer trabalho de menores de 16 (dezesseis) anos, a não na condição de aprendiz a partir de 14 (quatorze) anos.

16.2.15. ter fraudado ou frustrado, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo da Licitação.

16.2.16. ter impedido, perturbado ou fraudado a realização de qualquer ato de procedimento licitatório público.

16.2.17. ter afastado ou procurado afastar licitante, por intermédio de fraude ou oferecimento de vantagem de qualquer natureza.

16.2.18. ter fraudado licitação pública ou contrato dela decorrente.

16.2.19. ter criado, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação pública ou celebrar contrato administrativo.

16.2.20. ter obtido vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogação de contratos celebrados pela Administração Pública, sem autorização em lei no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais.

16.2.21. ter manipulado ou fraudado o equilíbrio econômico-financeiro dos contratos celebrados com a Administração Pública, e

16.2.22. ter prejudicado atividade de investigação ou fiscalização de órgãos, entidades de controle ou agentes públicos, ou ter intervindo em sua atuação, inclusive no âmbito das agências reguladoras e de órgãos do sistema financeiro nacional.

16.2.23. as práticas passíveis de rescisão definidas entre os incisos 16.2.15 e 16.2.22, podem ser definidas, entre outras, como:

a) Corrupta - oferecer, dar, receber ou solicitar, direta ou indiretamente, qualquer vantagem com o objetivo de influenciar a ação do empregado da **IMBEL** no procedimento aquisitivo ou na execução contratual.

b) Fraudulenta - falsificar ou omitir fatos, com o objetivo de influenciar o procedimento licitatório ou a execução contratual.

c) Colusiva - esquematizar ou estabelecer um acordo entre dois ou mais licitantes, com ou sem conhecimento de representantes da **IMBEL**, visando o estabelecimento de preços em níveis artificiais e não competitivos.

d) Coercitiva - causar danos ou ameaçar, direta ou indiretamente, pessoas físicas ou jurídicas, visando influenciar sua participação em procedimento licitatório ou afetar a execução contratual, e.

e) Obstrutiva - destruir, falsificar, alterar ou ocultar provas ou fazer declarações falsas, com o objetivo de impedir materialmente a apuração a apuração de práticas ilícitas.

16.2.24. As práticas retro mencionadas, além de acarretarem a responsabilização administrativa e judicial da pessoa jurídica, implicarão da responsabilização individual dos dirigentes das empresas contratadas e dos administradores ou gestores, enquanto autores, nos termos da Lei nº 12.846/13.

16.3. A rescisão do contrato pode ser:

16.3.1. amigável, em comum acordo entre as partes, ou

16.3.2. por determinação judicial.

16.4. A rescisão amigável não é cabível nos casos em que forem constados descumprimentos contratuais sem apuração de responsabilidade iniciada ou com procedimento apuratório ainda em curso.

16.5. Quando a rescisão ocorrer sem que haja culpa ou responsabilidade da parte **CONTRATANTE**, este será ressarcido dos prejuízos que eventualmente tiver sofrido, quando devida e regularmente comprovados, e no caso da **CONTRATADA** terá esta, ainda, o direito a:

16.5.1. pagamentos devidos pela execução contratual até a data da rescisão, e

16.5.2. pagamento referente ao custo de desmobilização.

16.6. Os casos de rescisão contratual devem ser formalmente motivados nos autos processuais, devendo ser assegurado o direito ao exercido prévio do contraditório e da ampla defesa.

16.7. A rescisão deverá ser formalizada por intermédio de Termo de Rescisão Contratual, devendo o respectivo extrato ser publicado no Diário Oficial da União.

CLÁUSULA DÉCIMA SÉTIMA - DA ALTERAÇÃO DO CONTRATO

17.1. O contrato poderá ser alterado por acordo entre as partes, nos seguintes casos:

17.1.1. quando houver modificação do projeto ou das especificações, para melhor adequação técnica aos seus objetivos;

17.1.2. quando necessária a modificação do valor contratual em decorrência de acréscimo ou diminuição quantitativa de seu objeto, nos limites permitidos na Lei nº 13.303/16;

17.1.3. quando conveniente a substituição da garantia de execução; quando necessária a modificação do regime de execução do serviço, bem como do modo de fornecimento, em face de verificação técnica da inaplicabilidade dos termos contratuais originários;

17.1.4. quando necessária a modificação da forma de pagamento, por imposição de circunstâncias supervenientes, mantido o valor inicial atualizado, vedada a antecipação do pagamento, com relação ao cronograma financeiro fixado, sem a correspondente contraprestação de fornecimento de bens ou execução de obra ou serviço; e

17.1.5. para restabelecer a relação que as partes pactuaram inicialmente entre os encargos do contratado e a retribuição da administração para a justa remuneração do serviço, objetivando a manutenção do equilíbrio econômico-financeiro inicial do contrato, na hipótese de sobrevirem fatos imprevisíveis, ou previsíveis porém de consequências incalculáveis, retardadores ou impeditivos da execução do ajustado, ou, ainda, em caso de força maior, caso fortuito ou fato do príncipe, configurando álea econômica extraordinária e extracontratual.

CLÁUSULA DÉCIMA OITAVA - DOS ACRÉSCIMOS E SUPRESSÕES

18.1. O contratado poderá aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem, até 25% (vinte e cinco por cento) do valor inicial do contrato

18.2. Nenhum acréscimo ou supressão poderá exceder os limites estabelecidos no item 18.1 acima, salvo as supressões resultantes de acordo celebrado entre as partes.

CLÁUSULA DÉCIMA NONA - DO REAJUSTAMENTO

19.1. A avença que poderá ser firmada, sofrerá reajuste de preços, obedecendo as seguintes regras:

19.1.1. O primeiro reajustamento poderá ocorrer após decorridos 12 (doze) meses, contados a partir da data efetiva da proposta de preços;

19.1.2. Os reajustes subsequentes ocorrerão decorridos 12 (doze) meses, a contar da data do primeiro reajustamento;

19.1.3. Será admitido pela **IMBEL** o reajustamento com base no Índice de Custos de Tecnologia da Informação (ICTI), de acordo com a Portaria nº 6.432/MPDG/STIC, de 11 de julho de 2018 sobre o valor praticado no contrato;

19.1.4. Caso ocorra a extinção do índice previsto no subitem anterior, o novo índice a ser aplicado será o Índice de Preços ao Consumidor Amplo - IPCA; e

19.1.5. O valor contratual poderá ser reajustado para mais ou para menos, de acordo com a variação do índice indicado no item 19.1.3. acima, com base na fórmula abaixo, vedada a periodicidade de reajuste inferior a um ano (12 meses), contados da data limite para apresentação

da proposta (redação dada pelo Decreto nº 1.110, de 13/04/1994) - Decreto nº 1054, de 07/02/1994.

$R = V\left[\frac{I-Io}{Io}\right]$, onde,

R = valor do reajuste procurado.

V = valor contratual do fornecimento, obra ou serviço a ser reajustado.

Io = índice inicial - refere-se ao índice de custos ou de preços correspondente à data fixada para entrega da proposta da licitação.

I = índice relativo à data do reajuste.

CLÁUSULA VIGÉSIMA – DA SUBCONTRATAÇÃO

Não será admitida em nenhuma espécie a subcontração do objeto deste contrato.

CLÁUSULA VIGÉSIMA PRIMEIRA – DA ALTERAÇÃO SUBJETIVA

É admissível a fusão, cisão ou incorporação da **CONTRATADA** com/em outra pessoa jurídica, desde que sejam observados todos os requisitos de habilitação e qualificação ora exigidos, e sejam mantidas as condições deste contrato.

CLÁUSULA VIGÉSIMA SEGUNDA – DA VINCULAÇÃO

Consideram-se integrantes do presente instrumento contratual as condições prescritas no Termo de Referência, na Proposta de preços da **CONTRATADA**, de 26 de maio de 2022 e demais documentos pertinentes, independentes de sua transcrição.

CLÁUSULA VIGÉSIMA TERCEIRA- DA SUSTENTABILIDADE AMBIENTAL

23.1. A **CONTRATADA** deverá adotar as seguintes práticas de sustentabilidade ambiental.

23.2. Fornecer aos seus empregados os equipamentos de segurança que se fizerem necessários, para a execução do serviço, quando couber.

23.3. Respeitar as Normas Brasileiras - NBR publicadas pela Associação Brasileira de Normas Técnicas sobre resíduos sólidos.

23.4. A **CONTRATADA** deverá observar, durante a execução de suas atribuições contratuais, o cumprimento das diretrizes e critérios de sustentabilidade ambiental, de acordo com o previsto no Art. nº 225 da Constituição Federal de 1988.

CLÁUSULA VIGÉSIMA QUARTA - DA GARANTIA CONTRATUAL

24.1. De acordo com o Art. 70, da Lei 13.303, de 30 de junho de 2016, será exigido da **CONTRATADA** para o fiel cumprimento da avença firmada, a garantia contratual.

24.2. Caberá ao contratado optar por uma das seguintes modalidades de garantia:

I - Caução em dinheiro feita na Caixa Econômica Federal (CEF);

II - Seguro-garantia; e

III - Fiança bancária.

24.3. A garantia a que se refere o item 24.1 será de a 5% (cinco por cento) do valor global deste contrato e terá sua validade com 90 (noventa) dias após o término deste contrato, para cobrir qualquer prejuízo verificado que a **CONTRATADA** tenha causado a **CONTRATANTE**, durante a vigência desta avença.

24.4. A garantia prestada pela **CONTRATADA** será liberada ou restituída após decorridos noventa dias após o término deste contrato.

24.5. Caso a **CONTRATADA** opte por apresentar a garantia contratual na modalidade de caução em dinheiro, deverá ser feita na Caixa Econômica Federal - CEF, em conta remunerada.

24.6. A **CONTRATADA** deverá apresentar, em até 10 (dez) dias úteis após a assinatura deste contrato, no valor de R$ 16.767,50 (dezesseis mil, setecentos e sessenta e sete reais e cinquenta centavos) para assegurar o integral cumprimento de todas as obrigações previstas neste instrumento, inclusive pagamento de multas eventualmente aplicadas, com validade de 03 (três) meses após o término da vigência contratual.

24.7. Caso a garantia contratual vier a ser executada, em parte ou em sua totalidade, a **CONTRATADA** deverá repor o valor, total ou parcial, dentro do prazo de 15 (quinze) dias úteis, após notificada pela **CONTRATANTE**.

CLÁUSULA VIGÉSIMA QUINTA- DA MANUTENÇÃO DE QUALIFICAÇÃO E HABILITAÇÃO

A **CONTATADA** se obriga a manter durante todo o período de execução do objeto deste contrato, relativamente às obrigações por intermédio deste assumidas, as condições de habilitação e qualificação exigidas.

CLÁUSULA VIGÉSIMA SEXTA - DOS RECURSOS

26.1. Do ato de rescisão deste contrato e da respectiva aplicação das penalidades de advertência, suspensão temporária e multa, cabe recurso no prazo de 5 (cinco) dias úteis a contar do recebimento da intimação do ato, que deve ser dirigido à autoridade superior àquela que praticou o ato recorrido.

26.2. A intimação do ato de suspensão temporária deve ser efetuado por intermédio de publicação no Diário Oficial da União, e as de advertência ou multa registradas no SICAF e, concomitantemente, comunicadas por escrito à **CONTRATADA**.

CLÁUSULA VIGÉSIMA SÉTIMA - DA MATRIZ DE RISCO

27.1. A seguir, é apresentado as tabelas, que definem a probabilidade e o impacto que serão aplicados aos possíveis riscos.

Probabilidade	
Situação	**Pontuação**
Improvável	0
Pouco provável	1
Possível	2
Muito possível	3

Impacto	
Situação	**Pontuação**
Sem impacto	0
Baixo impacto	1
Médio impacto	2
Alto impacto	3

27.2. Listagem de possíveis eventos supervenientes à assinatura desta avença que possam interferir no equilíbrio econômico-financeiro deste contrato.

EVENTO	**PROBABILIDADE**		**IMPACTO**	
	Situação	**Pontuação**	**Situação**	**Pontuação**
Estratégia inadequada de implantação do FIREWALL	Pouco provável	1	Médio impacto	2
Não integração do Firewall da SEDE com os Firewalls das Fábricas	Pouco provável	1	Alto impacto	3
Funcionários envolvidos com a instalação e configuração do hardware e sistema não estarem preparados para a sua alta complexidade.	Médio Impacto	2	Médio impacto	2
Configuração inadequada da Solução de Firewall.	Médio Impacto	2	Alto impacto	3

27.3. Caso ocorra o previsto no item 27.2 acima, todas as despesas do aditamento ocorrerão por conta da **CONTRATADA**.

27.4. Apenas a execução do serviço previsto no objeto, haverá liberdade da **CONTRATADA** para inovação metodológica ou tecnológica, nas obrigações de resultado ou na melhoria no padrão das soluções previamente estabelecidas no Termo de Referência.

CLÁUSULA VIGÉSIMA OITAVA – DO FORO

28.1. As partes elegem o foro da Justiça Federal na cidade de Brasília-DF para conhecer e julgar disputas judiciais que possam resultar da execução do presente contrato.

28.2. E, por estarem justas e contratadas, as Partes assinam o presente contrato, por intermédio de seus representantes legais, em 02 (duas) vias de igual forma e teor, para um só efeito que, depois de lido e achado conforme, produza seus efeitos jurídicos e legais.

Brasília-DF, 23 de junho de 2022.

Pela CONTRATANTE:

E.X.C.
Ordenador de Despesas
CPF ***.178.581-**
RG **568** SSP/DF

_____
Rubrica

Pela CONTRATADA:

W.L.DE.M.M.
Diretor de Soluções
CPF ***.944.761-**
RG **694**-DGPC/GO

_____
Rubrica

Testemunhas:

Nome:
CPF

_____
Rubrica

Nome:
CPF

_____
Rubrica

(CPF e RG protegidos pela lei n° 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais – LGPD, Redação dada pela Lei n° 13.853, de 2019.)