EDITAL DE COLETA DE PREÇO

Edital nº 009/2026 - Instituto Gnosis

O Instituto Gnosis, inscrito no CNPJ sob o no 10.635.117/0001-03, em atenção ao **art. 7º do Regulamento de Compras e Contratação de Serviços**, torna público o presente processo de seleção de empresa especializada para prestação de serviços de sustentação do ambiente de segurança da informação, incluindo o fornecimento, implantação, configuração e gerenciamento de firewalls de próxima geração (Next-Generation Firewalls – NGFW), com prestação de serviços gerenciados de segurança (Managed Security Services – MSS) através de um Centro de Operações 24x7x365, suporte técnico, resposta a incidentes nos firewalls, emissão de relatórios e dashboards executivos, visando assegurar a confidencialidade, integridade e disponibilidade das informações. Incluem-se no objeto o fornecimento de acesso à internet através de links dedicados, full duplex, com abordagem via fibra óptica com conexão em alta velocidade à internet, permanente e estável, sem variações, por meio de IP fixo, alta performance e 100% de garantia de banda, não possuindo limites de Download e Upload, conectividade e segurança LAN-2-LAN / MPLS, para atender as necessidades do SCCDTI – Super Centro Carioca de Diagnóstico e Tratamento por Imagem, localizado na Rua Dr. Rodrigues de Santana nº 53, Bairro de Benfica e suas unidades Avançadas, administrados pelo Instituto Gnosis, através de Termo de Colaboração celebrado com a prefeitura do Rio de Janeiro, conforme as disposições técnicas contidas no Termo de Referência.

O presente Instrumento Convocatório rege-se pelo **Regulamento de Compras e Contratação de Serviços** do Instituto Gnosis, que se encontra disponível no sítio eletrônico da **Instituição**.

A contratação será efetuada pelo proponente que apresentar o **MENOR PREÇO GLOBAL**, obedecendo aos critérios do Edital e seus anexos.

1. OBJETO

1.1. Constitui objeto do presente Edital a contratação de empresa especializada para prestação de serviços de sustentação do ambiente de segurança da informação, incluindo o fornecimento, implantação, configuração e gerenciamento de firewalls de próxima geração (Next-Generation Firewalls – NGFW), com prestação de serviços gerenciados de segurança (Managed Security Services – MSS) através de um Centro de Operações 24x7x365, suporte técnico, resposta a incidentes nos firewalls, emissão de relatórios e dashboards executivos, visando assegurar a confidencialidade, integridade e disponibilidade das informações. Incluem-se no objeto o fornecimento de acesso à internet através de links dedicados, full duplex, com abordagem via fibra óptica com conexão em alta velocidade à internet, permanente e estável, sem variações, por meio de IP fixo, alta performance e 100% de garantia de banda, não possuindo limites de Download e Upload, conectividade e segurança LAN-2-LAN / MPLS, para atender as necessidades do SCCDTI – Super Centro Carioca de Diagnóstico e Tratamento por Imagem, localizado na Rua Dr. Rodrigues de Santana nº 53, Bairro de Benfica e suas unidades Avançadas, administrados pelo Instituto Gnosis, através de Termo de Colaboração celebrado com a prefeitura do Rio de Janeiro, conforme disposições técnicas contidas no Termo de Referência.

2. CONDIÇÕES PARA PARTICIPAÇÃO

2.1. Somente poderão participar desta seleção, as empresas:

2.1.1. Estabelecidas no País, que satisfaçam as condições e disposições contidas neste Edital;

2.1.2. Que explorem ramo de atividade compatível com o objeto cotado.

2.2. Não se admitirá nesta seleção a participação de empresas:

2.2.1. Que estejam sob regime de recuperação judicial ou falência;

2.2.2. Estrangeiras, que não funcionem no País;

2.2.3. Que tenham em seu quadro societário, cônjuges ou parentes de Diretores ou Conselheiros do Instituto Gnosis.

2.2.4. É vedada a qualquer pessoa física ou jurídica a representação de mais de uma empresa na presente seleção.

3. DO PROCEDIMENTO

3.1. O processo de seleção de empresas será realizado em duas fases, sendo que a primeira consiste na verificação do preço apresentado pelos Proponentes e a segunda na verificação da documentação necessária.

3.2. As **Propostas de Preço** deverão ser entregues por meio eletrônico, direcionado a: propostas@institutognosis.org.br.

3.2.1. Os e-mails deverão exibir como "assunto" da mensagem o número do presente Edital e a identificação do proponente no corpo da mensagem.

3.3. As propostas de preço deverão ser entregues **até o dia 27 de março de 2026 às 17:00 horas**.

3.4. As propostas enviadas fora do prazo não serão consideradas.

4. PROPOSTA DE PREÇOS

4.1 Todos os encargos e impostos gerados deverão estar informados detalhadamente dentro do preço final apresentado.

4.2 A proposta apresentada deverá conter identificação da pessoa jurídica responsável pela mesma (razão social, endereço, CNPJ, telefone, e-mail).

4.3 O prazo de validade da proposta não poderá ser inferior a 30 (trinta) dias corridos, a contar da data de sua apresentação.

4.4 A participação no presente processo, assim como o envio da proposta de preços, implica na aceitação plena das condições estipuladas neste Termo e seus anexos.

4.5 O preço proposto será de exclusiva responsabilidade do **PROPONENTE**, não lhe sendo dado o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro argumento não previsto em lei.

4.6 O preço deverá ser expresso em moeda nacional com, no máximo, duas casas decimais após a vírgula. Na elaboração da proposta devem ser computados todos os impostos, encargos fiscais e comerciais, taxas, fretes, seguros, deslocamentos de pessoal e quaisquer outros custos ou despesas

que incidam ou venham a incidir direta ou indiretamente sobre o objeto da proposta, visando seu pleno atendimento.

4.7 Se alguma proposta de preços enviada contrariar qualquer dispositivo deste Edital a mesma será desclassificada.

4.8 Propostas manifestamente inexequíveis serão sumariamente desclassificadas, com base nos estudos referenciais preliminares que antecederam o presente procedimento.

4.9 É facultado ao Gnosis, após o recebimento das propostas, tentar negociar possíveis reduções com os proponentes para a busca do menor preço.

5. DOCUMENTOS DE HABILITAÇÃO

5.1. A **PROPONENTE** vencedora deverá apresentar a seguinte documentação para fins de habilitação:

5.1.1. Habilitação Jurídica:

5.1.1.1. Empresa individual: Registro Comecial, devidamente inscrito na Junta Comecial;

5.1.1.2. Sociedades Comerciais por ações: Ato constitutivo, estatuto ou contrato social, ou última consolidação e alterações posteriores, devidamente registradas, acompanhados de documentos de eleição dos atuais administradores;

5.1.1.3. Sociedades civis: Inscrição do ato constitutivo, acompanhada de prova de diretoria em exercício;

5.1.1.4. Empresas ou sociedades estrangeiras: Decreto de autorização para que se estabeleçam no País e ato de registro de autorização para funcionamento expedido pelo órgão competente.

Observação: O Objeto social deverá ser compatível com o objeto do contrato.

5.1.2 Regularidade Fiscal e Trabalhista:

5.1.2.1 Prova de inscrição no Cadastro Nacional de Pessoa Jurídica (CNPJ);

5.1.2.2. Prova de regularidade fiscal com a Fazenda Federal (SRF – Secretaria da Receita Federal e PGFN – Procuradoria Geral da Fazenda Nacional);

5.1.2.3. Prova de regularidade com a Fazenda Estadual;

5.1.2.4. Prova de regularidade com a Fazenda Municipal;

5.1.2.5. Certificado de Regularidade Fiscal para com o Fundo de Garantia por Tempo de Serviço (FGTS) – CRF;

5.1.2.6. Certidão Negativa de Débitos Trabalhistas;

5.1.3. Qualificação Técnica:

5.1.3.1 Comprovação de que possui instalações e aparelhamentos adequados e disponíveis para a realização dos serviços que são objeto do presente Edital e Termo de Referência.

5.1.3.2 Mínimo de 01 (um) Atestado (s) de Capacidade Técnica, expedido por pessoa (s) jurídica (s) de direito público ou privado, que comprove(m) a aptidão no fornecimento de objeto similar ao descrito neste Termo de Referência, com o seguinte termo de maior relevância:

5.1.3.2.1. Fornecimento de Next Generation Firewalls, com licenciamento, implantação completa e passagem de conhecimento;

5.1.3.2.2. Prestação de serviços de sustentação do ambiente de Segurança da Informação, através de Centro de Operações de Segurança, no formato 24x7x365;

5.1.3.3. A empresa deverá comprovar, possuir certificação nas Normas ISO 27001 e 27701, por serem referências globalmente reconhecidas, que especificam requisitos para estabelecer, implementar, manter e aprimorar de forma contínua um Sistema de Gestão da Segurança da Informação (SGSI) e um Sistema de Gestão de Privacidade da Informação (SGPI), respectivamente;

5.1.3.4. A empresa deverá apresentar certificação na Norma ISO 9001, que estabelece requisitos para o Sistema de Gestão da Qualidade (SGQ) e ISO 45001, que estabelece políticas e objetivos para Saúde e Segurança do Trabalho;

5.1.3.5. Para comprovação técnico profissional a empresa deverá apresentar Registro em Carteira de Trabalho e Previdência Social ou Contrato Registrado de pelo menos 1 (um) profissional capacitado com certificação de Engenheiro, pelo fabricante do Next Generation Firewall;

5.1.3.6. A empresa deverá apresentar Registro em Carteira de Trabalho e Previdência Social ou Contrato Registrado de pelo menos 1 (um) profissional capacitado, com a certificação CISSP e ITIL V4;

5.1.3.6.1. O profissional certificado oficialmente pela fabricante da solução, ficará responsável, por parte da empresa vencedora, pela elaboração das etapas de execução dos serviços, conforme cronograma de execução, contemplando acompanhamento e suporte técnico remoto e onsite à equipe técnica da CONTRANTE durante toda a vigência do contrato;

5.1.3.6.2. O Profissional detentor da certificação CISSP, é extremamente importante na Integração da Rede com a Segurança da Informação, em ambiente que define a arquitetura, design, gestão e/ou controles que garantem a segurança de ambientes corporativos, projetando filtros de segurança para evitar invasões e vazamento de informações confidenciais da rede, aplicações e banco de dados. Tal profissional analisa toda a integração da implantação do Backbone em integração com toda a Segurança do Ambiente. A credencial demonstra um nível reconhecido globalmente de competência fornecido pelo CBK® do (ISC)2®. O profissional CISSP tem total habilidade com tópicos críticos em segurança atual, incluindo computação em nuvem, segurança móvel, gerenciamento integrado, segurança no desenvolvimento de aplicativos, segurança em ambientes de rede LAN, MAN e WAN, gestão de riscos, gestão de incidentes, hardening (boas práticas para segurança de ambientes de rede corporativo) e outros, garantindo assim a parte segura do ambiente em produção.

5.1.3.7. A empresa vencedora deverá apresentar carta direcionada ao processo, a fim de comprovar ser parceira oficial do fabricante;

5.1.3.7.1. Caso não seja possível a emissão da carta, a empresa vencedora deverá comprovar ser parceira oficial através do site do fabricante.

5.1.3.7.2. Este item é imprescindível para garantir o perfeito atendimento ao fornecimento da solução, assim como a prestação dos serviços de forma qualificada.

5.1.3.8. Somente serão consideradas as propostas das proponentes cujas atividades estejam contidas no Alvará de Licença e no documento de licenciamento sanitário.

5.1.3.9. Plano de Segurança do Trabalho dos empregados, equipamentos e instalações, relativo às atividades a serem desenvolvidas.

5.1.3.10. Declaração formal assinada pelo representante legal da empresa, sob as penalidades da lei, de que tem pleno conhecimento das condições e peculiaridades inerentes à natureza dos trabalhos, assumindo total responsabilidade por esse fato e informando que não o utilizaria para quaisquer questionamentos futuros que ensejassem avenças técnicas ou financeiras.

5.1.3.11. Demais documentos técnicos exigidos no Termo de Referência.

6. VENCEDOR

6.1. Constatado o atendimento pleno das exigências deste Edital e seus anexos, será declarado vencedor o **PROPONENTE** que apresentar o **menor custo** para a execução dos serviços descritos no objeto deste Edital e seus anexos.

6.2. A realização do presente Edital não obriga o Instituto Gnosis a formalizar a contratação da empresa vencedora, podendo o procedimento de seleção ser cancelado, não cabendo indenização de qualquer natureza aos participantes.

7. CONTRATAÇÃO

7.1. Declarado o vencedor, seu representante legal será convocado para firmar o contrato objeto deste procedimento.

7.2. Caso o adjudicatário no ato da assinatura do contrato recuse-se a assiná-lo, serão convocados os proponentes remanescentes, observada a ordem de classificação.

7.3. Na hipótese de convocação dos proponentes remanescentes, estes deverão manter sua última proposta registrada.

7.4. O representante legal do proponente que tiver apresentado a proposta vencedora deverá assinar o contrato, dentro do prazo máximo de 3 (três) dias corridos a contar do recebimento da comunicação.

7.5. Qualquer solicitação de prorrogação de prazo para assinatura do contrato, decorrentes deste procedimento, somente será analisada se apresentada antes do decurso do prazo para tal e devidamente fundamentada.

8. DISPOSIÇÕES GERAIS

8.1. Os interessados poderão obter mais informações sobre as especificações técnicas do objeto deste Edital através do e-mail: propostas@institutognosis.org.br.

8.2. Os participantes do presente Edital assumem todos os custos de preparação e apresentação de suas respectivas propostas.

8.3. Os participantes são responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase do processo.

Rio de Janeiro, 18 de março de 2026.

Instituto Gnosis

TERMO DE REFERÊNCIA

Serviço de sustentação do ambiente de segurança da informação, incluindo o fornecimento, implantação, configuração e gerenciamento de firewalls de próxima geração (Next-Generation Firewalls – NGFW) e conectividade de rede – CDDTI e UA

1. JUSTIFICATIVA

Justifica-se a presente contratação por força do Termo de Colaboração nº 009/2022, celebrado entre a Prefeitura do Rio de janeiro e o Instituto Gnosis, para o gerenciamento, operacionalização e execução das ações e serviços de saúde do CCDTI – Centro Carioca de Diagnóstico e Tratamento por Imagem e suas Unidades Avançadas. Para a execução de um dos serviços inerentes no objeto contratualizado no Termo de Colaboração, se faz necessário a contratação de empresa especializada para serviços de sustentação do ambiente de segurança da informação, incluindo o fornecimento, implantação, configuração e gerenciamento de firewalls de próxima geração (Next-Generation Firewalls – NGFW), com prestação de serviços gerenciados de segurança (Managed Security Services – MSS) através de um Centro de Operações 24x7x365, suporte técnico, resposta a incidentes nos firewalls, emissão de relatórios e dashboards executivos, visando assegurar a confidencialidade, integridade e disponibilidade das informações. Assim como, fornecimento de acesso à internet através de links dedicados, full duplex, com abordagem via fibra óptica com conexão em alta velocidade à internet, permanente e estável, sem variações, por meio de IP fixo, alta performance e 100% de garantia de banda, não possuindo limites de Download e Upload, conectividade e segurança LAN-2-LAN / MPLS, para atender as necessidades do SCCDTI – Super Centro Carioca de Diagnóstico e Tratamento por Imagem, localizado na Rua Dr. Rodrigues de Santana nº 53, Bairro de Benfica e suas unidades Avançadas, administrados pelo Instituto Gnosis, através de Termo de Colaboração com a Prefeitura do Rio de Janeiro, de acordo com as condições e especificações constantes neste documento.

2. OBJETIVO

Contratação de empresa especializada para serviços de sustentação do ambiente de segurança da informação, incluindo o fornecimento, implantação, configuração e gerenciamento de firewalls de próxima geração (Next-Generation Firewalls – NGFW), com prestação de serviços gerenciados de segurança (Managed Security Services – MSS) através de um Centro de Operações 24x7x365, suporte técnico, resposta a incidentes nos firewalls, emissão de relatórios e dashboards executivos, visando assegurar a confidencialidade, integridade e disponibilidade das informações. Assim como, fornecimento de acesso à internet através de links dedicados, full duplex, com abordagem via fibra óptica com conexão em alta velocidade à internet, permanente e estável, sem variações, por meio de IP fixo, alta performance e 100% de garantia de banda, não possuindo limites de Download e Upload, conectividade e segurança LAN-2-LAN / MPLS, para atender as necessidades do CCDTI – Centro Carioca de Diagnóstico e Tratamento por Imagem localizado na Rua Dr. Rodrigues de Santana nº 53, Bairro de Benfica e suas Unidades Avançadas, administradas pelo Instituto Gnosis, através de Termo de Colaboração com a

Prefeitura do Rio de Janeiro, de acordo com as condições e especificações constantes neste documento.

3. ESPECIFICAÇÃO DOS SERVIÇOS

1. LINK DEDICADO 1Gbps com dupla abordagem (redundante) com Conectividade e Segurança 100Mbps LAN-2-LAN / MPLS – CCDTI - R. Dr. Rodrigues de Santana, 53 - Benfica, Rio de Janeiro - RJ, 20910-240.

2. Link Dedicado 300Mbps com KMZ e Backbone Distintos – CCDTI - R. Dr. Rodrigues de Santana, 53 - Benfica, Rio de Janeiro - RJ, 20910-240.

3. Link Dedicado 100Mbps com Conectividade e Segurança 100Mbps LAN-2-LAN / MPLS – HM Souza Aguiar - Praça da República, 111 - Centro, Rio de Janeiro - RJ, 20211-350.

4. Link Dedicado 100Mbps com Conectividade e Segurança 100Mbps LAN-2-LAN / MPLS – HM Lourenço Jorge - Av. Ayrton Senna, 2.000 - Barra da Tijuca, Rio de Janeiro - RJ, 22793-000.

5. Link Dedicado 100Mbps com Conectividade e Segurança 100Mbps LAN-2-LAN / MPLS – HM Miguel Couto - Rua Mario Ribeiro, 117 - Gávea, Rio de Janeiro - RJ, 22430-160.

6. Link Dedicado 100Mbps com Conectividade e Segurança 100Mbps LAN-2-LAN / MPLS –HM Salgado Filho - R. Arquias Cordeiro, 370 - Méier, Rio de Janeiro - RJ, 20770-000.

7. Link Dedicado 100Mbps com Conectividade e Segurança 100Mbps LAN-2-LAN / MPLS – HM Francisco Telles - Av. Ubirajara, 25 - Irajá, Rio de Janeiro - RJ, 21230-300.

8. Link Dedicado 100Mbp com Conectividade e Segurança 100Mbps LAN-2-LAN / MPLS s – HM Ronaldo Gazolla - Av. Pastor Martin Luther King Jr., 10.976 - Acari, Rio de Janeiro - RJ, 21531-010.

9. Link Dedicado 100Mbps com Conectividade e Segurança 100Mbps LAN-2-LAN / MPLS – HM Jesus - R. Oito de Dezembro, 717 - Vila Isabel, Rio de Janeiro - RJ, 20551-050.

10.Link Dedicado 100Mbps com Conectividade e Segurança 100Mbps LAN-2-LAN / MPLS – HM Piedade - R. da Capela, 96 - Piedade, Rio de Janeiro - RJ, 20740-310.

11.Link Dedicado 100Mbps com Conectividade e Segurança 100Mbps LAN-2-LAN / MPLS – UPA Madureira - Praça dos Lavradores, s/n - Campinho, Rio de Janeiro - RJ, 21310-200.

12.Link Dedicado 100Mbps com Conectividade e Segurança 100Mbps LAN-2-LAN / MPLS – UPA Cidade de Deus - Rua Edgard Werneck, s/n - Freguesia (Jacarepaguá), Rio de Janeiro - RJ, 22763-011.

13.Link Dedicado 100Mbps com Conectividade e Segurança 100Mbps LAN-2-LAN / MPLS – Policlínica Rodolpho Rocco - Estrada Adhemar Bebiano, 339 - Del Castilho, Rio de Janeiro - RJ, 21050-454.

14.Link Dedicado 100Mbps com Conectividade e Segurança 100Mbps LAN-2-LAN / MPLS – Policlínica Manoel Guilherme - Av. Ribeiro Dantas, 571 - Bangu, Rio de Janeiro - RJ, 21870-170.

15.Link Dedicado 100Mbps com Conectividade e Segurança 100Mbps LAN-2-LAN / MPLS – Policlínica Lincoln de Freitas - R. Álvaro Alberto, 601 - Santa Cruz, Rio de Janeiro - RJ, 23550-000.

16.Link Dedicado 100Mbps com Conectividade e Segurança 100Mbps LAN-2-LAN / MPLS – SMS Harvey Ribeiro - Av. Guiomar Novaes, 133 - Recreio dos Bandeirantes, Rio de Janeiro - RJ, 22790-590.

17.Link Dedicado 100Mbps com Conectividade e Segurança 100Mbps LAN-2-LAN / MPLS – SMS Belizário Pena - R. Franklin, 29 - Campo Grande, Rio de Janeiro - RJ, 23080-360.

18.Link Dedicado 100Mbps com Conectividade e Segurança 100Mbps LAN-2-LAN / MPLS – CF Otto Alves de Carvalho - Av. Eng. Souza Filho, 200 - Jacarepaguá, Rio de Janeiro - RJ, 22753-039.

19.Link Dedicado 100Mbps com Conectividade e Segurança 100Mbps LAN-2-LAN / MPLS – CF Adib Jatene - Via B Um, 589-501 - Maré, Rio de Janeiro - RJ, 21046-030.

20.Link Dedicado 100Mbps com Conectividade e Segurança 100Mbps LAN-2-LAN / MPLS – Centro de Imagem Rocinha - Rocinha, Rio de Janeiro - RJ, 22451-264.

21.Link Dedicado 100Mbps com Conectividade e Segurança 100Mbps LAN-2-LAN / MPLS – H Cardoso Fontes - Av. Menezes Cortes, 3245 - Jacarepaguá, Rio de Janeiro – RJ.

22.Link Dedicado 100Mbps com Conectividade e Segurança 100Mbps LAN-2-LAN / MPLS –H Andaraí - R. Leopoldo, 280 - Andaraí, Rio de Janeiro - RJ, 20541-170.

23.Link Dedicado 100Mbps com Conectividade e Segurança 100Mbps LAN-2-LAN / MPLS – HM Albert Schweitzer - R. Nilópolis, 239 - Realengo, Rio de Janeiro - RJ, 21720-040.

24.Link Dedicado 100Mbps com Conectividade e Segurança 100Mbps LAN-2-LAN / MPLS – HM Evandro Freire - Estrada do Galeão, 2.920 - Portuguesa, Rio de Janeiro - RJ, 21931-582.

25.Link Dedicado 100Mbps com Conectividade e Segurança 100Mbps LAN-2-LAN / MPLS – HM Pedro II - R. do Prado, 325 - Santa Cruz, Rio de Janeiro - RJ, 23555-012.

Link ADSL de velocidade igual ou superior ao principal – LINK BACKUP – TODAS AS UNIDADES.

4. EXECUÇÃO DO SERVIÇO

4.1 Os serviços deverão ser prestados dentro dos parâmetros e rotinas estabelecidos, com fornecimento de mão-de-obra e equipamentos, e ainda a observância às recomendações aceitas pela boa técnica, normas e legislação aplicável.

4.2 Oferecer soluções Corporativas de Internet, que permitem ter acesso permanente e exclusivo à Internet com alta velocidade, garantia de banda contratada, sem a necessidade de

um provedor.

4.3 Instalação, configuração, detecção e correção de problemas.

4.4 Circuitos de comunicação necessários.

4.5 Tecnologia preparada para trafegar dados.

4.6 A disponibilização do serviço de internet deve ser permanente durante 24 (vinte e quatro) horas por dia x 7 (sete) dias por semana x 365 (trezentos e sessenta e cinco) dias por ano;

4.7 As paradas para manutenção emergenciais, interrupções preventivas ou programadas e a substituição de equipamentos devem ser informadas ao Dep. Tecnologia da Informação com antecedência mínima de 03 (três) dias úteis;

4.8 As interrupções preventivas devem ser em regra realizadas no horário de 00:00 até as 06:00 horas; se as paradas descritas causarem comprovada interferência no desempenho das atividades, o CONTRATADO concederá ao CONTRATANTE desconto na mensalidade à razão de 1/30 (uns trinta avos) por dia ou fração superior a 2 (duas) horas;

4.9 Disponibilidade de Link 1 Gbps Corporativo.

4.10 Link secundário de 300 MB Corporativo

4.11 Sem Custo de Instalação e/ou Disponibilização Serviço.

4.12 A velocidade contratada deverá ser garantida nos dois sentidos: download e upload.

4.13 Deverá ser enviado o KMZ que comprove que o POP do link e Enlace possui caminhos 100% distintos entre ambos os links, bem como o KMZ dos anéis de fibra do link com dupla abordagem.

4.14 Deverão estar inclusos na solução todos os recursos de conectividade, tais como: modems, conversores, roteadores appliance firewall com licenciamento UTP em alta disponibilidade para controle de trafego e failover automático entre as conexões com backbone internet com load balance activo e outros correlatos, bem como a infraestrutura para instalação dos equipamentos de transmissão necessária à prestação dos serviços.

4.15 Prestar serviço de gerenciamento incluindo a disponibilização de uma “Central de Atendimento” para rápida resposta às falhas/incidentes.

4.16 Os serviços de operação, manutenção e gerenciamento da rede serão de responsabilidades da CONTRATADA com a CONTRATANTE tendo plenos acessos caso seja necessário.

4.17 Os equipamentos necessários para implementar os serviços de comunicação de dados deverão ser disponibilizados e configurados pela CONTRATADA.

4.18 Os recursos de hardware e software dos equipamentos envolvidos devem ser atualizados tecnologicamente, sem ônus para a CONTRATANTE, durante a vigência do contrato.

4.19 Sempre que houver lançamento de nova versão de firmware que faça correções de segurança dos serviços prestados, a contratada deverá providenciar as devidas atualizações com prévia aprovação, sem ônus para a CONTRATANTE.

4.20 Todos os equipamentos e enlaces fornecidos pela CONTRATADA, nas suas condições de

fabricação, operação, manutenção, funcionamento, alimentação e instalação, deverão obedecer às normas e recomendações em vigor, elaboradas por órgãos oficiais competentes ou entidades autônomas reconhecidas na área – ABNT (Associação Brasileira de Normas Técnicas) e ANATEL (Agência Nacional de Telecomunicações), além de entidades de padrões reconhecidas internacionalmente – ITU (International Telecommunication Union), ISO (International Standardization Organization), IEEE (Institute of Electrical and Electronics Engineers), EIA/TIA (Electronics Industry Alliance and Telecomumnication Industry Association).

4.21 A empresa deverá apresentar junto a Nota Fiscal, relatório de atividades.

Unidades:

CCDTI - Centro Carioca de Diagnóstico e Tratamento por Imagem e UA - Unidades Avançadas

TIPO DE UNIDADE	NOME UNIDADE AVANÇADA	HORÁRIO FUNCIONAMENTO
SEDE	CENTRO CARIOCA DE DIAGNÓSTICO E TRATAMENTO POR IMAGEM	07:00 - 22:00h
UNIDADE AVANÇADA	HOSPITAL MUNICIPAL SOUZA AGUIAR	24HS
UNIDADE AVANÇADA	HOSPITAL MUNICIPAL LOURENÇO JORGE	24HS
UNIDADE AVANÇADA	HOSPITAL MUNICIPAL SALGADO FILHO	24HS
UNIDADE AVANÇADA	HOSPITAL MUNICIPAL MIGUEL COUTO	24HS
UNIDADE AVANÇADA	HOSPITAL MUNICIPAL RONALDO GAZOLLA	24HS
UNIDADE AVANÇADA	HOSPITAL MUNICIPAL FRANCISCO TELLES	24HS
UNIDADE AVANÇADA	HOSPITAL MUNICIPAL JESUS	24HS
UNIDADE AVANÇADA	HOSPITAL MUNICIPAL PIEDADE	24HS
UNIDADE AVANÇADA	UPA MADUREIRA	24HS
UNIDADE AVANÇADA	UPA CIDADE DE DEUS	24HS
UNIDADE AVANÇADA	POLICLÍNICA RODOLPHO ROCCO	24HS
UNIDADE AVANÇADA	POLICLÍNICA GUILHERME DA SILVEIRA	07:00 - 22:00h
UNIDADE AVANÇADA	POLICÍNICA LICOLN DE FREITAS	07:00 - 22:00h
UNIDADE AVANÇADA	HOSPITAL MUNICIPAL BELIZÁRIO PENNA	07:00 - 22:00h
UNIDADE AVANÇADA	CENTRO MUNICIPAL DE SAÚDE ADIB JATENE	07:00 - 22:00h
UNIDADE AVANÇADA	CLÍNICA DA FAMÍLIA OTTO ALVES DE CARVALHO	07:00 - 22:00h
UNIDADE AVANÇADA	CENTRO DE IMAGEM ROCINHA	07:00 - 22:00h
UNIDADE AVANÇADA	CENTRO MUNICIPAL DE SAÚDE HARVEY RIBEIRO	07:00 - 22:00h
UNIDADE AVANÇADA	HOSPITAL DO ANDARAÍ	24HS
UNIDADE AVANÇADA	HOSPITAL CARDOSO FONTES	24HS
UNIDADE AVANÇADA	HOSPITAL MUNICIPAL ALBERT SCHWEITZER	24HS
UNIDADE AVANÇADA	HOSPITAL MUNICIPAL EVANDRO FREIRE	24HS
UNIDADE AVANÇADA	HOSPITAL MUNICIPAL PEDRO II	24HS

5. FIREWALLS

5.1. CARACTERÍSTICAS TÉCNICAS DOS FIREWALLS

5.1.1. Todos os firewalls a serem fornecidos deverão ser Next-Generation Firewall (NGFW) para proteção de informação perimetral e de rede interna que inclui stateful firewall com capacidade para operar em alta disponibilidade (HA) em modo ativo-passivo ou ativo-ativo para controle de tráfego de dados por identificação de usuários e por camada 7, com controle de aplicação, administração de largura de banda (QoS), VPN IPsec e SSL, IPS, prevenção contra ameaças de vírus, *malwares*, Filtro de URL, criptografia de email, inspeção de tráfego criptografado e proteção de firewall de aplicação Web. Deverá ser fornecida console de gerenciamento dos equipamentos e centralização de logs em nuvem ou hardware específico ou virtualizado.

5.1.2. A console de gerenciamento em nuvem, deve estar no Brasil.

5.1.3. A console de gerenciamento deve ser possível atribuir configurações de concentradores de SD-WAN;

5.1.4. A console de gerenciamento deve dispor de configurações globais para replicação nos firewalls;

5.1.5. Deverão ser fornecidas as licenças para atualização de todos os componentes de software, vacinas de antivírus / malwares, endpoints, softwares de criptografia de armazenamento em nuvem e assinaturas de IPS, filtro de conteúdo web, controle de aplicações e proteção de firewall de aplicação web sem custo adicional, pelo período mínimo de 12 (doze) meses.

5.1.6. Para os itens que representem bens materiais, a CONTRATADA deverá fornecer produtos novos, sem uso anterior.

5.1.7. Por cada appliance físico que compõe a plataforma de segurança, entende-se o hardware, software e as licenças necessárias para o seu funcionamento.

5.1.8. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico.

5.1.9. Deve possuir processadores próprios e para fins específicos, desenvolvidos exclusivamente pelo fabricante da solução, com a finalidade de processar tráfegos de redes e acelerar o processamento destes pacotes de redes, permitindo o uso de diversas funcionalidades de segurança ao mesmo tempo sem diminuir a performance do equipamento.

5.1.10. Todos os equipamentos de rede deverão possuir certificado de homologação expedido pela Agência Nacional de Telecomunicações (ANATEL).

5.1.11. Por alta disponibilidade (HA) entende-se que a solução deverá ser composta ao menos por dois appliances, licenciados para funcionamento em redundância.

5.1.12. Caso a solução ofertada ofereça link dedicado para gerenciamento de HA, deverá suportar interfaces LAG e VLAN para o link HA dedicado e interfaces VLAN para links monitorados;

5.1.13. Cada appliance deverá ser capaz de executar a totalidade das capacidades exigidas para cada função, não sendo aceitos somatórias para atingir os limites mínimos.

5.1.14. O hardware e o software fornecidos não podem constar, no momento da apresentação da proposta, em listas de end-of-sale, end-of-support, end-of-engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante.

5.2. QUANTIDADES PREVISTAS

Aquisição de solução compreende aquisição de equipamentos (hardwares), softwares e prestação de serviços, conforme tabela abaixo:

5.2.1. **FIREWALL TIPO 1**

Item	Descrição	Quantidade
HARDWARE FIREWALL TIPO 1		
1	Firewall de Próxima Geração **Tipo 1** - Solução em cluster de alta disponibilidade (HA) ativo-passivo ou ativo-ativo composta de 04 (quatro) *appliances* (dois ativos e dois passivos) - Com 12 meses de suporte e garantia de hardware.	4 un
SOFTWARE FIREWALL TIPO 1		
2	Pacote de licenças de Firewall, IPS, Antivírus, Anti-spyware, Filtro de Web, Proteção contra ameaças avançadas e firewall de aplicação web para *appliance de Firewall de Próxima Geração* **Tipo 1** pelo prazo de 12 (doze) meses.	4 un
3	Pacote de licenças da Console de Gerência Administrativa e Centralização de Logs e Relatórios das soluções de Firewall de Próxima Geração **Tipo 1.**	1 un

5.2.2. **FIREWALL TIPO 2**

Item	Descrição	Quantidade
HARDWARE FIREWALL TIPO 2		
1	Firewall de Próxima Geração **Tipo 2** - Solução em cluster de alta disponibilidade (HA) ativo-passivo ou ativo-ativo composta de 23 (vinte e três) *appliances* (um ativo e um passivo) - Com 12 meses de suporte e garantia de hardware.	23 un
SOFTWARE FIREWALL TIPO 2		
2	Pacote de licenças de Firewall, IPS, Antivírus, Anti-spyware, Filtro de Web, Proteção contra ameaças avançadas e firewall de aplicação web para *appliance de Firewall de Próxima Geração* **Tipo 2** pelo prazo de 12 (doze) meses.	23 un

Item	Descrição	Quantidade
3	Pacote de licenças da Console de Gerência Administrativa e Centralização de Logs e Relatórios das soluções de Firewall de Próxima Geração **Tipo 2.**	1 un

5.3. CARACTERÍSTICAS ESPECÍFICAS DE DESEMPENHO E HARDWARE DO FIREWALL DE PRÓXIMA GERAÇÃO TIPO 1

5.3.1. Performance mínima de 19 Gbps de throughput para firewall.

5.3.2. Performance mínima de 4.6 Gbps de throughput de IPS.

5.3.3. Performance mínima de 4.3 Gbps de throughput para controle de NGFW.]

5.3.4. Performance mínima de 4 Gbps de Threat Protection throughput

5.3.5. Suportar no mínimo 1.45 Gbps de throughput de Inspeção SSL;

5.3.6. Performance mínima de 15 Gbps de throughput de IPsec VPN.

5.3.7. Suporte a, no mínimo, 6.000.000 de conexões simultâneas.

5.3.8. Suporte a, no mínimo, 72.000 novas conexões por segundo.

5.3.9. Possuir o número irrestrito quanto ao máximo de usuários licenciados.

5.3.10. Possuir armazenamento interno de no mínimo de 64 GB para sistema operacional, quarentena local, logs e relatórios.

5.3.11. Possuir no mínimo 8 GB de memória RAM

5.3.12. Possuir no mínimo 9 (nove) interfaces de rede 1000Base-TX;

5.3.13. Possuir no mínimo 1 (uma) interfaces 1GbE SFP;

5.3.14. Possuir 1 (uma) interface do tipo console ou similar.

5.3.15. Possuir 1 (uma) fonte 100-240VAC interna ou externa

5.3.16. O equipamento deverá possuir suporte a fontes de alimentação redundantes, permitindo a instalação de duas fontes de energia, sendo obrigatória a presença de pelo menos uma fonte instalada no momento da entrega, e a segunda disponível como opção para aquisição posterior.

5.4. CARACTERÍSTICAS GERAIS PARA FIREWALLS DE PRÓXIMA GERAÇÃO TIPO 1

5.4.1. A solução deve consistir em appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência, monitoração e logs.

5.4.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.

5.4.3. O fabricante deverá disponibilizar todas as funcionalidades de segurança (IPS, Web, Aplicações, Sandboxing, Antivírus, Controle de Aplicação, SSL Inspection e SD-WAN) em licenciamento unificado, sem necessidade de chaves, pacotes ou módulos adicionais.

5.4.4. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação.

5.4.5. A solução deverá incluir tecnologia de sandboxing para análise dinâmica e comportamental de arquivos suspeitos e objetos em ambiente isolado (sandbox), integrada à plataforma de segurança do fabricante, podendo ser implementada de forma nativa ou dedicada, desde que sob console e gerenciamento do mesmo fabricante dos firewalls.

5.4.6. A solução deverá permitir SD-WAN com roteamento baseado em medição de latência, jitter e perda de pacotes em tempo real, aplicável a redes de origem, redes de destino e aplicações.

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

5.4.8. O software deverá ser fornecido em sua versão mais atualizada.

5.4.9. O HA (modo de alta disponibilidade) deve suportar o uso de dois equipamentos em modo ativo-passivo ou modo ativo-ativo e deve possibilitar monitoração de falha de link.

5.4.10. Uma interface completa de comando de linha (CLI command-line-interface) deverá ser acessível através da interface gráfica e via porta serial.

5.4.11. A atualização de software deverá enviar avisos de atualização automáticos.

5.4.12. O sistema de objetos deverá permitir a definição de redes, serviços, hosts períodos de tempos, usuários e grupos, clientes e servidores.

5.4.13. O backup e o reestabelecimento de configuração deverão ser feitos localmente, via FTP ou email com frequência diária, semanal ou mensal, podendo também ser realizado por demanda.

5.4.14. As notificações deverão ser realizadas via email e SNMP.

5.4.15. Suportar SNMPv3 e Netflow.

5.4.16. O firewall deverá ser stateful, com inspeção profunda de pacotes.

5.4.17. As zonas deverão ser divididas pelo menos em WAN, LAN e DMZ, sendo necessário que as zonas LAN e DMZ possam ser customizáveis.

5.4.18. As políticas de NAT deverão ser customizáveis para cada regra.

5.4.19. A proteção contra flood deverá ter proteção contra DoS (Denial of Service), DdoS (Distributed DoS).

5.4.20. Proteção contra anti-spoofing.

5.4.21. Suportar IPv4 e IPv6.

5.4.22. Possuir certificação IPv6 Ready;

5.4.23. IPv6 deve suportar os tunelamentos 6in4, 6to4, 4in6 e IPv6 Rapid Deployment (6rd) de acordo com a RFC 5969.

5.4.24. Suportar NAT64 e NAT66 minimamente;

5.4.25. Suporte aos roteamentos estáticos, dinâmico (RIP, BGP e OSPF, OSPFv3) e multicast (PIM-SM e IGMP).

5.4.26. Deve suportar Roteamento BGP com uso de IPv6;

5.4.27. Suportar Delegação de Prefixo IPV6 (DHCP PD);

5.4.28. O firewall deve possuir integração com a plataforma de ZTNA do mesmo fabricante ou integrar de terceiros;

5.4.29. Deve possuir tecnologia de conectividade SD-WAN;

5.4.30. A funcionalidade SD-WAN deve suportar conectividade com o Secure SD-WAN oferecido no serviço Microsoft Azure Virtual WAN;

5.4.31. Deve suportar perfis de SD-WAN para balancear a carga das conexões entre as interfaces,

5.4.32. Deve possuir métodos de balanceamento: round-robin e persistência de sessão com as seguintes opções:

a. 1.4.24.1 conexão:
b. 1.2.24.2 IP de origem;
c. 1.4.24.3 IP de destino;
d. 1.4.24.4 IP de origem e destino.

5.4.33. Os links podem ser ponderados para determinar como o tráfego é distribuído entre eles, podendo usar o SLA para selecionar quais links serão incluídos no balanceamento de carga.

5.4.34. Deve suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SDWAN;

5.4.35. Deve suportar o uso de, no mínimo, 3 (três) links;

5.4.36. Deve suportar o uso de links de interfaces físicas, sub-interfaces lógicas de VLAN e túneis IPSec;

5.4.37. Deve gerar log de eventos que registrem alterações no estado dos links do SD-WAN, monitorados pela checagem de saúde;

5.4.38. A solução deverá ser capaz de medir o status de saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Threshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN;

5.4.39. A solução de SD-WAN deve ser capaz de apresentar de forma gráfica, todos os dados de análise da saúde dos links, contendo gráficos que apresentam no mínimo os critérios descritos acima;

5.4.40. Os gráficos devem ser apresentados em tempo real e possibilitar a visualização histórica de pelo menos 24 horas, 48 horas, 1 semana e 1 mês;

5.4.41. A checagem de estado de saúde deve suportar a marcação de pacotes com DSCP, para avaliação mais precisa de links que possuem QoS configurado

5.4.42. A solução deve possuir funcionalidade de criação da malha SD-WAN em diversos firewalls em um único concentrador;

5.4.43. Esta funcionalidade deve facilitar a configuração do SD-WAN de múltiplos firewalls, criando automaticamente todas as informações necessárias para que o SD-WAN aconteça, como pelo menos, mas não se limitando a: criação de rotas, regras de firewall, objetos e túneis VPNs necessárias;

5.4.44. A mesma console do concentrador de SD-WAN deve monitorar os links de cada dispositivo implementado, garantindo uma visualização única de todos os dispositivos implementados;

5.4.45. Deve possibilitar o roteamento baseado em VPNs;

5.4.46. Deve suportar criar políticas de roteamento;

5.4.47. Para as políticas de roteamento, devem ser permitidas pelo menos as seguintes condições:

5.4.48. Interface de entrada do pacote;

5.4.49. IPs de origem;

5.4.50. IPs de destino;

5.4.51. Portas de destino;

5.4.52. Usuários ou grupos de usuários;

5.4.53. Aplicação em camada 7

5.4.54. Deve ser possível escolher um gateway primário e um gateway de backup para as políticas de roteamento

5.4.55. Deve suportar a definição de VLANs no firewall conforme padrão IEEE 802.1q e tagging de VLAN.

5.4.56. O balanceamento de link WAN deve permitir múltiplas conexões de links Internet, checagem automática do estado de links, failover automático e balanceamento por peso.

5.4.57. A solução deverá permitir port-aggregation de interfaces de firewall suportando o protocolo 802.3ad, para escolhas entre aumento de throughput e alta disponibilidade de interfaces;

5.4.58. Deve permitir a configuração de jumbo frames nas interfaces de rede;

5.4.59. Deve permitir a criação de um grupo de portas layer2;

5.4.60. A Solução física deverá apresentar compatibilidade com modens USB (4G/5G), onde apenas seja acionado na eventualidade de falha no link principal;

5.4.61. A solução deverá permitir configurar os serviços de DNS, Dynamic DNS, DHCP e NTP;

5.4.62. O traffic shapping (QoS) deverá ser baseado em rede ou usuário.

5.4.63. A solução deve permitir o tráfego de cotas baseados por usuários para upload/download e pelo tráfego total, sendo cíclicas ou não-cíclicas.

5.4.64. Deve possuir otimização em tempo real de voz sobre IP.

5.4.65. Deve implementar o protocolo de negociação Link Aggregation Control Protocol (LACP).

5.5. CARACTERÍSTICAS ESPECÍFICAS DE DESEMPENHO E HARDWARE DO FIREWALL DE PRÓXIMA GERAÇÃO TIPO 2

5.5.1. Performance mínima de 9.9 Gbps de throughput para firewall.

5.5.2. Performance mínima de 2 Gbps de throughput de IPS.

5.5.3. Performance mínima de 2 Gbps de throughput para controle de NGFW.]

5.5.4. Performance mínima de 2 Gbps de Threat Protection throughput

5.5.5. Suportar no mínimo 600 Mbps de throughput de Inspeção SSL;

5.5.6. Performance mínima de 6 Gbps de throughput de IPsec VPN.

5.5.7. Suporte a, no mínimo, 1.600.000 de conexões simultâneas.

5.5.8. Suporte a, no mínimo, 40.400 novas conexões por segundo.

5.5.9. Possuir o número irrestrito quanto ao máximo de usuários licenciados.

5.5.10. Possuir armazenamento interno de no mínimo de 16 GB

5.5.11. Possuir no mínimo 4 GB de memória RAM

5.5.12. Possuir no mínimo 4 (quatro) interfaces de rede 1000Base-TX;

5.5.13. Possuir 1 (uma) interface do tipo console ou similar.

5.5.14. Possuir 1 (uma) fonte 100-240VAC interna ou externa.

5.6. CARACTERÍSTICAS GERAIS PARA FIREWALLS DE PRÓXIMA GERAÇÃO TIPO 2

5.6.1. A solução deve consistir em appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência, monitoração e logs.

5.6.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.

5.6.3. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação.

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

5.6.5. O software deverá ser fornecido em sua versão mais atualizada.

5.6.6. O HA (modo de alta disponibilidade) deve suportar o uso de dois equipamentos em modo ativo-passivo ou modo ativo-ativo e deve possibilitar monitoração de falha de link.

5.6.7. Uma interface completa de comando de linha (CLI command-line-interface) deverá ser acessível através da interface gráfica e via porta serial.

5.6.8. A atualização de software deverá enviar avisos de atualização automáticos.

5.6.9. O sistema de objetos deverá permitir a definição de redes, serviços, hosts períodos de tempos, usuários e grupos, clientes e servidores.

5.6.10. O backup e o reestabelecimento de configuração deverão ser feitos localmente, via FTP ou email com frequência diária, semanal ou mensal, podendo também ser realizado por demanda.

5.6.11. As notificações deverão ser realizadas via email e SNMP.

5.6.12. Suportar SNMPv3 e Netflow.

5.6.13. O firewall deverá ser stateful, com inspeção profunda de pacotes.

5.6.14. As zonas deverão ser divididas pelo menos em WAN, LAN e DMZ, sendo necessário que as zonas LAN e DMZ possam ser customizáveis.

5.6.15. As políticas de NAT deverão ser customizáveis para cada regra.

5.6.16. A proteção contra flood deverá ter proteção contra DoS (Denial of Service), DdoS (Distributed DoS).

5.6.17. Proteção contra anti-spoofing.

5.6.18. Suportar IPv4 e IPv6.

5.6.19. Possuir certificação IPv6 Ready;

5.6.20. IPv6 deve suportar os tunelamentos 6in4, 6to4, 4in6 e IPv6 Rapid Deployment (6rd) de acordo com a RFC 5969.

5.6.21. Suportar NAT64 e NAT66 minimamente;

5.6.22. Suporte aos roteamentos estáticos, dinâmico (RIP, BGP e OSPF, OSPFv3) e multicast (PIM-SM e IGMP).

5.6.23. Deve suportar Roteamento BGP com uso de IPv6;

5.6.24. Suportar Delegação de Prefixo IPV6 (DHCP PD);

5.6.25. O firewall deve possuir integração com a plataforma de ZTNA do mesmo fabricante ou integrar de terceiros;

5.6.26. Deve possuir tecnologia de conectividade SD-WAN;

5.6.27. A funcionalidade SD-WAN deve suportar conectividade com o Secure SD-WAN oferecido no serviço Microsoft Azure Virtual WAN;

5.6.28. Deve suportar perfis de SD-WAN para balancear a carga das conexões entre as interfaces,

5.6.29. Deve possuir métodos de balanceamento: round-robin e persistência de sessão com as seguintes opções:

a. 1.4.24.1 conexão:
b. 1.2.24.2 IP de origem;
c. 1.4.24.3 IP de destino;
d. 1.4.24.4 IP de origem e destino.

5.6.30. Os links podem ser ponderados para determinar como o tráfego é distribuído entre eles, podendo usar o SLA para selecionar quais links serão incluídos no balanceamento de carga.

5.6.31. Deve suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SDWAN;

5.6.32. Deve suportar o uso de, no mínimo, 3 (três) links;

5.6.33. Deve suportar o uso de links de interfaces físicas, sub-interfaces lógicas de VLAN e túneis IPSec;

5.6.34. Deve gerar log de eventos que registrem alterações no estado dos links do SD-WAN, monitorados pela checagem de saúde;

5.6.35. A solução deverá ser capaz de medir o status de saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN;

5.6.36. A solução de SD-WAN deve ser capaz de apresentar de forma gráfica, todos os dados de análise da saúde dos links, contendo gráficos que apresentam no mínimo os critérios descritos acima;

5.6.37. Os gráficos devem ser apresentados em tempo real e possibilitar a visualização histórica de pelo menos 24 horas, 48 horas, 1 semana e 1 mês;

5.6.38. A checagem de estado de saúde deve suportar a marcação de pacotes com DSCP, para avaliação mais precisa de links que possuem QoS configurado

5.6.39. A solução deve possuir funcionalidade de criação da malha SD-WAN em diversos firewalls em um único concentrador;

5.6.40. Esta funcionalidade deve facilitar a configuração do SD-WAN de múltiplos firewalls, criando automaticamente todas as informações necessárias para que o SD-WAN aconteça, como pelo menos, mas não se limitando a: criação de rotas, regras de firewall, objetos e túneis VPNs necessárias;

5.6.41. A mesma console do concentrador de SD-WAN deve monitorar os links de cada dispositivo implementado, garantindo uma visualização única de todos os dispositivos implementados;

5.6.42. Deve possibilitar o roteamento baseado em VPNs;

5.6.43. Deve suportar criar políticas de roteamento;

5.6.44. Para as políticas de roteamento, devem ser permitidas pelo menos as seguintes condições:

5.6.45. Interface de entrada do pacote;

5.6.46. IPs de origem;

5.6.47. IPs de destino;

5.6.48. Portas de destino;

5.6.49. Usuários ou grupos de usuários;

5.6.50. Aplicação em camada 7

5.6.51. Deve ser possível escolher um gateway primário e um gateway de backup para as políticas de roteamento

5.6.52. Deve suportar a definição de VLANs no firewall conforme padrão IEEE 802.1q e tagging de VLAN.

5.6.53. O balanceamento de link WAN deve permitir múltiplas conexões de links Internet, checagem automática do estado de links, failover automático e balanceamento por peso.

5.6.54. A solução deverá permitir port-aggregation de interfaces de firewall suportando o protocolo 802.3ad, para escolhas entre aumento de throughput e alta disponibilidade de interfaces;

5.6.55. Deve permitir a configuração de jumbo frames nas interfaces de rede;

5.6.56. Deve permitir a criação de um grupo de portas layer2;

5.6.57. A solução deverá permitir configurar os serviços de DNS, Dynamic DNS, DHCP e NTP;

5.6.58. O traffic shapping (QoS) deverá ser baseado em rede ou usuário.

5.6.59. A solução deve permitir o tráfego de cotas baseados por usuários para upload/download e pelo tráfego total, sendo cíclicas ou não-cíclicas.

5.6.60. Deve possuir otimização em tempo real de voz sobre IP.

5.6.61. Deve implementar o protocolo de negociação Link Aggregation Control Protocol (LACP).

5.7. CONTROLE POR POLÍTICAS DE FIREWALL

5.7.1. Deve suportar controles por: porta e protocolos TCP/UDP, origem/destino e identificação de usuários.

5.7.2. O controle de políticas deverá monitorar as políticas de redes, usuários, grupos e tempo, bem como identificar as regras não-utilizadas, desabilitadas, modificadas e novas políticas.

5.7.3. As políticas deverão ter controle de tempo de acesso por usuário e grupo, sendo aplicadas por zonas, redes e por tipos de serviços.

5.7.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.

5.7.5. Controle de políticas por países via localização por IP.

5.7.6. Suporte a objetos e regras IPv6.

5.7.7. Suporte a objetos e regras multicast.

5.8. PREVENÇÃO DE AMEAÇAS

5.8.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus, Anti-Malware e integrados no próprio appliance de Firewall ou entregue em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação.

5.8.2. Deve realizar a inspeção profunda de pacotes para prevenção de intrusão (IPS) e deve incluir assinaturas de prevenção de intrusão (IPS).

5.8.3. As assinaturas de prevenção de intrusão (IPS) devem ser customizadas.

5.8.4. Deve possuir proteção de DNS, inclusa no licenciamento para fornecer um serviço de resolução de DNS seguro disponível globalmente com relatórios e controles de política integrados a console de gerenciamento centralizado.

5.8.5. Deve suportar o recebimento de feeds de ameaças de terceiros (IoC) minimamente com os seguintes formatos e autenticações: IP, domínio, URL, sem autenticação, autenticação de usuário e senha e via chave de API, sendo compatível com bases como: CrowdSec, GreyNoise, Cisco Talos, GitHub, TOR;

5.8.6. Entende-se que feeds de ameaças são uma lista de endereços IP, domínios e URLs envolvidos em atividades de ameaças, como phishing e malware. Esses objetos são chamados de Indicadores de Comprometimento (IoCs) ou indicadores de ataque.

5.8.7. Em appliances exclusivamente deve dispor de camada de proteção contra ameaças analizando os fluxos de tráfego usando o NDR ML (Network Detect and Response com Machine Learning) em nuvem, realizando análise de carga útil criptografada sem a necessidade de descriptografia TLS.

5.8.8. Exceções por usuário, grupo de usuários, IP de origem ou de destino devem ser possíveis nas regras;

5.8.9. Deve suportar granularidade nas políticas de IPS Antivírus e Anti-Malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens, com customização completa;

5.8.10. A solução contratada deve realizar a emulação de malwares desconhecidos em ambientes de sandbox em nuvem;

5.8.11. Para a eficácia da análise de malwares Zero-Day, a solução de Sandbox deve possuir algoritmos de inteligência artificial, como algoritmos baseados em machine learning;

5.8.12. A funcionalidade de sandbox deve atuar como uma camada adicional ao motor de antimalware, e ao fim da análise do artefato, deverá gerar um relatório contendo o resultado da análise, bem como os screenshots das telas dos sistemas emulados pela plataforma;

5.8.13. Deve permitir configuração da exclusão de tipos de arquivos para que não sejam enviados para o sandbox em nuvem;

5.8.14. A proteção Anti-Malware deverá bloquear todas as formas de vírus, web malwares, trojans e spyware em HTTP e HTTPS, FTP e web-emails.

5.8.15. A proteção Anti-Malware deverá realizar a proteção com emulação JavaScript.

5.8.16. Deve ter proteção em tempo real contra novas ameaças criadas.

5.8.17. Deve possuir pelo menos duas engines de antivírus independentes e de diferentes fabricantes para a detecção de malware, podendo ser configuradas isoladamente ou simultaneamente.

5.8.18. Deve permitir o bloqueio de vulnerabilidades.

5.8.19. Deve permitir o bloqueio de exploits conhecidos.

5.8.20. Deve detectar e bloquear o tráfego de rede que busque acesso a command and control e servidores de controle utilizando múltiplas camadas de DNS, AFC e firewall.

5.8.21. Deve incluir proteção contra-ataques de negação de serviços.

5.8.22. Ser imune e capaz de impedir ataques básicos como: SYN flood, ICMP flood, UDP Flood, etc.

5.8.23. Suportar bloqueio de arquivos por tipo.

5.8.24. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.

5.8.25. Os eventos devem identificar o país de onde partiu a ameaça.

5.8.26. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas de segurança considerando uma das opções ou a combinação de todas elas: usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por usuários, grupos de usuários, origem, destino, zonas de segurança.

5.9. CONTROLE E PROTEÇÃO DE APLICAÇÕES

5.9.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações por assinaturas e camada 7, utilizando portas padrões (80 e 443), portas não padrões, port hopping e túnel através de tráfego SSL encriptado.

5.9.2. Deve ser possível inspecionar os pacotes criptografados com os algoritmos SSL 2.0, SSL 3.0, TLS 1.2 e TLS 1.3

5.9.3. O motor de análise de tráfego criptografado deve reconhecer, mas não limitado a, pelo menos os seguintes algorítimos: curvas elipticas (ECDH, ECDHE, ECDSA), DH, DHE, Authentication, RSA, DSA, ANON, Bulk ciphers, RC4, 3DES, IDEA, AES128, AES256, Camellia, ChaCha20-Poly1305, GCM, CCM, CBC, MD5, SHA1, SHA256, SHA384.

5.9.4. O motor de inspeção dos pacotes criptografados deve ser configurável e permitir definir ações como não descriptografar, negar o pacote e criptografar para determinadas conexões criptografadas

5.9.5. Reconhecer pelo menos 3.680 aplicações diferentes, classificadas por nível de risco, características e tecnologia, incluindo, mas não limitado a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, IA Generativa, update de software, serviços de rede, VoIP, streaming de mídia, proxy e tunelamento, mensageiros instantâneos, compartilhamento de arquivos, web e-mail e update de softwares.

5.9.6. Reconhecer pelo menos as seguintes aplicações: 4Shared File Transfer, Active Directory/SMB, Citrix ICA, DHCP Protocol, Dropbox Download, Easy Proxy, Facebook Graph API, Firefox Update, Freegate Proxy, FreeVPN Proxy, Gmail Video, Chat Streaming, Gmail WebChat, Gmail WebMail, Gmail-Way2SMS WebMail, Gtalk Messenger, Gtalk Messenger File Transfer, Gtalk-Way2SMS, HTTP Tunnel Proxy, HTTPort Proxy, LogMeIn Remote Access, NTP, Oracle database, RAR File Download, Redtube Streaming, RPC over HTTP Proxy, Skydrive, Skype, Skype Services, skyZIP, SNMP Trap, TeamViewer Conferencing e File Transfer, TOR Proxy, Torrent Clients P2P, Ultrasurf Proxy, UltraVPN, VNC Remote Access, VNC Web Remote Access, WhatsApp, WhatsApp File Transfer e WhatsApp Web.

5.9.7. Deve realizar o escaneamento e controle de micro app incluindo, mas não limitado a: Facebook (Applications, Chat, Commenting, Events, Games, Like Plugin, Message, Pics Download e Upload, Plugin, Post Attachment, Posting, Questions, Status Update, Video Chat, Video Playback, Video Upload, Website), Freegate Proxy, Gmail (Android Application, Attachment), Google Drive (Base, File Download, File Upload), Google Earth Application, Google Plus, LinkedIN (Company Search, Compose Webmail, Job Search, Mail Inbox, Status Update), SkyDrive File Upload e Download, Twitter (Message, Status Update, Upload, Website), Yahoo (WebMail, WebMail File Attach) e Youtube (Video Search, Video Streaming, Upload, Website).

5.9.8. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante.

5.9.9. Atualizar a base de assinaturas de aplicações automaticamente.

5.9.10. Reconhecer aplicações em IPv6.

5.9.11. Limitar a banda usada por aplicações (traffic shaping).

5.9.12. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory e Azure AD, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários.

5.9.13. Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras.

5.9.14. Deve permitir o uso individual de diferentes aplicativos para usuários que pertencem ao mesmo grupo de usuários, sem que seja necessária a mudança de grupo ou a criação de um novo grupo. Os demais usuários deste mesmo grupo que não possuírem acesso a estes aplicativos devem ter a utilização bloqueada.

5.10. CONTROLE E PROTEÇÃO WEB

5.10.1. Deve permitir especificar política de navegação Web por tempo, ou seja, a definição de regras para um determinado dia da semana e horário de início e fim, permitindo a adição de múltiplos dias e horários na mesma definição de política por tempo. Esta regra de tempo pode ser recorrente ou em uma única vez.

5.10.2. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs e redes;

5.10.3. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via LDAP, Active Directory, Azure AD, Radius, E-directory e base de dados local;

5.10.4. Deve permitir autenticação em 2 fatores em conjunto com a autenticação Radius;

5.10.5. Permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;

5.10.6. Possuir pelo menos 90 categorias de URLs;

5.10.7. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

5.10.8. Deve ser capaz de forçar o uso da opção Safe Search em sites de busca;

5.10.9. Deve ser capaz de forçar as restrições do Youtube.

5.10.10. Deve ser capaz de categorizar as URLs a partir de base ou cache de URLs locais ou através de consultas dinâmicas na nuvem do fabricante, independentemente do método de classificação a categorização não deve causar atraso na comunicação visível ao usuário;

5.10.11. Suportar a criação categorias de URLs customizadas;

5.10.12. Suportar a opção de bloqueio de categoria HTTP e liberação da categoria apenas em HTTPS.

5.10.13. Deve ser possível reconhecer o pacote HTTP independentemente de qual porta esteja sendo utilizada

5.10.14. Suportar a inclusão nos logs do produto de informações das atividades dos usuários;

5.10.15. Deve salvar nos logs as informações adequadas para geração de relatórios indicando usuário, tempo de acesso, bytes trafegados e site acessado.

5.10.16. Deve permitir realizar análise flow dos pacotes, entendendo exatamente o que aconteceu com o pacote em cada checagem;

5.10.17. Deve ser possível realizar caching do conteúdo web;

5.10.18. Deve realizar filtragem por mime-type, extensão e tipos de conteúdo ativos, tais como, mas não limitado a: ActiveX, applets e cookies.

5.10.19. Deve ser possível realizar a liberação de cotas de navegação para os usuários, permitindo que os usuários tenham tempos pré-determinados para acessar sites na internet.

5.10.20. A console de gerenciamento deve possibilitar a visualização do tempo restante para cada usuário, bem como reiniciar o tempo restante com o intuito de zerar o contador.

5.10.21. Deve possuir capacidade de alguns usuários previamente selecionados realizarem um bypass temporário na política de bloqueio atual.

5.10.22. A solução deve permitir o enforce dos domínios do Google e Office365 a fim de determinar em quais domínios os usuários poderão se autenticar;

5.11. IDENTIFICAÇÃO DE USUÁRIOS

5.11.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticando via LDAP, Active Directory, Azure AD, Radius, eDirectory, TACACS+ e via base de dados local, para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.

5.11.2. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal).

5.11.3. Deve permitir autenticação em modos: transparente, autenticação proxy (explicito, NTLM e Kerberos) e autenticação via clientes nas estações com os sistemas operacionais Windows, macOS e Linux 32/64.

5.11.4. Ao se utilizar da opção de proxy explicito, deve permitir a autenticação por cada conexão, a fim de garantir que usuários logados em servidores de multisessão sejam identificados corretamente pelo firewall, mesmo quando utilizando-se apenas 1 IP de origem;

5.11.5. Deve possuir a autenticação Single sign-on para, pelo menos, os sistemas de diretórios Active Directory, Azure AD e eDirectory.

5.11.6. Dever suportar a configuração de logon único (Single sign-on) para que os administradores façam logon no console da Web usando o Azure AD

5.11.7. Deve suportar SSO do Azure AD para o Captive Portal;

5.11.8. Deve possuir um portal de acesso seguro a configurações e agente de VPN

5.11.9. Deve ser compatível com SSO Entra ID (Azure AD) para o agente de VPN client to site IPsec, SSL e o Portal de VPN

5.11.10. Deve possuir portal do usuário para que os usuários tenham acesso ao uso de internet pessoal, troquem senhas da base local e façam o download de softwares para as estações presentes na solução.

5.12. QUALIDADE DE SERVIÇO – QoS

5.12.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações.

5.12.2. A solução deverá suportar Traffic Shaping (Qos) e a criação de políticas baseadas em categoria web e aplicação por: endereço de origem; endereço de destino; usuário e grupo do LDAP/AD.

5.12.3. Deve ser configurado o limite e a garantia de upload/download, bem como ser priorizado o tráfego total e bitrate de modo individual ou compartilhado.

5.12.4. Suportar priorização Real-Time de protocolos de voz (VoIP).

5.12.5. Deve permitir aplicar prioridade mesmo após o roteamento, utilizando o protocolo DSCP;

5.13. REDES VIRTUAIS PRIVADAS – VPN

5.13.1. Suportar VPN Site-to-Site e Cliente-to-Site.

5.13.2. Suportar IPsec VPN.

5.13.3. Suportar SSL VPN.

5.13.4. Suportar L2TP e PPTP.

5.13.5. Suportar acesso remoto SSL, IPSec e VPN Client para Android e iPhone/iPAD.

5.13.6. Deve ser disponibilizado o acesso remoto ilimitado, até o limite suportado de túneis VPN pelo equipamento, sem a necessidade de aquisição de novas licenças e sem qualquer custo adicional para o licenciamento de clientes SSL.

5.13.7. Deve possuir o acesso via o portal de usuário para o download e configuração do cliente SSL para Windows.

5.13.8. Deve possuir opção de VPN IPSEC com client nativo do fabricante.

5.13.9. Deve possuir um portal encriptado baseado em HTML5 para suporte pelo menos a: RDP, SSH, Telnet e VNC, sem a necessidade de instalação de clientes VPN nas estações de acesso.

5.13.10. A VPN IPsec deve suportar: DES, 3DES, GCM, Suite-B, Autenticação MD5 e SHA-1; Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; Algoritmo Internet Key Exchange (IKE); AES 128, 192 e 256 (Advanced Encryption Standard); SHA 256, 384 e 512; Autenticação via certificado PKI (X.509) e Pre-shared key (PSK).

5.13.11. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, SonicWALL, Fortinet, Huawei, Juniper, Palo Alto Networks e Sophos.

5.13.12. Deve suportar nativamente a integração com a Amazon, a fim de estabelecer um túnel seguro entre os appliances e o VPN da AWS.

5.13.13. Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, Anti-Malware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

5.13.14. Suportar autenticação via AD/LDAP, Token e base de usuários local;

5.13.15. Permitir estabelecer um túnel SSL VPN com uma solução de autenticação via LDAP, Active Directory, Azure AD, Radius, eDirectory, TACACS+ e via base de dados local;

5.14. GERÊNCIA ADMINISTRATIVA CENTRALIZADA

5.14.1. Deve possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos através de uma única console central, com administração de privilégios e funções.

5.14.2. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança.

5.14.3. Estar licenciada para gerenciar as soluções de firewall de próxima geração Tipo1 e Tipo 2.

5.14.4. O sistema de gerenciamento centralizado deverá suportar nativamente todos os firewalls de próxima geração do Tipo I e Tipo II adquiridos neste edital, de forma simultânea, sem necessidade de aquisição de licenças adicionais ou custo adicionais por parte da contratante.

5.14.5. Devem ser fornecidas soluções virtuais ou via appliances desde que obedeçam a todos os requisitos desta especificação.

5.14.6. Deve ser centralizada a gerência de todas as políticas do firewall e configurações para as soluções de firewall de próxima geração Tipo1 e Tipo 2, sem necessidade de acesso direto aos equipamentos.

5.14.7. Deve permitir a criação de Templates para configurações.

5.14.8. Deve possuir indicadores do estado de equipamentos e rede.

5.14.9. Deve emitir alertas baseados em thresholds customizáveis, incluindo também alertas de expiração de subscrição, mudança de status de gateways, uso excessivo de disco, eventos ATP, IPS, ameaças de vírus, navegação, entre outros.

5.14.10. Deve permitir a criação de grupos de equipamentos por nome, modelo, firmware e regiões.

5.14.11. Deve ter controle de privilégios administrativos, com granularidade de funções (VPN admin, App e Web admin, IPS admin, etc);

5.14.12. Deve ter logs de auditoria de uso administrativo e atividades realizadas nos equipamentos.

5.14.13. Deve ter integração com a solução de logs e relatórios, habilitando o provisionamento automático de novos equipamentos e a sincronização dos administradores da centralização da gerência com a centralização de logs e relatórios.

5.14.14. Deve possibilitar o envio dos logs via syslog com conexão segura (TLS)

5.15. GERÊNCIA DE LOGS E RELATÓRIOS CENTRALIZADOS

5.15.1. Deve possuir solução de logs e relatórios centralizados, possibilitando a consolidação total de todas as atividades da solução através de uma única console central.

5.15.2. Estar licenciada para gerenciar as soluções de firewall de próxima geração Tipo1 e tipo 2.

5.15.3. Devem ser fornecidas soluções virtuais, ou em nuvem ou via appliances desde que obedeçam a todos os requisitos desta especificação, com armazenamento mínimo de 8TB de dados.

5.15.4. O sistema de gerenciamento e análise de logs deverá possuir capacidade de armazenamento e processamento mínimo de 110 GB (cento e dez gigabytes) de logs por dia, considerando os registros provenientes de todos os firewalls de próxima geração (Tipo I e Tipo II) fornecidos neste processo.

5.15.5. Deverá prover relatórios baseados em usuários, com visibilidade sobre acesso a aplicações, navegação, eventos ATP, downloads e consumo de banda, independente em qual rede ou IP o usuário esteja se conectando.

5.15.6. Deve possibilitar a identificação de ataques como a identificação de malware identificados pelos eventos ATP, usuários suspeitos, tráfegos anômalos incluindo tráfego ICMP e consumo não-usual de banda.

5.15.7. Deve conter relatórios pré-configurados, pelo menos de: aplicações, navegação, web server (WAF), IPS, ATP e VPN;

5.15.8. Deve fornecer relatórios históricos para análises de mudanças e comportamentos.

5.15.9. Deve conter customizações dos relatórios para inserção de logotipos próprios.

5.15.10. Deve fornecer relatórios de compliance SOX, HIPAA, GLBA, FISMA, PCI, CIPA

5.15.11. Deve permitir a exportação via PDF ou Excel.

5.15.12. Deve fornecer relatórios sobre os acessos de procura no Google, Yahoo, Bing e Wikipedia.

5.15.13. Deve fornecer relatórios de tendências.

5.15.14. Deve fornecer logs em tempo real, de auditoria e arquivados.

5.15.15. Deve possuir mecanismo de procura de logs arquivados.

5.15.16. Deve ter acesso baseado em Web com controles administrativos distintos.

6. SERVIÇOS GERENCIADOS DE SEGURANÇA – MSS

Prestação de serviços gerenciados de segurança (Managed Security Services – MSS), incluindo o fornecimento, implantação, gestão, operação, monitoramento, suporte e manutenção de firewalls de perímetro e internos, de modo a garantir a proteção contínua da infraestrutura de rede corporativa, para atender as necessidades do CDC - Centro Diagnóstico Carioca.

6.1. ESCOPO DO SERVIÇO

6.1.1. **O serviço abrangerá:**

- Fornecimento e implantação de firewalls com recursos de IPS, VPN, web filtering, controle de aplicações e HA.
- Gestão e monitoramento contínuo (24x7) via SOC.
- Tratamento e resposta a incidentes, atualização de firmware, backups e análise de tráfego.
- Gestão de políticas e correlação de eventos de segurança.
- Entrega de relatórios técnicos e gerenciais.
- Gestão de eventos e alertas.
- Monitoramento de disponibilidade e performance.
- Gestão de versões de firmware.

6.2. EXECUÇÃO DOS SERVIÇOS DO CENTRO DE OPERAÇÕES

6.2.1. A CONTRATADA deverá, para atendimento a esse requisito, possuir um Centro de Operações próprio, redundante de Gerenciamento, monitoramento e atendimento com profissionais capacitados para atendimento 24x7 para resoluções de problemas de incidentes de segurança; atendendo a todas as características exigidas no Termo de Referência.

6.2.2. O Centro de Operações não pode ser terceirizado ou ser contratado na nuvem, para a prestação dos serviços, devendo ser físico e possuir uma instância dedicada para o INSTITUTO GNOSIS;

6.2.3. A disposição Geográfica, para estabelecer redundância de ambiente físico é de no mínimo uma distância de 400 (quatrocentos) km;

6.2.4. A contratada deverá comprovar que dispõe de uma infraestrutura de Centro de Operações robusta, equivalente ou superior ao local onde os serviços serão prestados. A infraestrutura mínima do site principal, deverá ser composta por:

6.2.4.1.1. Dupla entrada de energia elétrica;

6.2.4.1.2. Sistema de fornecimento de energia elétrica estabilizada e ininterrupta, com potência total mínima de 300 KVA;

6.2.4.1.3. Grupos geradores dimensionados para suportar 100% da demanda do edifício, e com redundância;

6.2.4.1.4. Segurança armada 24x7;

6.2.5. A CONTRATANTE poderá realizar diligências no site principal da CONTRATADA, onde esta fisicamente o seu Centro de Operações e serão realizados todos os serviços aqui descritos, para verificações de atendimento aos requisitos deste serviço, sendo item desclassificatório;

6.2.6. A CONTRATADA deverá implantar a solução e realizar todas as integrações com o ambiente do INSTITUTO GNOSIS, conforme escopo abaixo:

- Levantamento de requisitos;
- Definição de escopo;
- Desenho da solução;
- Escolha das ferramentas;
- Deploy de agentes;
- Integração de logs e telemetria;
- Configuração de Regras e Playbooks;
- Ajuste fino;
- Capacitação da Equipe;
- Documentação;
- Monitoração Intensiva;
- Controle de Cronograma;

6.2.7. A CONTRATADA deverá gerenciar o ambiente 24x7x365, quanto à disponibilidade e desempenho dos equipamentos de NGFW;

6.2.8. A CONTRATADA deverá fazer a gestão dos incidentes (criação de alertas, detecção e abertura de chamados);

6.2.9. A CONTRATADA deverá fazer o acompanhamento completo dos incidentes de segurança, performance e disponibilidade;

6.2.10. A CONTRATADA deverá realizar a monitoração de performance e disponibilidade dos ativos de segurança (NGFW);

6.2.11. A CONTRATADA deverá realizar o acionamento por matriz de escalação hierárquica e funcional, para eventos de segurança, performance e disponibilidade.

6.2.12. Possuir processo de escalação funcional, mapeamento e documentado, com os seguintes níveis de atendimento: N1, N2 e N3, conforme melhores práticas descritas pelo ITIL;

6.2.13. A CONTRATADA deverá possuir canal com o fabricante envolvido na solução dos incidentes, bem como ser responsável pela abertura e acompanhamento dos chamados junto ao mesmo;

6.2.14. A CONTRATADA deverá possuir análise técnica documentada pelos Especialistas Seniores do Centro de Operações, antes do envolvimento do fabricante, a fim de garantir o processo de escalação funcional;

6.2.15. A CONTRATADA deverá possuir os processos de gerenciamento de incidente, requisição, eventos, problemas, mudanças, incidentes críticos e atendimento aos usuários VIPs mapeados e documentados de acordo com as melhores práticas descritas pelo ITIL;

6.2.16. Os administradores de tecnologia do CONTRATANTE terão total acesso à plataforma para fins de auditoria, porém a responsabilidade pela operação diária da solução será da CONTRATADA.

6.2.17. A CONTRATADA deverá realizar de forma proativa as ações necessárias para manter o ambiente de segurança da informação do INSTITUTO GNOSIS adequado às melhores práticas do mercado, devendo:

6.2.18. Atualizar os firmwares e/ou softwares das soluções que compõe a solução e das respectivas consoles de gerenciamento;

6.2.19. Propor ajustes e melhorias constantes, de acordo com as melhores práticas dos fabricantes, as mantendo documentadas;

6.2.20. Após aprovação da CONTRATANTE, executar tais ajustes e melhorias nas soluções entregues como parte do objeto deste edital, as mantendo documentadas e acessíveis no portal do cliente;

6.2.21. Sugerir tais ajustes e melhorias nas tecnologias de segurança sob operação da CONTRATANTE;

6.2.22. A CONTRATADA deverá manter uma rotina mensal de avaliação dos processos e práticas em todos as áreas de atuação do escopo deste contrato com o objetivo de avaliar a eficácia, propor melhorias e auxiliar na implementação desses ajustes;

6.2.23. A CONTRATADA deverá manter uma rotina mensal de análise de indicadores internos e pesquisa de mercado com o objetivo de apresentar à contratante um relatório com as inovações tecnológicas e solução que possam aumentar a qualidade e o grau de maturidade da segurança da informação do ambiente tecnológico;

6.2.24. A CONTRATADA deverá atuar quando ocorrer a falha dos controles de segurança ou situação previamente desconhecida e que tenha probabilidade de comprometer as aplicações, sistemas e serviços de TI;

6.2.25. A CONTRATADA deverá gerenciar, monitorar permanentemente e avaliar criticamente as plataformas de NGFW, aplicações e sistemas de segurança do CONTRATANTE;

6.2.26. A CONTRATADA deverá consolidar em manuais de procedimentos e em base de conhecimento todas as soluções adotadas na execução das atividades;

6.2.27. A CONTRATADA deverá elaborar mensalmente relatórios de desempenho, auditoria, operação e vulnerabilidades dos ativos sob sua administração;

6.2.28. A CONTRATADA deverá atuar proativamente na antecipação e identificação de incidentes de segurança, antes mesmo do impacto nos serviços;

6.2.29. A CONTRATADA deverá sugerir novas tecnologias para modernizar o ambiente tecnológico, buscando subsidiar a equipe do CONTRATANTE na gestão de segurança da informação;

6.2.30. A CONTRATADA deverá monitorar e propor soluções aos projetos/atividades em andamento otimizando-os quanto aos requisitos de Segurança da Informação;

6.2.31. A CONTRATADA deverá participar, quando solicitado, de reunião com os gerentes e participantes dos projetos de desenvolvimento e manutenção de sistemas e administração de dados, a fim de prover soluções para projetos/atividades em andamento;

6.2.32. A CONTRATADA deverá participar da implantação de projetos/soluções, substituição e atualização de soluções destinadas à Segurança, que possam impactar nas aplicações monitoradas pelo serviço de Gerenciamento;

6.2.33. A CONTRATADA deverá elaborar relatório detalhado das funcionalidades necessárias de equipamentos e softwares a serem adquiridos, destinados à Segurança da Informação.

6.3. REQUISITOS MÍNIMOS DO PRESTADOR

6.3.1. Possuir SOC próprio, localizados em território nacional

6.3.2. Possuir redundância física do SOC principal, com disposição geográfica de no mínimo 400 Km entre as estruturas.

6.3.3. A contratada deverá comprovar obrigatóriamente que dispõe de uma infraestrutura operacional robusta, equivalente ou superior ao local onde os serviços serão prestados.

6.3.3.1. Dashboard próprio para acompanhamento dos indicadores.

6.3.3.2. Prestador com no mínimo as seguintes certificações obrigatórias: ISO 27001, ISO 9001, ISO 27701, ISO 14001, ISO 45001.

6.3.3.3. Equipe técnica obrigatoriamente certificada em: Certificação ao nível de engenharia do fabricante do Firewalls, ITIL V4 e CISSP.

6.3.3.4. Experiência comprovada em MSS.

6.3.3.5. Adoção de práticas ISO/IEC 27001 e NIST CSF.

6.3.3.6. A empresa vencedora deverá comprovar, possuir certificação nas Normas ISO 27001 e 27701, por serem referências globalmente reconhecidas, que especificam requisitos para estabelecer, implementar, manter e aprimorar de forma contínua um Sistema de Gestão da Segurança da Informação (SGSI) e um Sistema de Gestão de Privacidade da Informação (SGPI), respectivamente;

6.3.3.7. Além das normas acima, a empresa também deverá comprovar, possuir certificação na Norma ISO 9001, que estabelece requisitos para o Sistema de Gestão da Qualidade (SGQ) e ISO 45001, que estabelece políticas e objetivos para Saúde e Segurança do Trabalho;

6.3.3.8. Para comprovação técnico profissional a empresa vencedora deverá apresentar Registro em Carteira de Trabalho e Previdência Social ou Contrato Registrado de pelo menos 1 (um) profissional capacitado com certificação de Engenheiro, pelo fabricante do Next Generation Firewall;

6.3.3.9. A empresa vencedora deverá apresentar Registro em Carteira de Trabalho e Previdência Social ou Contrato Registrado de pelo menos 1 (um) profissional capacitado, com a certificação CISSP e ITIL V4;

6.3.3.10. O profissional certificado oficialmente pela fabricante da solução, ficará responsável, por parte da CONTRATADA, pela elaboração das etapas de execução dos serviços, conforme cronograma de execução, contemplando acompanhamento e suporte técnico remoto e onsite à equipe técnica da CONTRANTE durante toda a vigência do contrato;

6.3.3.11. O Profissional detentor da certificação CISSP, é extremamente importante na Integração da Rede com a Segurança da Informação, em ambiente que define a arquitetura, design, gestão e/ou controles que garantem a segurança de ambientes corporativos, projetando filtros de segurança para evitar invasões e vazamento de informações confidenciais da rede, aplicações e banco de dados. Tal profissional analisa toda a integração da implantação do Backbone em integração com toda a Segurança do Ambiente. A credencial demonstra um nível reconhecido globalmente de competência fornecido pelo CBK® do (ISC)2®. O profissional CISSP tem total habilidade com tópicos críticos em segurança atual, incluindo computação em nuvem, segurança móvel, gerenciamento integrado, segurança no desenvolvimento de aplicativos, segurança em ambientes de rede LAN, MAN e WAN, gestão de riscos, gestão de incidentes, hardening (boas práticas para segurança de ambientes de rede corporativo) e outros, garantindo assim a parte segura do ambiente em produção.

6.3.3.12. A empresa vencedora deverá apresentar carta direcionada ao processo, a fim de comprovar ser parceira oficial do fabricante;

6.3.3.13. Caso não seja possível a emissão da carta, a empresa vencedora deverá comprovar ser parceira oficial através do site do fabricante.

6.3.3.14. Este item é imprescindível para garantir o perfeito atendimento ao fornecimento da solução, assim como a prestação dos serviços de forma qualificada.

6.4. ENTREGÁVEIS E RELATÓRIOS

6.4.1. O contratado deverá fornecer dashboards e relatórios conforme a seguir:

6.4.1.1. Dashboard Operacional (tempo real).

6.4.1.2. Relatório Gerencial Mensal.

6.4.1.3. Relatório Técnico Trimestral.

6.4.1.4. Plano de Melhoria Contínua, propondo ajustes e melhorias constantes, de acordo com as melhores práticas dos fabricantes, e mantendo as documentações atualizadas;.

6.4.1.5. Os relatórios deverão conter gráficos, indicadores e comparativos históricos.

6.4.1.6. Relatórios de Top aplicações, top origens/destinos, tentativas de ataque.

6.4.1.7. Políticas alteradas e justificativas.

6.4.2. NÍVEIS DE SERVIÇO (SLA)

6.4.2.1. Disponibilidade SOC: 99,5% mensal.

6.4.2.2. Disponibilidade dos firewalls: ≥ 99,5%

PLANILHA DE SLA PARA ATENDIMENTO AOS INCIDENTES			
PRIORIDADE	**TIPO**	**INÍCIO DO ATENDIMENTO**	**TEMPO DE RESPOSTA**
Crítica	Incidente que cause parada total no ambiente de produção do Instituto GNOSIS. Impacto muito crítico sobre a rede e acesso aos sistemas por usuários internos e externos	Em menos de ≤ 30 minutos, o técnico da contratada deverá realizar o atendimento inicial de forma remota.	≤ 2 horas após o início do atendimento remoto.
Alta	Incidente intermitente, que não cause parada total no ambiente de produção do Instituto Gnosis. Impacto alto sobre a rede e acesso aos sistemas por usuários internos e externos.	Em menos de ≤ 30 minutos, o técnico da contratada deverá realizar o atendimento inicial de forma remota.	≤ 4 horas após o início do atendimento remoto.
Média	Solicitação de alteração de configurações, criação ou modificação de regras e políticas nas soluções de segurança do Instituto Gnosis. Suporte	Em ≤ 30 minutos, o técnico da contratada deverá realizar o	≤ 8 horas após o início do atendimento remoto.

	com impacto médio no ambiente de produção do Instituto Gnosis.	atendimento inicial de forma remota.	
Baixa	Dúvidas técnicas, aperfeiçoamentos ou esclarecimentos de usuários. Suporte com baixo impacto no ambiente de produção da CEDAE.	Em ≤ 30 minutos, o técnico da contratada deverá realizar o atendimento inicial de forma remota.	≤ 24 horas após o início do atendimento remoto.

6.4.3. SUPORTE E ESCALONAMENTO

6.4.3.1. Canal de suporte 24x7 (telefone 0800, portal, whatsapp e e-mail), com níveis de atendimento:

6.4.3.1.1. N1 – Triagem, N2 – Especialista, N3 – Engenheiro/Fabricante, sendo:

- N1 Operador SOC Monitoramento, registro de incidentes, triagem inicial
- N2 Analista de Segurança Diagnóstico, ajuste de política, mitigação
- N3 Engenheiro de Segurança, Ações corretivas complexas, integração com fabricante, atualização de firmware.

7. OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATADA

A CONTRATADA obriga-se a:

a) Executar o serviço discriminado neste TERMO DE REFERÊNCIA;

b) Disponibilizar mão-de-obra e equipamentos em quantidades necessárias a perfeita execução dos serviços;

c) Garantir confidencialidade das informações.

d) Manter documentação atualizada.

e) Notificar incidentes críticos em até 30 minutos.

f) Registrar logs por 180 dias.

g) Cumprir políticas internas de segurança.

h) Não vincular o pagamento dos salários e demais vantagens de seus empregados ao pagamento das faturas emitidas contra o CONTRATANTE;

i) Nomear encarregados responsáveis pelos serviços, com a missão de garantir o bom andamento dos mesmos, fiscalizando e ministrando a orientação necessária aos executantes dos serviços. Estes encarregados terão a obrigação de reportarem-se, quando houver necessidade, ao responsável pelo acompanhamento dos serviços da Administração e tomar as providências pertinentes para que sejam corrigidas todas as falhas detectadas;

j) Manter todos os equipamentos, ferramental e utensílios necessários a execução dos serviços, em perfeitas condições de uso, devendo os danificados serem substituídos em até 8 (vinte e quatro) horas.

f) Responsabilizar-se por acidentes na execução dos serviços, bem como responder civil e/ou criminalmente, por quaisquer danos causados, diretamente ou indiretamente, à CONTRATANTE ou a terceiros, decorrentes de sua culpa ou dolo e manter a CONTRATANTE a salvo de quaisquer queixas, reivindicações ou reclamações de seus empregados e/ou de terceiros, em decorrência da prestação dos serviços contratados.

g) Informar ao INSTITUTO GNOSIS, sistematicamente, sobre o andamento dos serviços;

h) Cumprir rigorosamente as exigências da legislação tributária, fiscal, trabalhista, previdenciária, assumindo todas as obrigações e encargos legais inerentes e respondendo integralmente pelos ônus resultantes das infrações cometidas;

i) Reservar exclusivamente ao INSTITUTO GNOSIS o direito de utilização e divulgação dos trabalhos elaborados;

j) Preparar e fornecer aos seus empregados, quando aplicável, o formulário PPP (Perfil Profissiográfico Previdenciário), quando exigível, na forma da Lei;

8. OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATANTE:

8.1. Permitir o livre acesso dos funcionários da Contratada, quando em serviço e devidamente identificados, às dependências da unidade.

8.2. Exercer a fiscalização dos serviços por técnicos especialmente designados;

8.3. Indicar, formalmente, o gestor e/ou o fiscal para acompanhamento da execução contratual;

8.4. Expedir Autorização de Serviços;

8.5. Encaminhar a liberação de pagamento das faturas da prestação de serviços aprovadas;

8.6. Disponibilizar instalações sanitárias;

8.7. Efetuar periodicamente a programação dos serviços a serem executados pela Contratada.

8.9. Notificar a CONTRATADA de todas as falhas, erros, imperfeições ou irregularidades que encontrar na prestação dos serviços, dando-lhe, inclusive, prazo para sua correção;

8.10. Fornecer à CONTRATADA, quando aplicável, os subsídios necessários para a elaboração dos laudos técnicos e documentos previstos na legislação previdenciária em vigor;

8.11. Exigir da CONTRATADA, quando aplicável, os laudos técnicos e documentos previstos na legislação previdenciária em vigor (LTCAT, PCMSO, PGR, PPRA e PCMAT);

8.12. Exigir da CONTRATADA, quando aplicável, a declaração, sob as penas da lei, de que as atividades exercidas pelos segurados empregados no presente TERMO CONTRATUAL não estão sujeitas à concessão de aposentadoria especial.

9. ACOMPANHAMENTO DA EXECUÇÃO

9.1. Não obstante a contratada ser a única e exclusiva responsável pela execução de todos os serviços, à contratante é reservado o direito de, sem de qualquer forma restringir a plenitude

dessa responsabilidade, exercer a mais ampla e completa fiscalização dos serviços, diretamente ou por prepostos designados, podendo para isso:

9.2. Solicitar à contratada a substituição de qualquer produto, método e/ou funcionário, cuja atuação considere prejudicial ou inadequado;

9.3. Vetar o prosseguimento normal do serviço, baseados na legislação em vigor;

9.4. Verificar o cumprimento pela contratada das cláusulas do contrato e adotar medidas necessárias quanto à regularização de eventuais transgressões.

9.5. Receber da contratada, documentação pertinente ao serviço ou as questões que envolvam o serviço, sempre que solicitado em prazo máximo de 72 horas.

9.6. Assegurar-se de que o número de empregados alocados ao serviço pela CONTRATADA é suficiente para o bom desempenho dos serviços;

9.7. Permitir o livre acesso dos empregados da CONTRATADA para execução dos serviços;

9.8. Prestar as informações e os esclarecimentos que venham a ser solicitados pela

CONTRATADA;

9.9. Ordenar a imediata retirada do local, bem como a substituição de empregado da contratada que estiver sem uniforme ou crachá, que embaraçar ou dificultar a sua fiscalização ou cuja permanência na área, a seu exclusivo critério, julgar inconveniente;

9.10. Rejeitar, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser corrigidos/refeitos/substituídos no prazo fixado pelo fiscal do contrato, às custas da Contratada, sem prejuízo da aplicação de penalidades.

10. DA QUALIFICAÇÃO TÉCNICA

10.1 Comprovação de que possui instalações e aparelhamentos adequados e disponíveis para a realização dos serviços que são objeto deste Termo de Referência.

10.2 Para comprovação técnico operacional a licitante vencedora deverá apresentar Atestado (s) de Capacidade Técnica, expedido por pessoa (s) jurídica (s) de direito público ou privado, que comprove(m) a aptidão no fornecimento de objeto similar ao descrito neste Termo de Referência, com o seguinte termo de maior relevância:

i. Fornecimento de Next Generation Firewalls, com licenciamento, implantação completa e passagem de conhecimento;

ii. Prestação de serviços de sustentação do ambiente de Segurança da Informação, através de Centro de Operações de Segurança, no formato 24x7x365;

10.3 A empresa vencedora deverá comprovar, possuir certificação nas Normas ISO 27001 e 27701, por serem referências globalmente reconhecidas, que especificam requisitos para estabelecer, implementar, manter e aprimorar de forma contínua um Sistema de Gestão da

Segurança da Informação (SGSI) e um Sistema de Gestão de Privacidade da Informação (SGPI), respectivamente;

10.4 Além das normas acima, a empresa também deverá comprovar, possuir certificação na Norma ISO 9001, que estabelece requisitos para o Sistema de Gestão da Qualidade (SGQ) e ISO 45001, que estabelece políticas e objetivos para Saúde e Segurança do Trabalho;

10.5 Para comprovação técnico profissional a empresa vencedora deverá apresentar Registro em Carteira de Trabalho e Previdência Social ou Contrato Registrado de pelo menos 1 (um) profissional capacitado com certificação de Engenheiro, pelo fabricante do Next Generation Firewall;

10.6 A empresa vencedora deverá apresentar Registro em Carteira de Trabalho e Previdência Social ou Contrato Registrado de pelo menos 1 (um) profissional capacitado, com a certificação CISSP e ITIL V4;

10.7 O profissional certificado oficialmente pela fabricante da solução, ficará responsável, por parte da CONTRATADA, pela elaboração das etapas de execução dos serviços, conforme cronograma de execução, contemplando acompanhamento e suporte técnico remoto e onsite à equipe técnica da CONTRANTE durante toda a vigência do contrato;

10.8 O Profissional detentor da certificação CISSP, é extremamente importante na Integração da Rede com a Segurança da Informação, em ambiente que define a arquitetura, design, gestão e/ou controles que garantem a segurança de ambientes corporativos, projetando filtros de segurança para evitar invasões e vazamento de informações confidenciais da rede, aplicações e banco de dados. Tal profissional analisa toda a integração da implantação do Backbone em integração com toda a Segurança do Ambiente. A credencial demonstra um nível reconhecido globalmente de competência fornecido pelo CBK® do (ISC)2®. O profissional CISSP tem total habilidade com tópicos críticos em segurança atual, incluindo computação em nuvem, segurança móvel, gerenciamento integrado, segurança no desenvolvimento de aplicativos, segurança em ambientes de rede LAN, MAN e WAN, gestão de riscos, gestão de incidentes, hardening (boas práticas para segurança de ambientes de rede corporativo) e outros, garantindo assim a parte segura do ambiente em produção.

10.9 A empresa vencedora deverá apresentar carta direcionada ao processo, a fim de comprovar ser parceira oficial do fabricante;

10.10 Caso não seja possível a emissão da carta, a empresa vencedora deverá comprovar ser parceira oficial através do site do fabricante.

10.11 Este item é imprescindível para garantir o perfeito atendimento ao fornecimento da solução, assim como a prestação dos serviços de forma qualificada.

10.12 Somente serão consideradas as propostas das proponentes cujas atividades estejam contidas no Alvará de Licença e no documento de licenciamento sanitário.

10.13 Plano de Segurança do Trabalho dos empregados, equipamentos e instalações, relativo às atividades a serem desenvolvidas.

10.14 Declaração formal assinada pelo representante legal da empresa, sob as penalidades da lei, de que tem pleno conhecimento das condições e peculiaridades inerentes à natureza dos trabalhos, assumindo total responsabilidade por esse fato e informando que não o utilizaria para quaisquer questionamentos futuros que ensejassem avenças técnicas ou financeiras.

11. HABILITAÇÃO

Apresentação dos seguintes documentos:

Empresa individual: Registro Comercial, devidamente inscrito na Junta Comercial.

Ato Constitutivo: Contrato Social ou Estatuto em vigor devidamente inscrito na Junta Comercial, em se tratando de Sociedades Comerciais por ações, deverá ser apresentado acompanhado de ata de eleição de seus administradores.

Sociedade Civil: Inscrição do ato constitutivo, no caso de sociedades civis, acompanhada de prova de diretoria em exercício.

Decreto de Autorização: Quando tratar-se de empresa ou sociedade estrangeira em funcionamento no País.

- Prova de Inscrição no Cadastro de Pessoas Jurídicas
- Prova de Inscrição no cadastro de contribuintes, ICMS/ISS
- Prova de Regularidade com a Fazenda Federal
- Prova de Regularidade com a Fazenda Estadual
- Prova de Regularidade com a Fazenda Municipal
- Prova de Regularidade com a Procuradoria da Fazenda Nacional
- Prova de Regularidade com a Seguridade Social
- Prova de Regularidade com FGTS
- Prova de regularidade com a justiça do trabalho

12. AVALIAÇÃO DO SERVIÇO PRESTADO

12.1. O INSTITUTO GNOSIS terá o direito de exercer ampla fiscalização sobre a prestação dos serviços objeto do presente TERMO CONTRATUAL, por intermédio de prepostos seus, devidamente credenciados, aos quais deverá a CONTRATADA facilitar o pleno exercício de suas funções, não importando isso em supressão ou mesmo atenuação das responsabilidades desta, por quaisquer erros, falhas ou omissões ocorridas.

§1º - O INSTITUTO GNOSIS credenciará perante a CONTRATADA um representante investido de plenos poderes para, diretamente ou através de auxiliares, exercer a fiscalização geral e total dos serviços ora contratados, tendo como atribuições precípuas as seguintes:

a) Exigir da CONTRATADA a estrita obediência às estipulações deste Termo de Referência, à documentação a ele anexa e à melhor técnica consagrada pelo uso para a execução dos serviços objeto deste Instrumento;

b) Fazer, corrigir, ou refazer trabalhos defeituosos, por conta do INSTITUTO GNOSIS, através de terceiros, debitando à CONTRATADA os gastos daí decorrentes, caso essa última não os refaça ou corrija dentro do prazo determinado pela Fiscalização;

c) Recusar os equipamentos e eventuais serviços de reparo ou manutenção que, a seu critério, estejam em desacordo com as exigências e padrões técnicos estipulados pelo presente TERMO CONTRATUAL;

d) Controlar as condições de trabalho, ajustando com a CONTRATADA as alterações na sequência da execução que forem consideradas convenientes ou necessárias, e controlar tais condições de modo a exigir desta, na ocorrência de atraso nos serviços, a adoção de regime de trabalho diferente;

e) Dar permanente assistência aos serviços, na interpretação e na solução de problemas surgidos;

f) Encaminhar à CONTRATADA as comunicações que se façam necessárias, com relação aos trabalhos de fiscalização e controle dos serviços;

g) Atestar a execução dos serviços referentes às faturas a serem apresentadas;

h) Sustar os serviços, total ou parcialmente, em qualquer tempo, sempre que, a seu critério, considerar esta medida necessária à boa execução dos mesmos, ou à salvaguarda dos interesses do INSTITUTO GNOSIS. Quaisquer ônus provenientes dessa rejeição serão de inteira responsabilidade da CONTRATADA.

§2º- À Fiscalização caberá, ainda, determinar os prazos para cumprimento das exigências feitas.

13. DISPOSIÇÕES GERAIS

13.1. Todos os materiais e equipamentos a serem utilizados na prestação dos serviços, deverão ser fornecidos e distribuídos em quantidades necessárias e suficientes para a execução dos serviços.

14. VIGÊNCIA DO CONTRATO

O prazo de execução do serviço será de 24 meses, contados a partir da assinatura do contrato, com seu término em 31/05/2028, podendo ser prorrogado, por analogia, dentro do limite previsto na Lei nº 14.133/2021. Ou rescindido antes disso, em caso de término do contrato de gestão com a prefeitura de do Rio de Janeiro.

15. VEDAÇÃO DE SUBCONTRATAÇÃO

É vedada a subcontratação total ou parcial da execução do objeto, tendo em vista a contratação por notória especialização. A CONTRATADA também não poderá ceder ou transferir, no todo ou em parte, ainda que em função de reestruturação societária, fusão, cisão e incorporação, os direitos e obrigações decorrentes do contrato com a CONTRATANTE, inclusive, seus créditos.

16. DECLARAÇÃO DE RELAÇÃO EMPREGATÍCIA

É importante que a contratada declare, por escrito, como anexo ao futuro contrato, o seguinte: Que em cumprimento ao disposto no inciso XXXIII do artigo 7º da Constituição Federal, durante a vigência do contrato não serão empregados, em trabalho noturno, perigoso ou insalubre,

menores de dezoito anos, bem como não serão empregados, em qualquer trabalho, menores de dezesseis anos, salvo na condição de aprendiz, a partir de quatorze anos.

17. CRITÉRIOS DE AVALIAÇÃO

a) O valor do objeto deverá ser cotado em moeda corrente nacional, devendo incluir todas as despesas, inclusive impostos e encargos sociais, previdenciários e trabalhistas incidentes em seu escopo de prestação de serviços;

b) **É obrigatória a apresentação de planilha com a formação dos preços, sob pena de desclassificação;**

c) As características do objeto de forma clara e precisa, observadas as especificações constantes nesse Termo de Referência.

d) **Serão desclassificadas propostas com preços irrisórios e/ou inexequíveis**, cabendo ao INSTITUTO GNOSIS à faculdade de promover verificações ou diligências que se fizeram necessárias, objetivando a comparação da regularidade da cotação ofertada;

e) Será julgada vencedora a proposta que ofertar o MENOR PREÇO, devendo o preço proposto incluir todos os custos diretos e indiretos pertinentes, cumprindo todos os requisitos técnicos previstos no Termo de Referência.

f) O envio da proposta será considerado como anuência a todas as Cláusulas do Termo de Referência.

18. PROCEDIMENTOS DE ENVIO DA PROPOSTA

As propostas deverão ser enviadas, para propostas@institutognosis.org.br até **27/03/2026.**

Rio de Janeiro, 26 de fevereiro de 2026.