

**MEMORIAL DESCRITIVO PARA CONTRATAÇÃO DE EMPRESA ESPECIALIZADA  
EM SOLUÇÕES DE CONECTIVIDADE DE REDE E SEGURANÇA DA INFORMAÇÃO**

## SUMÁRIO

|       |  |    |
|-------|--|----|
| 1.    | DEFINIÇÃO DO OBJETO DA CONTRATAÇÃO                 | 4  |
| 2.    | JUSTIFICATIVA DA NECESSIDADE DE CONTRATAÇÃO        | 6  |
| 3.    | PREMISSAS  | 7  |
| 3.1.  | DIAGRAMA ATUAL DA REDE                             | 7  |
| 4.    | JUSTIFICATIVA DA MODALIDADE DE LICITAÇÃO           | 10 |
| 5.    | RESULTADOS E BENEFÍCIOS ESPERADOS:                 | 11 |
| 6.    | APRESENTAÇÃO DA COMPANHIA DE GÁS DO ESPÍRITO SANTO | 12 |
| 7.    | REQUISITOS PARA CONTRATAÇÃO                        | 13 |
| 7.1.  | CAPACITAÇÃO TÉCNICA DA PROPONENTE E DE SUA EQUIPE  | 13 |
| 8.    | CANAIS DE COMUNICAÇÃO                              | 16 |
| 9.    | HORÁRIO DE ATENDIMENTO.                            | 18 |
| 10.   | MODALIDADE DE ATENDIMENTO.                         | 18 |
| 11.   | ACESSIBILIDADE E CONFIDENCIALIDADE.                | 19 |
| 12.   | AQUISIÇÃO DE EQUIPAMENTOS DE PROTEÇÃO DE PERÍMETRO | 20 |
| 12.1. | SERVIÇO DE PROTEÇÃO DE PERÍMETRO                   | 20 |
| 12.2. | IMPLANTAÇÃO DOS SERVIÇOS DE PROTEÇÃO DE PERÍMETRO  | 37 |
| 13.   | RECONFIGURAÇÃO DA REDE DE CONECTIVIDADE            | 40 |
| 14.   | SOLUÇÃO DE PROTEÇÃO AVANÇADA DE ENDPOINT (EPP/EDR) | 42 |
| 15.   | DESENVOLVIMENTO DO TRABALHO                        | 52 |
| 16.   | IMPLANTAÇÃO  | 52 |
| 17.   | PRAZO  | 57 |
| 18.   | RESPONSABILIDADES DA CONTRATADA                    | 57 |
| 19.   | SUBCONTRATAÇÃO                                     | 58 |
| 20.   | PLANILHA DE PREÇOS UNITÁRIOS                       | 59 |
| 21.   | CRITÉRIOS DE MEDIÇÃO                               | 60 |
| 22.   | VISITA TÉCNICA                                     | 60 |
| 23.   | CONDIÇÕES DE PAGAMENTO                             | 60 |
| 24.   | GARANTIA   | 63 |
| 25.   | MECANISMOS FORMAIS DE COMUNICAÇÃO                  | 64 |
| 26.   | ACEITE, ALTERAÇÃO E CANCELAMENTO                   | 64 |
| 27.   | ANEXOS   | 66 |



## **1. DEFINIÇÃO DO OBJETO DA CONTRATAÇÃO**

O objeto da licitação é a contratação de empresa especializada para aquisição, implantação, prestação de suporte técnico e manutenção, garantia e licenciamento de solução de conectividade de rede e segurança.

A solução é composta por:

### **1.1. SERVIÇO DE PROTEÇÃO DE PERÍMETRO:**

Contratação de empresa especializada para fornecimento de Solução de Firewall - Next Generation Firewall (NGFW) - Firewall de Próxima Geração - FortiGate - para segurança da informação de perímetro que possibilite a visibilidade e controle de tráfego e aplicações em camada 7. Firewall de aplicação Web, prevenção contra-ataques e ameaças avançadas e modernas, filtro de dados, SD-WAN e VPN, controle granular de banda de rede, com fornecimento de equipamentos, licenciamento, serviços de planejamento, instalação, configuração, testes, garantia, suporte técnico para as soluções ofertadas, de acordo com as especificações técnicas constantes nesse Edital.

### **1.2. SERVIÇO DE RECONFIGURAÇÃO DOS ATIVOS DE REDE ATUAIS ACCESS POINTS E SWITCHES:**

Contratação de empresa especializada para reconfiguração de equipamentos do parque atual, de forma personalizada para a ES Gás, segmentada por serviço para diminuir o broadcast na rede possibilitando melhor desempenho e segurança sendo elas.

Criação de três redes distintas a seguir: ES Gás-Corp – Acessa a rede corporativa interna, ES Gás-Mobile – Rede para conexões de celulares corporativos e ES Gás-Guest – Rede para conexões de visitante.

### **1.3. SOLUÇÃO DE PROTEÇÃO AVANÇADA DE ENDPOINT (EPP/EDR):**

Visa a implantação de solução de software de Endpoint Protection (EPP/EDR) como solução dedicada a proteção de estações e servidores do CONTRATANTE, realizando

de forma proativa o bloqueio de códigos maliciosos tipo vírus, malware - protegendo os ativos também contra ransomware oferecendo possibilidade de realização de “rollback” de arquivos alvos de código maliciosos, oferecendo ainda suporte à investigação de ataques através da trilha de registros de eventos forense.

#### **1.4. RECONFIGURAÇÃO DO FIREWALL DO SISTEMA SCADA:**

Reconfiguração para adequação à rede de conectividade da Es Gás de Firewall Fortinet 200A do sistema SCADA – integrado na rede da CONTRATANTE.

#### **1.5. Atendimento sob demanda:**

Prestação de atendimento técnico especializado – suporte N3 - sob demanda de acordo com o volume de horas técnicas especificadas por este termo.

## **2. JUSTIFICATIVA DA NECESSIDADE DE CONTRATAÇÃO**

Com a crescente onda de ataques contra as redes corporativas através da rede mundial de computadores, cada vez mais empresas e instituições necessitam implementar e renovar sua Segurança da Informação uma vez que ocorrem ataques diários através da web onde são lançados diversos tipos de vírus, “malwares” e “spams” que se propagam de forma assustadora, causando perdas de dados, sobrecarga nas redes de computadores com lentidão causando inoperância e até mesmo vazamento de dados.

Atualmente a ES Gás dispõe como usuária do serviço em seu contrato de BPO com a empresa VIBRA Energia, uma solução de segurança de rede, que compreende as funcionalidades de “firewall”, filtro de conteúdo, IPS, antivírus de borda e “antispam”, do fabricante Fortinet. A solução atual de conectividade de rede e segurança é composta de equipamentos FortiGate modelo 60E, instalados em suas unidades de negócio.

De forma a manter a padronização do ambiente tecnológico atualmente implantado, que já utiliza as soluções Fortinet, sem histórico de danos ou prejuízos ao ambiente computacional causados por invasões, vírus ou outro tipo de código malicioso, recomenda-se fortemente que a contratação das licenças seja da mesma solução provida pela empresa VIBRA Energia para a ES Gás, de forma que seja assegurada a otimização e padronização do ambiente da Companhia, sendo mais vantajoso em termos de menor complexidade e mitigação dos riscos, uma vez que a troca de uma solução atual de segurança por outra de outro fabricante poderá trazer riscos de inoperância do ambiente, ataques maliciosos ou até mesmo vazamentos de dados. Adicionalmente, ratificamos que haverá uma interconexão por meio de VPN com a rede implantada pela CONTRANTE com a rede de dados da empresa VIBRA com objetivo de possibilitar a transição dos serviços de TI entre os ambientes. Essa interconexão é importante para que a ES Gás continue acessando ainda alguns serviços até o final do contrato de BPO.

Em paralelo a necessidade descrita acima a ES Gás tem como objetivo também a contratação de serviço de implantação de ativos de rede de soluções de segurança da

informação do ambiente da ES Gás, serviço de proteção de Endpoints, serviço de controle de acesso à rede.

Tal contratação viabiliza algumas ações do Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), além de garantir a melhoria e continuidade dos serviços institucionais existentes e que se tornam, a cada dia, mais dependentes da Tecnologia da Informação, de forma que tais serviços continuem operacionais e transparentes aos usuários.

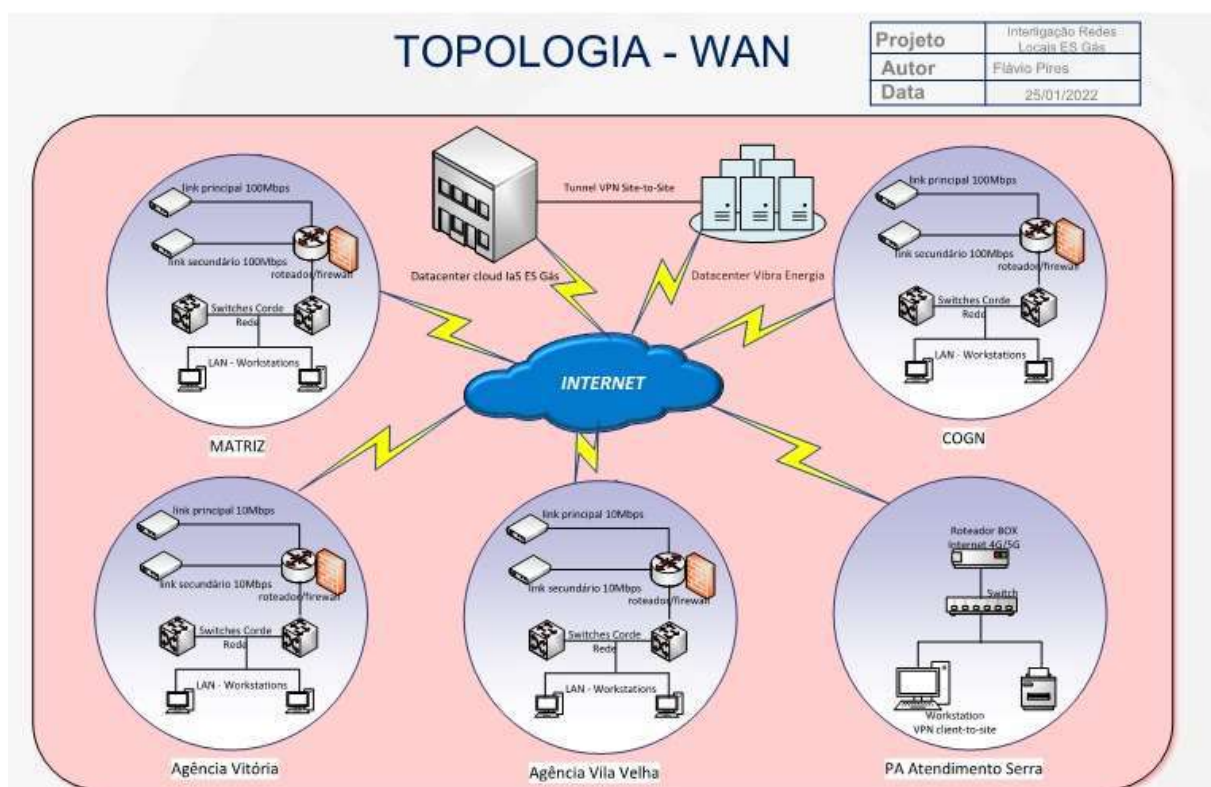
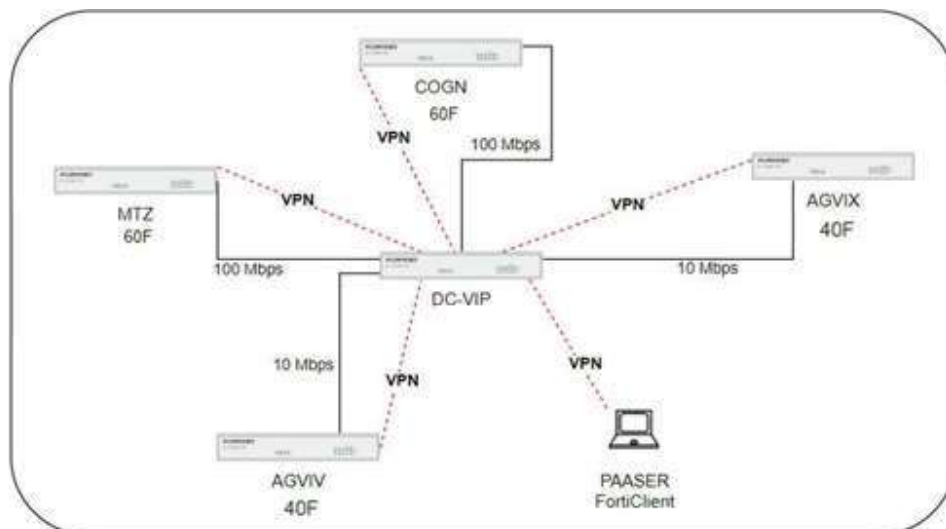
### **3. PREMISSAS**

Para que seja possível acessar o sistema ERP provido pelo Vibra Energia, será necessário a CONTRATADA configurar a conexão da rede SD-WAN que será implantada para a ES Gás (Datacenter) com a rede SD-WAN da empresa Vibra Energia com equipamentos FORTIGATE.

#### **3.1. DIAGRAMA ATUAL DA REDE**

O diagrama de rede da Sede e das Filiais está descrito no ANEXO II - Diagramas de Rede por Localidade.

Desenho Topologia



Link de dados dedicado full duplex

| Filial | Velocidade | Quantidade |
|--------|------------|------------|
|--------|------------|------------|



|            |               |   |
|------------|---------------|---|
| Matriz     | 100Mbps       | 2 |
| COGN       | 100Mbps       | 2 |
| AGVIT      | 10Mbps        | 2 |
| AGVIV      | 10Mbps        | 2 |
| PAASER     | 4G 20GB banda | 1 |
| Datacenter | 200Mbps       | 2 |

#### **4. JUSTIFICATIVA DA MODALIDADE DE LICITAÇÃO**

O objeto caracteriza-se como “serviço comum”, atendendo aos padrões abertos da indústria, sendo compatível no mercado com qualidade e preços, uma vez que seus padrões de desempenho e qualidade ensejam definições objetivas de produtos e serviços de tecnologia da informação e comunicação, com base nas especificações usuais de mercado, e tem como objetivo ser enquadrado na modalidade licitatória denominada Pregão.

##### **4.1. Justificativa para o agrupamento e Indivisibilidade do Objeto:**

Por se tratar de uma solução composta por diversos softwares aplicativos e mais hardware “appliances” (solução unificada), cada um contendo diversas funcionalidades, é fundamental para a garantia da qualidade do serviço, que sejam fornecidos por um mesmo fornecedor, visando otimizar custos e reduzir o tempo de atendimento em caso de problemas a operação assistida deverá ser adjudicado a uma mesma empresa. A adjudicação do objeto desta contratação a empresas distintas, além de aumentar seu custo administrativo, abre margem para que as empresas deixem de prestar o serviço contratado, alegando que a falha de um componente sob sua responsabilidade foi causada por falha de componente sob responsabilidade de outra CONTRATADA. De modo a impedir que esse cenário se torne realidade, comprometendo a disponibilidade de todos os serviços de TIC deste Edital, é fundamental que os itens objeto desta contratação seja adjudicado a uma única licitante.

## **5. RESULTADOS E BENEFÍCIOS ESPERADOS:**

Com a contratação das soluções de conectividade e segurança descritas neste objeto, almeja-se além da implantação dos hardwares (appliances) dos Firewalls entre o datacenter em nuvem contratado pela ES Gás, suas filiais e centros de operação, reconfigurar os dispositivos de rede atuais (switches, access points, firewalls e roteadores), alcançar um maior controle de segurança da informação e proteção de dados (Endpoints EPP/EDR) no âmbito da ES Gás e viabilizar a continuidade do negócio através da redução de spams, vírus, malwares, sistemas desatualizados, dentre outros problemas e ainda alcançar os seguintes pontos:

- Aumento da segurança da informação com a priorização e desenvolvimento de uma estratégia para lidar com aqueles mais críticos;
- Informações da empresa protegidas sem riscos de ataques e invasões;
- Análise de logs de segurança, e antecipação de novas ameaças;
- Alta disponibilidade de links, com redundância e contingência automática em tempo real;
- Controle de acesso ao ambiente de rede de forma geral;
- Controle de regras de acesso;
- Controle da Web e Aplicativos;
- Controle de wireless;
- Gerenciamento de Firmware;
- Ferramenta de Script / Automação de ações.
- Reconfiguração dos Firewalls do sistema Scada

## 6. APRESENTAÇÃO DA COMPANHIA DE GÁS DO ESPÍRITO SANTO

A Companhia de Gás do Espírito Santo (ES Gás), fundada em 22 de julho de 2019, tem por objeto a exploração dos serviços públicos de distribuição de gás canalizado no Estado do Espírito Santo.

Constituída pela Lei Ordinária N° 10.955/2018, a ES Gás é uma empresa de economia mista em que o Estado do Espírito Santo detém 51% do capital votante, tendo como sócia a BR Distribuidora, com os demais 49%. No Espírito Santo, é a concessionária responsável pela distribuição do gás natural canalizado, regulada pelo órgão estadual ARSP (Agência de Regulação de Serviços Públicos do Espírito Santo). Atua nos segmentos residencial, comercial, industrial, automotivo, de climatização e cogeração e termoelétrico, totalizando mais de 60 mil unidades consumidoras.

Apresentamos no quadro abaixo os principais dados referentes à concessão para distribuição de gás natural no Estado do ES:

|   |                              |
|---|------------------------------|
| Rede de distribuição em operação (maio/2019): | 451 Km                       |
| Número de Município atendidos:                | 13 municípios                |
| Quantidade de Usuários de GN (maio/2019):     | Industrial: 46 usuários      |
|   | Térmico: 1 usuário           |
|   | Veicular: 33 usuários        |
|   | Comercial: 608 usuários      |
|   | Residencial: 56.794 usuários |
| Volume total de gás distribuído:              | 2016: 2,6 milhões m³/dia     |
|   | 2017: 2,7 milhões m³/dia     |
|   | 2018: 2,8 milhões m³/dia     |

## **7. REQUISITOS PARA CONTRATAÇÃO**

### **7.1. CAPACITAÇÃO TÉCNICA DA PROPONENTE E DE SUA EQUIPE**

**7.1.** A LICITANTE deverá comprovar que possui experiência similar e compatível em características e quantitativos com o objeto deste Memorial Descritivo, devendo apresentar atestado de capacidade técnica em nome da empresa licitante ou de empresa do mesmo grupo empresarial, suas subsidiárias ou controladas, expedido por pessoa jurídica de direito público ou privado, que comprove a aptidão para a prestação dos serviços em características, quantidades e prazos compatíveis com o objeto desta licitação, ou com o item pertinente, mediante a apresentação de atestado(s) fornecido(s) por pessoas jurídicas de direito público ou privado.

**7.2.** Comprovação de ser um Parceiro designado pelos fabricantes de hardware e softwares que serão ofertados pela contratada como um provedor de serviços de suporte técnico e/ou Manutenção de Equipamentos e demais serviços nomeados a este mesmo fabricante. Deverá estar apta a prestar os serviços descritos pelo fabricante e estar coberto e regida por planos de acompanhamentos periódicos. Além de ser necessário a comprovação de que está apta a realizar a implementação e execução técnica por ele (fabricante) definido. Comprovar assim os termos e padrões definidos e aplicáveis.

**7.3.** Além de comprovar que mantém plano regular formalizado regido por acompanhamentos regulares de modo a ser monitorado o seu desempenho na consecução por este mesmo fabricante. Os itens aqui mencionados deverão ser regidos por acordo firmado e formalizado entre a CONTRATADA e o fabricante.

**7.4.** A confirmação dos itens se dará por documento assinado pelo fabricante, ou por consulta aos sítios do fabricante, contudo importa-se que a documentação apresentada demonstre e comprove a atenção integral aos itens pontuados e exigidos.

- 7.5.** A tomar pela criticidade dos equipamentos envolvidos e sua finalidade este requisito será de sobremaneira decisivo e critério de legibilidade, qualificação e classificação dos proponentes.
- 7.6.** A confirmação dos itens se dará por documento assinado pelo fabricante, ou por consulta aos sítios do fabricante, contudo importa-se que a documentação apresentada demonstre e comprove a atenção integralmente aos itens pontuados e exigidos.
- 7.7.** Apresentação de atestado de capacidade técnica emitidos por pessoa jurídica pública ou privada referente a contratos de objetos similares aos especificados no Termo de Referência, em características compatíveis com o objeto da contratação.
- 7.8.** O(s) Atestado(s) de Capacidade Técnica deverá(ão) ser emitido(s) em papel timbrado do atestante, contendo as seguintes informações: nome da empresa, razão social, CNPJ, nome completo do responsável pelas informações, período de realização do serviço, objeto/escopo contratual e manifestação quanto à qualidade e/ou satisfação do fornecimento. O objeto deverá ser compatível em características e prazos com os serviços a serem contratados.
- 7.9.** As comprovações solicitadas nos atestados supracitados visam garantir que a LICITANTE possua capacidade e porte suficiente para atender ao objeto desta contratação durante o prazo contratual.
- 7.10.** O Atestado/declaração de parceria e/ou representação comercial do fabricante deve estar vigente. Não havendo data de validade discriminada no documento, este deve ter sido emitido/assinado há no máximo 01 (um) ano.
- 7.11.** Como condição pré-contratual, a licitante vencedora deverá apresentar, no prazo máximo de 10 (dez) dias úteis contados da notificação da homologação da licitação, uma relação contendo a equipe de profissionais que serão colocados à disposição da execução dos serviços indicados neste Memorial Descritivo, bem como a comprovação da sua experiência profissional e certificações. No momento da habilitação, a licitante deverá apresentar declaração de que está ciente desta obrigatoriedade.

**7.12.** Não existe restrição ou limite para acúmulo de perfis em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos em cada grupo de atuação no objeto do contrato. Deverá ser de responsabilidade da CONTRATADA dimensionar o número de profissionais adequado para entrega de tal serviço, sem que haja impacto no acordo de nível de serviço formalizado com a CONTRATANTE.

**7.13.** Além das certificações especificadas a seguir, para todos os cargos a seguir serão exigidos: Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação. Para as demais graduações, deverá ser acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC);

**7.14.** A equipe-chave deverá ser composta os perfis profissionais, considerando as quantidades e qualificações a seguir elencadas:

7.14.1. 01 (um) Gerente de Projetos: Deve possuir certificação Project Management Professional (PMP®) do Project Management Institute (PMI®). Deve possuir no mínimo 03 (três) anos de experiência em gestão de projetos e pelo menos 01 (uma) experiência na gestão de projetos dos serviços a serem executados, conforme solicitado;

7.14.2. 01 (um) Analista de Segurança Perímetro deve possuir certificação ISFS (Information Security Foundation on ISO 27001) e Conhecimento avançado em segurança da informação, com experiência em operação, sustentação e suporte a ambientes similares ao supracitado.

7.14.3. (um) Analista de Segurança WAF deve possuir certificação CompTIA Security+; **Certificação sobre a plataforma/solução utilizada** e Conhecimento avançado em segurança da informação, com experiência em operação, sustentação e suporte a ambientes similares ao supracitado.

7.14.4. 01(um) Analista de Segurança Endpoint **deve possuir certificação sobre a plataforma/solução utilizada** e Conhecimento avançado em segurança da informação, com experiência em operação, sustentação e suporte a ambientes similares ao supracitado. Deverá possuir certificação homologada pelo fabricante da solução.

**7.15.** Os profissionais apresentados para a Habilitação Técnica podem ser trocados por outros após a contratação da empresa vencedora, desde que possuam experiência e certificação igual ou superior à apresentada no Pregão.

**7.16.** A comprovação de vinculação do profissional ao licitante será efetuada através da apresentação de cópia autenticada da CTPS, se empregado, contrato de prestação de serviço, se não empregado e, no caso de Sócio, mediante apresentação do contrato social em vigor, acompanhado das respectivas alterações, se houver.

**7.17.** Todas as informações prestadas pelos LICITANTES poderão ser objeto de diligência para fins de averiguação da veracidade e, havendo inconsistência ou discordância das informações prestadas, bem como, se constatada má-fé ou dolo, a LICITANTE será imediatamente inabilitada e estará sujeita a aplicação das penalidades cabíveis.

## **8. CANAIS DE COMUNICAÇÃO**

Para abertura de solicitações a CONTRATADA deverá disponibilizar os seguintes canais de comunicação, a saber:

| item | Grupo de Tecnologia  | Classificação |
|------|--|---------------|
| 1    | Telefone e E-mail para contato direto com a equipe de suporte especializado da CONTRATADA. | Tipo 1        |



|   |   |        |
|---|---|--------|
| 2 | Sistema de ITSM do inglês <i>Information Technology Service Management</i> (Gerenciamento de Serviços de TI). | Tipo 2 |
|---|---|--------|

Tabela 1 - TABELA 1 - TIPOS DE CANAIS DE COMUNICAÇÃO

Independente do canal de comunicação utilizado pelo CONTRATANTE, as solicitações devem ser convergidas, atualizadas, resolvidas e concentradas em um único sistema de ITSM do inglês *Information Technology Service Management* (Gerenciamento de Serviços de TI). Ou seja, imaginando que o CONTRATANTE realize a abertura de uma nova solicitação de serviço via linha telefônica, no segundo que segue a sua solicitação, a mesma deve constar no sistema de ITSM, assim também deve se proceder com a utilização do canal de comunicação do tipo 2: via e-mail.

Sobre o canal de comunicação do tipo 1: via linha telefonia, tais ligações obrigatoriamente devem ser atendidas e/ou recepcionadas por uma interface humana, não sendo permitido utilização de URA (Unidade de Resposta Audível), e/ou qualquer usufruto de atendimento eletrônico.

## **9. HORÁRIO DE ATENDIMENTO.**

Os **SERVIÇOS DE SUPORTE DE SEGURANÇA ESPECIALIZADOS**, devem obrigatoriamente serem ofertados, e estarem acessíveis ao CONTRATANTE em regime de 24 (vinte quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano, durante às atividades pertinentes e dentro do prazo de vigência do contrato.

## **10. MODALIDADE DE ATENDIMENTO.**

- 10.1.** A modalidade principal de atendimento será do tipo presencial, ou seja, a ser realizada nas dependências da CONTRANTE, obrigatoriamente obedecendo os critérios estabelecidos para execução dele, no presente termo de referência.
- 10.2.** A modalidade de atendimento poderá ser remota somente após os devidos critérios de segurança tiverem sido implementados e a conectividade for estabelecida por meio de VPN.
- 10.3.** Para o atendimento do suporte especializado sob demanda, todo acesso ao ambiente da Es Gás poderá ser remoto ou presencial.

## **11. ACESSIBILIDADE E CONFIDENCIALIDADE.**

A CONTRATADA deve assinar e entregar ao CONTRATANTE na data de reunião de início do contrato termo de confidencialidade e sigilo, conforme modelo vigente utilizado pela CONTRATANTE. Esse documento estabelece as condições para a prestação dos serviços acerca do sigilo das informações custodiadas, do acesso restrito das informações aos técnicos designados no projeto e da propriedade intelectual de todos os produtos e conhecimento advindos da execução.

Além disso, o termo de confidencialidade e sigilo deve ser assinado por todos os funcionários que venham executar serviços, diretamente ou indiretamente, no âmbito do contrato, sendo que o CONTRATANTE pode solicitar, a qualquer momento, a comprovação dessa obrigação. O respectivo termo deve ser entregue antes do início das atividades.

Por outro lado, a CONTRATADA deve revogar todas as credenciais relacionadas a soluções de responsabilidade da CONTRATADA, empregadas na prestação de serviços ao CONTRATANTE, bem como solicitar a revogação destas ao CONTRATANTE, para soluções de responsabilidade da CONTRATADA, no mesmo dia do encerramento das atividades.

A CONTRATADA deverá assumir integral obrigação de sigilo e confidencialidade em relação às informações a que tiver acesso e a todo material produzido, ficando vedada por qualquer modo a sua reprodução, cópia, comercialização, distribuição, publicação e ou divulgação, sob pena de responsabilização.

A CONTRATADA não poderá repassar a terceiros, em nenhuma hipótese qualquer informação sobre a arquitetura e/ou documentação; assim como dados e/ou metadados trafegados; produtos desenvolvidos e entregues, ficando responsável juntamente com a ES Gás por manter a segurança da informação relativa aos dados e códigos durante a execução das atividades e em período posterior ao término da execução dos serviços.

Tais exigências visam proteger o CONTRATANTE contra o uso indevido de informações sob sua custódia por parte de profissional da CONTRATADA, assim como estão em conformidade com boas práticas de gestão e governança de TI.

## **12. AQUISIÇÃO DE EQUIPAMENTOS DE PROTEÇÃO DE PERÍMETRO**

Os equipamentos objetos deste edital deverão ser adquiridos conforme as seguintes especificações:

### **12.1. SERVIÇO DE PROTEÇÃO DE PERÍMETRO**

A CONTRATADA deverá prover os equipamentos Appliance da solução de Firewall NGFW - Next Generation Firewall com as características descritas na tabela 1, e a configuração do firewall provido pela ES Gás em ambiente de Datacenter em Cloud descrito na Tabela 3;

O firewall provido pela ES Gás, instalado no Datacenter Cloud, será o equipamento principal e deverá ser configurado pela CONTRATADA em conformidade com os requisitos de segurança descritos nesse edital.

**Tabela 1 – Tipos de Appliances**

| Tipo         | Descrição   | Quantidade |
|--------------|---|------------|
| I            | Aquisição de Appliance do Firewall Projetado– Modelo: Next Generation Firewall - Secure SD-WAN FortiGate® 60F Series  | 2          |
| II           | Aquisição de Appliance do Firewall Projetado – Modelo: Next Generation Firewall - Secure SD-WAN FortiGate® 40F Series | 2          |
| <b>Total</b> |   | <b>4</b>   |

**Tabela 2 – Localidades de Instalação dos Appliances**

As instalações serão realizadas no Municípios de Vitória/ES, Vila Velha/ES e Serra/ES.

| Site | Unidade   | Endereço  | Usuários | Equip. Tipo I | Equip. Tipo II |
|------|---|---|----------|---------------|----------------|
| 1    | ADMSE – Administrativo Sede                           | Av Nossa Senhora da Penha, 1688, Edif Edivit Bloco 1, Andar 2, Barro Vermelho, <b>VITÓRIA/ES</b> , Cep 29.057-550 | 60       | 1             | 0              |
| 2    | COGNC – Centro de Operações de Gás Natural Canalizado | R Santos Dumont, s/n, Quadra 72, Lote 11 a 20, Rosario de Fatima, <b>SERRA/ES</b> , Cep 29.161-144                | 40       | 1             | 0              |

|                                      |   |   |    |          |          |
|--------------------------------------|---|---|----|----------|----------|
| 3                                    | AGVIT – Agência de Atendimento – Vitória      | Av Nossa Senhora da Penha, 356, Loja 30 e 31, Edif Boulevard da Praia, <b>VITÓRIA/ES</b> , Cep 29.055-131   | 05 | 0        | 1        |
| 4                                    | AGVIV – Agência de Atendimento – Vila Velha   | R Humberto Serrano, 99, Loja 1 Edif 1 Atlantico Sul, Praia da Costa, <b>VILA VELHA/ES</b> , Cep 29.101-461  | 05 | 0        | 1        |
| 5                                    | PAASE – Posto Avançado de Atendimento - Serra | Av Primeira Avenida, 231, Quiosque Piso 2, Parque Residencial Laranjeiras, <b>SERRA/ES</b> , Cep 29.165-155 | 1  | 0        | 0        |
| <b>Total por Tipo de Equipamento</b> |   |   |    | <b>2</b> | <b>3</b> |

**Tabela 3 – Tipo de Firewall Datacenter Cloud (IAAS)**

| <b>Tipo</b>  | <b>Descrição</b>   | <b>Quantidade</b> |
|--------------|--|-------------------|
| I            | Configuração do Firewall Projetado (Appliance ou Virtual) – Modelo: Next Generation Firewall - Secure SD-WAN equivalente as configurações de um FortiGate® 200F Series ou superior. Fornecido pelo Datacenter. | 1                 |
| <b>Total</b> |  | <b>1</b>          |

#### **12.1.1. CARACTÉRISTICAS DO HARDWARE TIPO 1 (FW01) 60f**

- 12.1.1.1. Deve possuir licença de software do tipo UTP (Unifed Threat Protection), o licenciamento se dará pelo período de 24 meses;
- 12.1.1.2. Devem ser liberadas, no mínimo, as seguintes licenças: Forticare, FortiGuard App Control Service, FortiGuard IPS Service, FortiGuard Advanced Malware Protection AMP, FortiGuard Web Filtering Service, FortiGuard Antispam Service;
- 12.1.1.3. Deve suportar performance de Firewall de 10 Gbps;
- 12.1.1.4. Deve suportar a performance considerando as funcionalidades de Next Generation firewall de 700 Mb;
- 12.1.1.5. Deve suportar a performance de inspeção SSL 600 Mbps;
- 12.1.1.6. Deve suportar performance de VPN de 6 Gbps;
- 12.1.1.7. Deve suportar 200 túneis de VPN simultâneos;
- 12.1.1.8. Deve suportar 35.000 novas sessões TCP por segundo;
- 12.1.1.9. O dispositivo deve conter o módulo de IPS, Anti-Malware, Filtro de Conteúdo, inclusos;
- 12.1.1.10. Devera suportar nativamente 200 clientes VPN autenticados em SSL;
- 12.1.1.11. Deve ser licenciado para suportar 200 tuneis de VPN IPSec;

- 12.1.1.12. Deve ter licenças habilitadas para funcionalidade SDWAN;
- 12.1.1.13. Deve possuir as seguintes quantidades de interfaces de rede abaixo:
  - 12.1.1.13.1. Deve possuir, no mínimo, 3 portas GE RJ45;
  - 12.1.1.13.2. Deve possuir, no mínimo, 1 portas USB;
  - 12.1.1.13.3. Deve possuir, no mínimo, 1 interface para console com conector RJ- 45.

#### **12.1.2. CARACTERÍSTICAS DO HARDWARE TIPO 2 (FW02) 40f**

- 12.1.2.1. Deve possuir licença de software do tipo UTP (Unified Threat Protection), o licenciamento se dará pelo período de 24 meses;
- 12.1.2.2. Devem ser liberadas, no mínimo, as seguintes licenças: Forticare, FortiGuard App Control Service, FortiGuard IPS Service, FortiGuard Advanced Malware Protection AMP, FortiGuard Web Filtering Service, FortiGuard Antispam Service;
- 12.1.2.3. Para este item, deve ser fornecido um cluster com, no mínimo, 2 (dois) Firewalls, para cada unidade fornecida;
- 12.1.2.4. Deve suportar performance de Firewall de 5 Gbps;
- 12.1.2.5. Deve suportar a performance considerando as funcionalidades de Next Generation firewall de 600 Mb;
- 12.1.2.6. Deve suportar a performance de inspeção SSL 300 Mbps;
- 12.1.2.7. Deve suportar 200 túneis de VPN simultâneos;
- 12.1.2.8. Deve suportar 35.000 novas sessões TCP por segundo;
- 12.1.2.9. O dispositivo deve conter o módulo de IPS, Anti-Malware, Filtro de Conteúdo, inclusos;
- 12.1.2.10. Devera suportar nativamente 200 clientes VPN autenticados em SSL;
- 12.1.2.11. Deve ser licenciado para suportar 200 tuneis de VPN IPSec;
- 12.1.2.12. Deve ter licenças habilitadas para funcionalidade SDWAN;

12.1.2.13. Deve possuir as seguintes quantidades de interfaces de rede abaixo:

12.1.2.13.1. Deve possuir, no mínimo, 3 portas GE RJ45;

12.1.2.13.2. Deve possuir, no mínimo, 1 portas USB;

12.1.2.13.3. Deve possuir, no mínimo, 1 interface para console com conector RJ- 45.

### **12.1.3. ESPECIFICAÇÕES DE LICENÇAS NECESSÁRIAS**

12.1.3.1. As licenças contratadas para os firewalls fornecidos deverão ativar as funcionalidades do pacote FortiGuard Unified Threat Protection(UTP) da Fortinet que inclui:

12.1.3.1.1. Devem ser liberadas, no mínimo, as seguintes licenças: Forticare, FortiGuard App Control Service, FortiGuard IPS Service, FortiGuard Advanced Malware Protection AMP, FortiGuard Web Filtering Service, FortiGuard Antispam Service;

12.1.3.1.2. Suporte abrangente 24 horas por dia, 7 dias por semana;

12.1.3.1.3. Substituição avançada de hardware (NBD);

12.1.3.1.4. Atualizações gerais e de firmware e o pacote de serviços UTP (controle de aplicativos, IDS/IPS, AV, IP/domínio de botnet, serviço de malware móvel, filtragem da Web, antispam).

12.1.3.1.5. Proteção contra ameaças em toda a superfície de ataque digital, fornecendo defesa líder do setor contra ataques sofisticados.

12.1.3.1.6. Cobertura para ataques baseados na Web e por e-mail.

12.1.3.2. As licenças contratadas para o Gerenciamento Centralizado (item 12.1.12) deverão contemplar:

12.1.3.2.1. FortiManager licenciado para gerenciar até 10 devices (licenciamento mínimo);

12.1.3.2.2. O FortiAnalyzer licenciado para no mínimo 25GB/log.

### **12.1.4. SOBRE AS FERRAMENTAS A SEREM UTILIZADAS**

- 12.1.4.1. Todos os produtos ofertados devem ser novos, sem uso anterior e, estar em linha de produção e comercialização pelo fabricante deles no momento da proposta, não devendo haver anúncio de "fim de produção" (EOL - End-of-Life) nem de apresentação do fim de comercialização (EOS - End-of-Sale) até esta data;
- 12.1.4.2. Devem ser fornecidas todas as licenças de hardware e software necessárias à implantação das funcionalidades especificadas a serem implementadas;
- 12.1.4.3. Solução deve consistir em plataforma de proteção de rede baseada em hardware dedicado, em um equipamento do tipo "appliance", possuindo sistema operacional próprio para a execução das funções especificadas. Não será aceito equipamento do tipo PC (Personal Computer) ou Servidor, com sistema operacional de uso genérico, adaptado para a função aqui especificada;
- 12.1.4.4. Todos os produtos ofertados devem ser entregues com a última versão de software e/ou firmware disponível no momento da aquisição;
- 12.1.4.5. Deve possuir 1 (uma) interface para console de acesso ao equipamento com conector RJ-45, USB e/ou serial;
- 12.1.4.6. Deve operar na faixa de temperatura de 0 a 40°C e, humidade relativa entre 10 e 90%;
- 12.1.4.7. Característica De Roteamento
- 12.1.4.8. Suporte a 4096 (quatro mil e noventa e seis) VLANs, conforme padrão IEEE 802.1q;
- 12.1.4.9. Agregação de links, conforme padrão IEEE 802.3ad;
- 12.1.4.10. Deve suportar proxy ARP e entradas estáticas de ARP definidos em endereço ipv4 e ipv6;
- 12.1.4.11. Policy Routing permitindo que o roteamento seja baseado tanto no endereço de origem como no endereço de destino.
- 12.1.4.12. Deve suportar DHCP Relay;
- 12.1.4.13. Possuir proteção contra anti-spoofing;



- 12.1.4.14. Deve possuir roteamento estático IPv4 e, no mínimo, os seguintes protocolos de roteamento dinâmico: BGP e OSPFv2;
- 12.1.4.15. Deve possuir ECMP (Equal-Cost Multi-Path) suportando até 8 caminhos entre origem e destino;
- 12.1.4.16. Deve possuir roteamento estático IPv6 e Multicast, no mínimo, o protocolo de roteamento dinâmico OSPFv3;
- 12.1.4.17. Deve suportar pelo menos os seguintes serviços em ipv4 e ipv6:
  - Dual stack IPv4/IPv6 e as seguintes aplicações:
  - 12.1.4.17.1. NDP;
  - 12.1.4.17.2. ICMPv6;
  - 12.1.4.17.3. DNSv6;
  - 12.1.4.17.4. NTP;
  - 12.1.4.17.5. Syslog;

#### **12.1.5. Funcionalidades de Segurança**

- 12.1.5.1. Deve possuir tecnologia Stateful Inspection;
- 12.1.5.2. Deve possuir políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
- 12.1.5.3. Deve possuir políticas baseadas em localização geográfica;
- 12.1.5.4. Deve possuir suporte os seguintes tipos de negação de tráfego nas políticas de firewall:
  - 12.1.5.5. Drop sem notificação do bloqueio a origem;
  - 12.1.5.6. Drop com notificação do bloqueio a origem (TCP reset ou mensagem de erro ICMP);
- 12.1.5.7. Blacklist (bloqueio de conexões por determinado período) local e distribuído com base em eventos de tráfego analisados pelos firewalls gerenciados;
- 12.1.5.8. Deve possuir controle de acesso com suporte a aplicações, serviços e protocolos pré-definidos;

- 12.1.5.9. Deve possuir regras a serem aplicadas em intervalos regulares de tempo, sendo determinados dias da semana e horários e determinados dias e horários do mês;
- 12.1.5.10. Deve possuir integração com diretórios LDAP, RADIUS, TACACS+ e Microsoft Active Directory para a autenticação de usuários;
- 12.1.5.11. Deve possuir capacidade de autenticação de administradores usando base interna, RADIUS, TACACS+ e LDAP;
- 12.1.5.12. Deve possuir capacidade de autenticar administradores com uso de certificados X.509;
- 12.1.5.13. 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. Deve possibilitar o uso deste recurso com segundo fator de autenticação através de certificados;
- 12.1.5.14. Deve possuir suporte a controle de aplicações do tipo multimídia, tais como, voz sobre IP, áudio e vídeo streaming;
- 12.1.5.15. Deve suportar os seguintes tipos de NAT:
  - 12.1.5.15.1. NAT estático: 1-para-1,
  - 12.1.5.15.2. Tradução de porta (PAT) N-para-1;
  - 12.1.5.15.3. Suportar NAT de Origem
- 12.1.5.16. Deve suportar definir o tráfego de saída baseado em aplicação web 2.0 suportando no mínimo as seguintes aplicações: Facebook, Twitter, Youtube, Salesforce, Office365 e Netflix.

#### **12.1.6. Alta Disponibilidade (HA)**

- 12.1.6.1. A solução deve ser escalável para no mínimo 2 (dois) e no máximo 8 (oito) membros em um único cluster no modo ativo/ativo ou ativo/Stand-by, ou seja, sendo possível a divisão de cargas entre todos os appliances, permitindo o investimento gradual ao longo do tempo,

- 12.1.6.2. A solução deve permitir o agrupamento de múltiplos equipamentos (cluster) que funcionem como um único equipamento, compartilhando única configuração de política de segurança entre os componentes;
- 12.1.6.3. O cluster deve suportar o uso conjunto de até 8 equipamentos simultâneos.
- 12.1.6.4. Deve garantir que todas as configurações sejam replicadas entre os componentes do cluster, garantindo a continuidade das conexões mesmo se um dos equipamentos do cluster estiver indisponível;
- 12.1.6.5. Deve possuir mecanismos de teste de link com o objetivo de fazer com que appliances do cluster fiquem offline se houver falha de link associado aquele appliance;
- 12.1.6.6. Deve possuir funcionalidade de ativação do cluster mesmo em versões de softwares diferentes por equipamento.

#### **12.1.7. Funcionalidades de Controle e Inspeção de Aplicações**

- 12.1.7.1. Deve suportar a liberação e o bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;
- 12.1.7.2. Deve possuir pelo menos 4.000 (quatro mil) aplicações diferentes, para os seguintes perfis de tráfego mínimo: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, VoIP, áudio, vídeo, proxy, serviços de mensagens instantâneas, compartilhamento de arquivos e e-mail;
- 12.1.7.3. Deve identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas avançadas de evasão como por exemplo divisão do malware em partes, enviá-los fora de ordem, via diferentes canais de comunicação;
- 12.1.7.4. Deve analisar tráfego criptografado SSL, possibilitando a leitura de payload para checagem de assinaturas das aplicações de forma granular;

- 12.1.7.5. Deve reconhecer e bloquear tráfego de rede do tipo ToR mesmo depois da primeira conexão aos proxies.
- 12.1.7.6. Deve modificar ao usuário quando uma aplicação for bloqueada;
- 12.1.7.7. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;
- 12.1.7.8. Deve identificar a diferença de tráfegos de Instant Messaging possuindo granularidade de controle e políticas;
- 12.1.7.9. Deve ser capaz de bloquear funcionalidades específicas de páginas Web ou aplicações, para no mínimo: Facebook, Facebook-chat, Facebook-Apps, Facebook-Live, Facebook-Plugins, Google, Google-Play, GoToMeeting, Zoom, Apple-FaceTime, Apple-Game-Center, Apple-iCloud (Adicionar aplicativos mais utilizados no cliente);
- 12.1.7.10. Deve possuir integração com Microsoft Active Directory (AD) para identificação de usuários e grupos, permitindo granularidade de controle e políticas baseadas em usuários e grupos de usuários;
- 12.1.7.11. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle do usuário e de grupo de usuários que estão utilizando as aplicações, através da integração com serviços de diretório Microsoft Active Directory (AD);

#### **12.1.8. Funcionalidades de IPS (Intrusion Prevention System)**

- 12.1.8.1. Deve suportar o funcionamento no modo IPS no mesmo appliance;
- 12.1.8.2. Deve suportar implementação em camada 2 e em camada 3;
- 12.1.8.3. Deve inspecionar o payload de pacote de dados com o objetivo de detectar aplicações conhecidas pelo fabricante independente de porta e protocolo;
- 12.1.8.4. As funcionalidades de IPS e Firewall devem ser implementadas em um mesmo appliance com sua comunicação entre as funcionalidades de maneira interna, sem a necessidade de uso de qualquer interface externa;

- 12.1.8.5. Deve possuir o bloqueio de vulnerabilidades;
- 12.1.8.6. Filtrar vulnerabilidades por referências do OSVDB, MS, BID e CVE;
- 12.1.8.7. Deve possuir o bloqueio de exploits conhecidos;
- 12.1.8.8. Deve possuir proteção contra-ataques de negação de serviços;
- 12.1.8.9. Deve incluir mecanismos para detecção de botnets tais como:
  - 12.1.8.9.1. Ghost
  - 12.1.8.9.2. njRAT
  - 12.1.8.9.3. PoisonIvy
  - 12.1.8.9.4. Pramro
  - 12.1.8.9.5. Pushdo
  - 12.1.8.9.6. Ramnit
- 12.1.8.10. Deve reconhecer pelo menos os seguintes protocolos: Ethernet, H.323, GRE, IPv4, IPv6, ICMP, IPv4 encapsulation, IPv6 encapsulation, UDP, TCP, DNS, FTP, HTTP, HTTPS, IMAP, IMAPS, MGCP, MSRPC, NetBIOS Datagram, OPC UA Binary, OPC UA, Oracle, MySQL, POP3, POP3S, SIP, SRP, SSH, TELNET, WINS, X11, RTSP, SMTP, SunRPC, NNTP, SCCP, SMB, SMB2 e TFTP.
- 12.1.8.11. Deve permitir a aplicação de Virtual Patching para vulnerabilidades tanto de clients como de servidores.
- 12.1.8.12. Deve bloquear técnicas avançadas de scan tais como: stealth scan e slow scan tanto em IPv4 como IPv6;
- 12.1.8.13. Deve suportar nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução através da utilização de expressões regulares;
- 12.1.8.14. Deve bloquear a origem de análises do tipo Portscan;
- 12.1.8.15. Deve possuir assinaturas e bloqueios contra-ataques do tipo buffer overflow;
- 12.1.8.16. Deve possuir pelo menos as seguintes ações de bloqueio.:

- 12.1.8.16.1. Bloqueio direto;
- 12.1.8.16.2. Reset de conexões;
- 12.1.8.16.3. Inclusão em Blacklist;
- 12.1.8.16.4. Página HTML;
- 12.1.8.16.5. HTTP redirect;
  
- 12.1.8.17. Deve suportar a captura e exportação de pacotes;
- 12.1.8.18. Deve possuir configurações de diferentes políticas de controle de ameaças baseadas no tipo de arquivos;
- 12.1.8.19. O mecanismo de inspeção deve receber e implementar em tempo real atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance;
- 12.1.8.20. Deve possuir exceções baseadas na fonte, destino, serviço, dias da semana, dias do mês, horário do dia, ligar ou desligar logs ou combinação entre eles;
- 12.1.8.21. Deve possuir um mecanismo de criação de exceções das políticas de IPS a partir do Log da solução, minimizando o impacto de falso-positivos no ambiente;

#### **12.1.9. Funcionalidades de VPN**

- 12.1.9.1. Deve proteger o tráfego corporativo em termos de confidencialidade através de encriptação e integridade entre os pontos finais, para estabelecer um canal virtual, através de um túnel seguro sobre uma rede tipicamente pública como a internet usando IPsec e SSL VPN;
- 12.1.9.2. Deve suportar os protocolos: IKEv1, IKEv2, and IPsec with IPv4 e IPv6;
- 12.1.9.3. Deve possuir os seguintes algoritmos de encriptação: AES-128, AES-256, AES-GCM-128, AES-GCM-256, Blowfish, DES, 3DES;

- 12.1.9.4. Deve possuir os seguintes métodos de autenticação: RSA, DSS, ECDSA signatures com certificados X.509, pre-shared key (PSK), XAUTH, EAP;
- 12.1.9.5. Deve possuir VPN site-to-site em topologias “Full Mesh” (cada gateway tem um link específico para os demais gateways), “Star” (gateways satélites se comunicam somente com o gateway central), “Hub and Spoke” (onde o gateway definido como Hub tem por responsabilidade redirecionar o tráfego para o seu gateway destino (spoke));
- 12.1.9.6. Deve suportar Main Mode e Aggressive mode em IKE Phase I;
- 12.1.9.7. Deve suportar CRL – Certificate Revocation Lists;
- 12.1.9.8. Deve suportar NAT-Transversal;
- 12.1.9.9. Deve suportar a criação de VPNs com base em rotas e com base em políticas;
- 12.1.9.10. Dever permitir a criação de políticas de controle de aplicações, IPS, anti malware e QoS para tráfego dos clientes remotos conectados na VPN, seja ela Site-to-Site ou Client-to-Site;
- 12.1.9.11. Deve possuir funcionalidade de acesso remoto incluindo tuneis SSL VPN e portal SSL VPN (mapeando URLs internas a URLs externas disponíveis a usuários que acessam o portal);
- 12.1.9.12. Deve possuir funcionalidades de SSL VPN permitindo:
  - 12.1.9.12.1. Que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento e por meio de interface Web;
  - 12.1.9.12.2. Atribuição de endereço de DNS aos clientes remotos;
- 12.1.9.13. Deve possuir funcionalidade de acesso remoto via cliente IPSec com as seguintes características:
  - 12.1.9.13.1. O cliente VPN deve ser compatível com pelos menos os seguintes sistemas operacionais: Android, MacOS, Windows 7 SP1, Windows 8.1 e Windows 10;

- 12.1.9.13.2. Deve possuir capacidade de autenticação via usuário e password (com integração a servidores externos como RADIUS e TACACS) e uso de certificados;
- 12.1.9.13.3. Deve permitir a configuração de MTU por parte do usuário;
- 12.1.9.13.4. Deve coletar informações de diagnóstico e permitir sua exportação;
- 12.1.9.13.5. Deve possuir ferramenta de captura de tráfego integrada ao cliente VPN;
- 12.1.9.13.6. Deve possuir funcionalidade de estabelecimento e manutenção automática de conexão VPN a gateway pré-estabelecido;

#### **12.1.10. Gerência de Tráfego WAN**

- 12.1.10.1. Deve ser fornecida uma solução de gerência de tráfego WAN integrada;
- 12.1.10.2. A solução de gerência de tráfego WAN poderá ser parte integrante da solução de firewall sem fazer com que os requisitos do firewall sejam prejudicados;
- 12.1.10.3. O balanceamento deve ser capaz de selecionar o caminho para o destino usando pelo menos os seguintes fatores:
  - 12.1.10.3.1. Banda Disponível
  - 12.1.10.3.2. Jitter
  - 12.1.10.3.3. Latência
- 12.1.10.4. Deve fornecer mecanismo de balanceamento de carga através dos enlaces para conexões VPN, sendo que as conexões possam ser balanceadas aumentando a capacidade do túnel VPN;
- 12.1.10.5. No caso de falha de um enlace, todas as conexões existentes devem ser automaticamente transferidas (statefully) para o outro enlace que estiver ativo, sem a necessidade de intervenção do administrador;
- 12.1.10.6. Deve possuir acrescentar novos enlaces de comunicação ao firewall sem que haja a necessidade de alterar enlaces existentes;



- 12.1.10.7. Deve fornecer o recurso de balanceamento de carga e agregação da capacidade de banda de enlace para estabelecimento de túneis VPN somando a capacidades destes enlaces de comunicação para o tráfego de dados dentro da VPN. Os enlaces devem ser agregados de modo a somar as capacidades dos enlaces;
- 12.1.10.8. Deve possuir funcionalidades de agregação de VPN site-to-site, baseando-se em políticas de VPN (quando a política define ser o tráfego deve ser enviado via VPN) ou com base em rotas, suportando topologias em hub e spoke, full-mesh ou malha parcial.
- 12.1.10.9. Deve ter a capacidade de realizar a seleção de links/agregação de links de forma dinâmica e automática;
- 12.1.10.10. A agregação de link deve possibilitar pelo menos dois modos:
- 12.1.10.11. Balanceamento de carga (load sharing): tráfego balanceado entre diferentes enlaces com base em medida de desempenho (tempo ao destino) ou banda relativa entre enlaces;
- 12.1.10.12. Deve ser possível a seleção de determinado link de comunicação em função do QoS (DSCP) associado a aplicação de rede sendo trafegada;
- 12.1.10.13. Deve realizar a seleção do link e estado de link (ativo/standby) em função de aplicação sendo usada na rede;
- 12.1.10.14. Deve ser possível decidir por qual link outbound o tráfego será encaminhado em função da aplicação transportada (aplicação esta identificada através de análise de conteúdo de pacote e não simplesmente através de análise de portas UDP/TCP);
- 12.1.10.15. Os equipamentos devem possuir mecanismos para facilitar a instalação onde seja possível carregar a configuração remotamente de um escritório central ou da nuvem, de tal forma que seja necessário apenas a configuração de um endereço ip restringindo a necessidade de interação local para localidades remotas;

#### **12.1.11. Funcionalidades de Filtro WEB**

- 12.1.11.1. Deve especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- 12.1.11.2. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs e redes;
- 12.1.11.3. Deve possuir a capacidade de criar políticas baseadas na visibilidade e controle de quem está utilizando os serviços de diretório, autenticação via LDAP, Active Directory;
- 12.1.11.4. Deve permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;
- 12.1.11.5. Deve suportar a capacidade de criar políticas baseadas no controle por URL e Categoria de URL;
- 12.1.11.6. Deve possuir no mínimo 70 categorias de URLs;
- 12.1.11.7. Deve suportar a customização de páginas de bloqueio;
- 12.1.11.8. Deve permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir o usuário continuar acessando o site);

#### **12.1.12. Sistema de Gerência Centralizada**

- 12.1.12.1. A interface de gerência centralizada deve suportar a edição de política da mesma política segurança por mais de um usuário administrador de forma simultânea.
- 12.1.12.2. A interface de gerência centralizada deve suportar a edição de políticas de segurança por mais de um usuário administrador de forma simultânea;
- 12.1.12.3. Deve permitir o gerenciamento centralizado (interface única de gerência) dos equipamentos a suas configurações de rede, de segurança, gerência de logs, geração de relatórios e sistema de gerência de tráfego WAN;

- 12.1.12.4. Deve suportar a definição de um modelo de regras (política de segurança), sobre as quais todas as demais regras ficarão subordinadas, seguindo o conceito de federalização ou hierarquização;
- 12.1.12.5. A gerência deve permitir a busca por ativos;
- 12.1.12.6. Deve permitir a criação de políticas de acordo com sistema operacional dos usuários;
- 12.1.12.7. Deve possuir a comparação entre a política atual e a última política;
- 12.1.12.8. Deve possuir o agrupamento por tipo e por geolocalização;
- 12.1.12.9. Deve permitir a visualização da utilização dos links por equipamento;
- 12.1.12.10. Deve permitir a visualização das aplicações mais utilizadas em cada link.
- 12.1.12.11. Possuir a visualização das VPN's, permitindo sua configuração através de ferramenta gráfica, com técnica facilitadora de arrasta e solta para alteração da política.
- 12.1.12.12. Deve possuir ferramenta integrada de validação de políticas, permitindo ao administrador verificar a parte da configuração que gerou questões associadas ao processo de validação;
- 12.1.12.13. Caso a solução possua licenças relacionadas a armazenamento, deve ser ofertada a de capacidade ilimitada;
- 12.1.12.14. Deve realizar o gerenciamento centralizado das licenças dos equipamentos monitorados;
- 12.1.12.15. O gerenciamento deve suportar comunicação via cliente ou web (GUI), utilizando protocolo seguro (criptografado), encriptação entre equipamento e sistema de gerenciamento;
- 12.1.12.16. Cliente para administração da solução de gerenciamento, deve possuir compatibilidade e homologação para os sistemas operacionais Windows e Linux;
- 12.1.12.17. Deve possuir perfis de acesso a console customizáveis, com permissões granulares, no mínimo com os seguintes perfis: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações, alteração em políticas de acesso.

- 12.1.12.18. Deve permitir a localização de regras em que determinado endereço IP, range de IP, sub-rede ou objeto estejam sendo utilizados;
- 12.1.12.19. Deve permitir a visualização do número de vezes que uma determinada regra foi usada (hits) em diferentes intervalos de tempo como dia, semana, mês e intervalo customizável como data e horário de início e de fim da contagem;
- 12.1.12.20. Deve permitir a exportação de logs de auditoria detalhados, no mínimo, informando alterações da configuração realizada com horário das alterações;
- 12.1.12.21. Deve possibilitar a coleta de estatísticas do tráfego realizado pelos dispositivos de segurança;
- 12.1.12.22. Deve permitir a geração de relatórios, em tempo real, para a visualização de origens e destinos do tráfego gerado na Instituição;
- 12.1.12.23. Deve possuir dashboard específico para gerência de tráfego WAN indicando a qualidade de links em função de perda de pacotes, atraso fim a fim e jitter (variação do atraso fim a fim);
- 12.1.12.24. Deve possuir a capacidade de gerar relatórios gráfico que permita visualizar as mudanças na utilização de aplicações na rede, no que se refere a um período anterior, para permitir comparação entre os diferentes consumos realizados pelas aplicações, no tempo presente com relação ao tempo passado;
- 12.1.12.25. Deve prover visualização sumarizada e possuir gerar relatórios de todas as ameaças (IPS, antivírus, anti-malware) e aplicações trafegadas pelos firewalls gerenciados;
- 12.1.12.26. Deve possuir a criação de dashboards customizados, possibilitando a visibilidade do tráfego de aplicações, usuários, ameaças identificadas pelo IPS, antivírus, malwares "Zero Day" detectados em sandbox (quando aplicável) e tráfego bloqueado;
- 12.1.12.27. Deve possuir mecanismo "Drill-Down" para visualização, em tempo real, das informações sumárias produzidas pela ferramenta de gerência;

- 12.1.12.28. Deve permitir que os relatórios sejam enviados via e-mail;
- 12.1.12.29. Deve permitir que os relatórios possam ser exportados em PDF, HTML e texto;
- 12.1.12.30. Deve possuir a capacidade de gerar alertas provenientes de eventos como:
  - 12.1.12.30.1. Erro no sistema operacional do gerenciador centralizado;
  - 12.1.12.30.2. Falhas detectadas em autoteste do firewall;
  - 12.1.12.30.3. O uso de uma determinada regra de uma política;
- 12.1.12.31. Deve permitir que os logs sejam rotacionados de forma que os registros mais antigos sejam apagados quando não houver espaço de armazenamento disponível;
- 12.1.12.32. Deve possuir a exibição, de forma histórica e em tempo real (permitindo a filtragem por firewall gerenciado), com atualização automática e contínua, a cada minuto, hora, dia, semana ou mês das seguintes informações:
  - 12.1.12.33. Situação do dispositivo e do cluster (geral);
  - 12.1.12.34. Principais aplicações;
  - 12.1.12.35. Principais aplicações por classificação (chat, redes sociais, compartilhamento de arquivos, ...);
  - 12.1.12.36. Principais aplicações por volume transferido;
  - 12.1.12.37. Volume de tráfego transferido nos túneis VPN;
  - 12.1.12.38. Deve permitir a atualização dos firewalls de forma remota;
  - 12.1.12.39. Em modo cluster o firewall deve ser atualizado sem interrupções, não havendo interferência no encaminhamento e tratamento das conexões;
  - 12.1.12.40. Coletar metadados das máquinas dos usuários, permitindo criação de políticas baseadas nas informações coletadas.

|  |
|--|
| <b>12.2. IMPLANTAÇÃO DOS SERVIÇOS DE PROTEÇÃO DE PERÍMETRO</b> |
|--|

- 12.2.1. Serão de responsabilidade da CONTRATADA as atividades de implantação, instalação, integração, configuração e testes de todos os produtos componentes de cada solução alocada, em conformidade com o Projeto Executivo a ser elaborado e apresentado pela CONTRATADA para prévia aprovação.
- 12.2.2. A CONTRATADA deverá levantar informações acerca dos locais de instalação dos produtos durante a elaboração do Projeto Executivo, e, se necessário, efetuar visita técnica para verificar eventuais requisitos físicos a serem providos para a correta instalação e prestação dos serviços;
- 12.2.3. A elaboração do Projeto Executivo é de responsabilidade da CONTRATADA, e deverá conter as fases do projeto, os cronogramas de execução, e a descrição detalhada dos produtos e subprodutos a serem entregues em cada fase.
- 12.2.4. No Projeto Executivo, a CONTRATADA deverá elaborar a descrição de topologia lógica e física da rede atual e topologia pretendida em cada etapa;
- 12.2.5. Efetuar o mapeamento de criticidade de todos os ativos envolvidos no projeto;
- 12.2.6. Projetar a engenharia de tráfego da Rede da ES Gás;
- 12.2.7. Planejar a migração das configurações do parque atualmente em funcionamento, sem nenhuma mudança nas configurações atuais sem prévia aprovação da ES Gás;
- 12.2.8. Para a implantação dos serviços, indicar de forma detalhada as condições de rollback de cada mudança no ambiente;
- 12.2.9. Estimar o consumo de unidades de rack em U's e de energia de cada ativo a ser instalado nas dependências da ES Gás;
- 12.2.10. Os hardwares e softwares e demais componentes necessários à correta prestação dos serviços deverão:
- 12.2.10.1. Conter os recursos necessários e estarem configurados de modo a garantir total operabilidade no ambiente computacional da ES Gás e

otimizados para usufruir das melhores condições em termos de desempenho e disponibilidade;

12.2.10.2. Conter a última versão de software e firmware homologado pelo fabricante;

12.2.10.3. Ter configuradas senhas de acesso, para que a equipe de funcionários designados pela ES Gás efetue o acesso para a visualização das configurações e logs (acesso seguro e remoto);

12.2.10.4. Ter configurada senha com direitos totais de administração e configuração a ser utilizada pela ES Gás em caso de emergência;

12.2.10.5. Ser configurados para enviar logs para as soluções de concentração de logs disponibilizados no site da ES Gás;

12.2.11. Para aprovação da instalação e configuração de qualquer item que ensejar a emissão de termo de recebimento definitivo, a CONTRATADA deve elaborar relatório técnico com análise dos resultados e impactos decorrentes da atividade executada;

12.2.12. Quando realizadas no ambiente de produção, as atividades poderão ser agendadas para serem executadas após o horário de expediente, a saber, em horários noturnos – após às 20h00 (vinte horas) – além de finais de semana e feriados, conforme disponibilidade da ES Gás;

### 13. RECONFIGURAÇÃO DA REDE DE CONECTIVIDADE

**13.1.** A CONTRATADA deverá prover a reconfiguração de equipamentos do parque atual, de forma personalizada para a ES Gás, como descrito abaixo:

13.1.1. Todo endereçamento IP deverá ser compatível ou seguir o padrão definido no serviço de DHCP da CONTRATANTE.

13.1.1.1. Caso necessário, a CONTRATADA deverá propor às melhores práticas de mercado adequadas às necessidades deste projeto.

13.1.2. A rede wireless deverá ser segmentada por serviço para diminuir o broadcast na rede possibilitando melhor desempenho e segurança sendo elas:

13.1.2.1.1. ES Gás-Corp – Acessa a rede corporativa interna por meio do Active Directory utilizando o protocolo RADIUS carregando para a estação de trabalho todas as GPOs e políticas da rede interna;

13.1.2.1.2. ES Gás-Mobile – Rede para conexões de celulares corporativos. Deve acessar outra faixa da rede/endereço e identificar apenas os smartphones com mac previamente cadastrado;

13.1.2.1.3. ES Gás-Guest – Rede para conexões de visitante. Acessa por meio de voucher, com identificação do usuário e aceite de consentimento. O acesso deverá ser de forma isolada em uma rede exclusiva e isolada, com a finalidade de prover acesso à Internet à visitantes.

13.1.2.2. Reconfiguração personalizada dos Access Points, Switches, Roteadores e Firewalls conforme as seguintes especificações e quantidades:

| Access Points            |                             |            |
|--------------------------|-----------------------------|------------|
| Unidade                  | Modelo                      | Quantidade |
| Matriz                   | Cisco® Aironet® 1830 Series | 3          |
| Centro de Operações COGN | Cisco air-sap2602i-t-k9     | 1          |



| Switches              |                       |            |
|-----------------------|-----------------------|------------|
| Unidade               | Modelo                | Quantidade |
| Sede                  | Juniper EX 4200 (48P) | 2          |
| Centro de Operações   | Juniper EX 4200 (48P) | 2          |
| Centro de Operações   | Juniper EX 3200 (24P) | 4          |
| Centro de Operações   | Juniper EX 2200 (24P) | 1          |
| Agência de Vitória    | Juniper EX 2200 (24P) | 1          |
| Agência de Vila Velha | Juniper EX 2200 (24P) | 1          |

| Roteadores          |                |            |
|---------------------|----------------|------------|
| Unidade             | Modelo         | Quantidade |
| Centro de Operações | CISCO – 2801   | 1          |
| Centro de Operações | CISCO - 2911K9 | 1          |

| Firewalls           |                               |            |
|---------------------|-------------------------------|------------|
| Unidade             | Modelo                        | Quantidade |
| Datacenter (Cloud)  | Fortinet 200F(ou equivalente) | 1          |
| Centro de Operações | Fortinet 200A                 | 1          |

### 13.2. ENTREGAS A SEREM REALIZADAS

Para este serviço a CONTRATADA deverá entregar os equipamentos de rede atuais da CONTRATANTE reconfigurados e integrados ao sistema de conectividade e segurança objeto deste edital. Ela deverá prover todas as configurações necessárias para garantir a disponibilidade e segurança da rede.

## **14. SOLUÇÃO DE PROTEÇÃO AVANÇADA DE ENDPOINT (EPP/EDR)**

Visa a implantação de solução dedicada a proteção de estações e servidores do CONTRATANTE, realizando de forma proativa o bloqueio de códigos maliciosos tipo vírus, malware - protegendo os ativos também contra ransomware, oferecendo a possibilidade de realização de “rollback” de arquivos alvos de código maliciosos, oferecendo ainda suporte à investigação de ataques através da trilha de registros de eventos forense.

### **14.1.1. SOBRE A PROTEÇÃO AVANÇADA DE ENDPOINT**

A implantação de solução de proteção avançada de endpoint (EPP/EDR) deverá seguir os preceitos técnicos definidos abaixo, com o intuito da CONTRATADA ofertar plataforma de solução avançada de segurança para endpoint, na modalidade de software licenciado para a ES Gás, agregando qualidade e mais proteção ao processo:

14.1.1.1. Cabe à CONTRATADA licenciar para a ES Gás e instalar toda a solução de Plataforma de Proteção de Endpoint - EPP Endpoint Protection Platform e Detecção e Resposta de Endpoint – EDR Endpoint Detection and Response para 200 ativos dentre estações de trabalho e servidores de rede.

14.1.1.2. Deverá ser criado usuário de administração e de leitura para equipe da CONTRATANTE, para acompanhamento das ações na console de gerenciamento;

### **14.1.2. Requerimentos Gerais da Solução**

14.1.2.1. A solução oferecida deve ser independente de qualquer outra solução de segurança implementada ou a ser implementada. Todos os recursos necessários devem ser fornecidos na contratação;

- 14.1.2.2. O gerenciamento da solução deverá ser feito na cloud do fabricante, via browser, não sendo aceitas soluções com gerenciamento on-premises;
- 14.1.2.3. Deve permitir gerar alertas das soluções integradas;
- 14.1.2.4. Deve permitir e possuir APIs bidirecionais para facilitar a integração de outras soluções;
- 14.1.2.5. Receber os índices de comprometimento de todas as soluções integradas (Endpoint) e realizar trocas transparentes entre elas, permitindo que uma detecção em um dos vetores, automaticamente seja implementada nas demais soluções, sem a necessidade de download de uma vacina ou novo pacote de inteligência;
- 14.1.2.6. Permitir bloqueio de artefatos com apenas uma única ação para todas as soluções do lote;
- 14.1.2.7. Deve implementar a tecnologia de EDR (Endpoint Detection and Response) nos endpoints sem a necessidade de nenhum agente adicional;
- 14.1.2.8. A solução completa deve utilizar um único agente, incluindo todas as funcionalidades (Antivírus, Anti-Malware, EDR, XDR, e as demais exigidas neste termo.);
- 14.1.2.9. A implementação das funcionalidades de EDR não devem requerer a utilização de nenhuma console adicional;
- 14.1.2.10. Dispor de proteção contra ransomware não baseada exclusivamente na detecção por assinaturas;
- 14.1.2.11. Dispor de prevenção contra a ação de criptografia maliciosa executada por ransomwares, possibilitando ainda o bloqueio dos computadores de onde partirem tal ação;
- 14.1.2.12. A solução deve possuir de forma bem documentada suas APIs públicas, as quais podem ser utilizadas para futuras integrações;
- 14.1.2.13. A solução deve possuir tecnologias de proteção contra ameaças avançadas e gerar alertas quando elas forem detectadas no ambiente;

14.1.2.14. A solução deve possuir capacidade para responder de forma efetiva durante as investigações realizadas pelo time de operações ou de resposta a incidente, provendo através de sua console centralizada capacidades para coleta de artefatos, análise de processos e isolamento de equipamentos;

14.1.2.15. A solução deve fornecer visibilidade abrangente que permitirá às equipes de segurança da CONTRATANTE procurar, identificar e discernir rapidamente o nível de ameaças detectadas, além de possuir recursos de detecção e resposta para identificar, investigar e conter equipamentos de forma rápida e agilizar a resposta;

14.1.3. Console de gerenciamento:

14.1.3.1. A solução deve possuir um console de gerenciamento centralizado para todos os agentes implantados;

14.1.3.2. A console de gerenciamento deve estar na nuvem do fabricante, não sendo aceitos soluções de gerenciamento on-premises;

14.1.3.3. O console de gerenciamento centralizado de terminais deve ter pelo menos as seguintes funcionalidades:

14.1.3.4. Permitir definir e gerenciar grupos de dispositivos, que devem ser definidos de forma estática ou por meio de um filtro lógico, com base nas características dos dispositivos que suportam a criação de combinações lógicas;

14.1.3.5. Permitir a exportação dos alertas através da própria console;

14.1.3.6. Deve permitir controlar dispositivos de armazenamento conectados via USB, permitindo bloquear o acesso ou liberar. Adicionalmente deve ser possível a criação de exceções na política pelo identificador do fabricante e tipo de dispositivo, para os sistemas operacionais Windows, Linux e MacOS.

14.1.3.7. Deve permitir controlar dispositivos conectados via Bluetooth, permitindo bloquear o acesso ou liberar. Adicionalmente deve ser

possível a criação de exceções na política pelo identificador do fabricante e tipo de dispositivo;

- 14.1.3.7.1. Deve permitir a criação de regras de Firewall, para os sistemas operacionais Windows, Linux e MacOS, por grupos de dispositivos, contendo minimamente as seguintes funções:
  - 14.1.3.7.2. Ação (Bloquear ou permitir);
  - 14.1.3.7.3. Protocolo;
  - 14.1.3.7.4. Caminho (path) de uma aplicação
  - 14.1.3.7.5. Endereço local;
  - 14.1.3.7.6. Porta local;
  - 14.1.3.7.7. Endereço remoto;
  - 14.1.3.7.8. Porta remota.
- 14.1.3.8. Deve fornecer acesso seguro ao console por meio de uma interface web HTTPS;
- 14.1.3.9. Deve gerenciar alertas antigos, permitindo a exclusão automática e/ou envio de alertas aos administradores;
- 14.1.3.10. O painel de controle da solução (dashboard) deve exibir pelo menos as seguintes métricas de detecção e contenção: Número de terminais com alertas, número total de alertas, número de indicadores separados por fonte de inteligência;
- 14.1.3.11. Todas as informações geradas pelo equipamento devem poder ser analisadas no mesmo console, sem ter que acessar outro software adicional;
- 14.1.3.12. A solução deve poder enviar alertas por e-mail;
- 14.1.3.13. O dashboard deve exibir pelo menos o número total de equipamentos monitorados e o número de equipamentos ativos;
- 14.1.3.14. O console deve oferecer as versões de agentes disponíveis para download;
- 14.1.3.15. A frequência de atualização dos agentes no console central deve ser de pelo menos 5 minutos.
- 14.1.3.16. Todos os agentes devem suportar a visualização de dados como:

- 14.1.3.17.Nome do usuário logado;
- 14.1.3.18.Nome do host;
- 14.1.3.19.Informações de sistema operacional (Build, Plataforma.);
- 14.1.3.20.Estado do equipamento (Online ou Offline);
- 14.1.3.21.Última data comunicação com a console de gerenciamento;
- 14.1.3.22.Informações relacionadas à rede (IP, DNS, DHCP.);
- 14.1.3.23.Versão do agente.
- 14.1.4. A solução deve permitir a criação de usuários com perfis para, no mínimo:
  - 14.1.4.1. Administrador (sysadmin);
  - 14.1.4.2. Administrador limitado;
  - 14.1.4.3. Usuários de monitoramento.
- 14.1.5. Requerimentos gerais do agente
  - 14.1.5.1. A solução deve possuir capacidade de ser instalada sem requerer nenhuma licença adicional de sistema operacional ou qualquer outra não fornecida pela CONTRATADA;
  - 14.1.5.2. Deve suportar pelo menos os sistemas operacionais Windows, Linux e MacOS.
  - 14.1.5.3. Uma solução baseada em agente deve ser fornecida para a proteção de ameaças de ataques de dia zero em ameaças que não utilizam assinaturas ou padrões como a principal forma de detecção e bloqueio de ameaças;
  - 14.1.5.4. A solução deve operar em tempo real, monitorando e bloqueando as ameaças;
  - 14.1.5.5. A solução deve detectar e bloquear tentativas de exploração por malware conhecido ou desconhecido, usando técnicas de análise de comportamento na interação entre componentes;
  - 14.1.5.6. A solução deve fornecer a capacidade de executar análises de estações de trabalho/servidores sem a necessidade de interagir com o

usuário. Essa capacidade deve ser centralizada e transparente para o usuário;

- 14.1.5.7. A solução deve fornecer suporte para estações de trabalho que não estão conectadas à rede interna, como computadores na Internet, sem perder a capacidade de proteger e atualizar;
- 14.1.5.8. Deve incluir recursos para detecção de malware conhecido, incluindo a capacidade de operar em conjunto com outras ferramentas de proteção a estações de trabalho;
- 14.1.5.9. A solução deve ter a capacidade de detectar metodologias e padrões de ataques, mesmo sem a presença de arquivos de malware (malware operando apenas na memória\fileless);
- 14.1.5.10. No caso de detecção de um incidente, a solução deve permitir a execução de rotinas automatizadas para rapidamente responder aos eventos gerados pelos dispositivos;
- 14.1.5.11. A solução deve poder colocar em quarentena máquinas infectadas, isolando-as logicamente da rede;
- 14.1.5.12. A solução deve implementar adicionalmente, as seguintes funcionalidades:
  - 14.1.5.12.1. Rastreio de detecção de possíveis movimentações laterais, criando um mapa visual das ocorrências;
  - 14.1.5.12.2. Rastreio de processos suspeitos, aos quais podem receber classificações através dos indicadores de comprometimentos mapeados pela rede de inteligência do fabricante;
  - 14.1.5.12.3. Rastreio de tentativas de roubo de credenciais e/ou tentativa de acessos indevidos a recursos chave do sistema operacional;
  - 14.1.5.12.4. Permitir a visualização automática de contexto adicional sobre alertas, fornecendo um fluxo de trabalho automatizado que coleta e analisa artefatos, destacando rapidamente índices de comprometimento já conhecidos;

- 14.1.5.12.5. A solução deve permitir a criação de exceção em caso de falso positivo ou até mesmo em casos pontuais para atendimento de possíveis regras do negócio;
- 14.1.5.12.6. A solução deve possuir módulos de detecção avançados, tais como mecanismos de machinelearning e proteção contra exploração de vulnerabilidades em aplicações, também permitindo que exceções ou customizações de regras sejam realizadas para impedir falsos positivos ou até mesmo para atender regras do negócio;
- 14.1.5.12.7. A solução deve permitir a configuração de autoproteção como, configurar uma senha para impedir sua remoção por usuários não autorizados;
- 14.1.5.12.8. A solução deve prover formas de segregar os equipamentos por grupo facilitando assim a aplicação de políticas granulares e outras configurações;
- 14.1.5.12.9. A solução deve permitir a criação de grupos de hosts de forma estática, ou seja, adicionando manualmente todos os ativos pertinentes;
- 14.1.5.12.10. A solução deve permitir a criação de grupos de hosts dinâmicos, movimentando os ativos automaticamente, baseado minimamente nos seguintes critérios:
- 14.1.5.12.11. Domínio na qual a máquina está inserida ou grupo de trabalho;
- 14.1.5.12.12. Sistema operacional;
- 14.1.5.12.13. Subnet.
- 14.1.5.12.14. A solução deve possuir capacidade de realizar ações tais como:
  - 14.1.5.12.14.1. Coleta de arquivos;
  - 14.1.5.12.14.2. Isolamento de hosts;
  - 14.1.5.12.14.3. Obter listagem de arquivos comprometidos da máquina;



14.1.5.12.14.4. Obter pacotes de diagnóstico para análise de saúde do agente;

14.1.5.12.14.5. Acessar remotamente os sistemas operacionais Windows, Linux e MacOS através de:

1.1.5.12.14.5.1. PowerShell;

1.1.5.12.14.5.2. Bash;

14.1.5.13.A solução deve permitir a customização de ações, facilitando assim o tipo de coleta durante uma investigação;

14.1.5.14.A solução deve permitir a realização de análise das coletas através da console centralizada, sem necessidade de extrair estes dados durante a análise inicial;

14.1.5.15.A solução deve permitir realizar buscas específicas sobre os eventos coletados e catalogados na console centralizada, assim como permitir a realização de buscas em tempo real de indicadores de comprometimento;

14.1.5.16.A plataforma deve submeter a rede de inteligência do fabricante todos os hashes de arquivos verificados pelos agentes, obtendo respostas rápidas sobre o nível de risco do artefato.

#### 14.1.6. Requerimentos técnicos do agente

14.1.6.1. Suportar a instalação em ambientes Windows, suportando minimamente:

14.1.6.2. Windows XP SP3;

14.1.6.3. Windows 7 SP1;

14.1.6.4. Windows 8;

14.1.6.5. Windows 10;

14.1.6.6. Windows 11;

14.1.6.7. Windows Server 2008 R2 SP1;

14.1.6.8. Windows Server 2012;

14.1.6.9. Windows Server 2016;

14.1.6.10.Windows Server 2019;

14.1.6.11.Windows Server 2022;

14.1.6.12.Deve suportar distribuições Linux para no mínimo, as seguintes versões:

14.1.6.12.1. Red Hat Enterprise Linux (RHEL) 6.8 a 6.10;

14.1.6.12.2. Red Hat Enterprise Linux (RHEL) 7.1 a 7.7;

14.1.6.12.3. Red Hat Enterprise Linux (RHEL) 8;

14.1.6.12.4. CentOS 6.8 a 6.10;

14.1.6.12.5. CentOS 7.1 a 7.7;

14.1.6.12.6. CentOS 8;

14.1.6.12.7. Ubuntu 14.04, 16.04, 18.04, 19,10 e 20.04;

14.1.6.12.8. SUSE Linux Enterprise 12 e 15;

14.1.6.12.9. Debian 8, 9 e 10;

14.1.6.12.10.Fedora 32 e 33

14.1.6.13.Deve suportar distribuições MacOS para no mínimo, as seguintes versões:

14.1.6.14.10.4

14.1.6.15.10.15.1 a 10.15.7

14.1.6.16.11.0 a 11.6

14.1.6.17.12.0 a 12.2

14.1.6.18.Deve suportar sistemas de 32 e 64 bits;

14.1.6.19.Agente único com mecanismos de detecção para minimizar a configuração e maximizar a detecção e o bloqueio;

14.1.6.20.A solução deve poder operar independentemente da localização da estação de trabalho, desde que esteja conectada à Internet.

14.1.7. Capacidades técnicas necessárias:

14.1.7.1. Capacidade de detectar malware conhecido, incluindo vírus, cavalos de tróia, worms, spyware, adware, keyloggers, rootkits e outros programas indesejados;

14.1.7.2. Detectar, possíveis incursões;

14.1.7.3. Responder, de forma a fazer a contenção e correção dos problemas;

- 14.1.7.4. A solução deve oferecer suporte ao uso de indicadores de comprometimento para detecção de presença e execução de malware. Os indicadores de compromisso devem ser fornecidos pelo fabricante e atualizados automaticamente e regularmente;
- 14.1.7.5. A solução deve fornecer uma API que permita a integração com outros produtos. A API deve ser adequadamente documentada para conhecer todas as operações possíveis e os valores e parâmetros necessários para utilização;
- 14.1.7.6. A API deve fornecer autenticação baseada em certificados digitais e deve ser acessada através de um protocolo SSL seguro;
- 14.1.7.7. A solução deve permitir que os agentes usem uma configuração de proxy para se conectar ao console;
- 14.1.7.8. A solução deve permitir fazer a reversão (rollback) de um ataque via ransomware, se integrando com o Volume Shadow Copy do Windows.
- 14.1.7.9. A solução deve incluir recursos de proteção baseados em malware conhecido e sua interação com os arquivos no sistema de arquivos. Qualquer arquivo malicioso deve ser isolado e armazenado em uma área de quarentena;
- 14.1.7.10. A solução deve incluir scans de todos os arquivos no disco do dispositivo.
- 14.1.7.11. Todos os requisitos de investigação devem ser listados juntamente com o status de execução, indicando se estão pendentes, em execução ou executados, bem como se algum erro foi detectado no processo;

## **15. DESENVOLVIMENTO DO TRABALHO**

Após a assinatura do contrato, a ES Gás emitirá uma Autorização de Serviço, documento que solicita e autoriza a execução dos serviços nele descritos.

## **16. IMPLANTAÇÃO**

**16.1.** Os serviços de implantação deverão contemplar o fornecimento de appliances Fortigate, implantação da rede SD-WAN e módulos de UTM/NGFW, configuração dos serviços EPP/EDR e reconfiguração dos ativos de rede (switches, roteadores, access points) e VLANs.

**16.2.** Os serviços de instalação dos equipamentos de proteção de perímetro serão prestados conforme Item 12.2. IMPLANTAÇÃO DOS SERVIÇOS DE PROTEÇÃO DE PERÍMETRO deste documento;

**16.3.** A Implantação de solução de segurança do Firewall deverá contemplar todos os produtos licenciados e com as soluções de UTM e NGFW descritas a seguir: (Forticare, FortiGuard App Control Service, FortiGuard IPS Service, FortiGuard Advanced Malware Protection AMP, FortiGuard Web Filtering Service, FortiGuard Antispam Service) devidamente configuradas e implantadas conforme as melhores práticas de mercado, como:

16.3.1. Módulo de conectividade para SD-WAN;

16.3.2. VPN ipsec;

16.3.3. IPS;

16.3.4. IDS;

- 16.3.5. WebBlocker;
- 16.3.6. Proxy;
- 16.3.7. WAF;
- 16.3.8. Antispam;
- 16.3.9. Antimalware;
- 16.3.10. SSL;
- 16.3.11. QoS;
- 16.3.12. Inspection;
- 16.3.13. AntiDoS;
- 16.3.14. SIEM.

**16.4.** A implantação dos Firewall deverá ser realizada em alta disponibilidade HA.

**16.5.** Deverá ser realizada a configuração dos equipamentos atuais: Roteadores, Access Point, Switches e VLANs necessárias na rede da ESGAS de acordo com as especificações do item 13. RECONFIGURAÇÃO DA REDE DE CONECTIVIDADE.

**16.6.** Deverá ser realizada a Implantação de solução End Point Protection - EPP e Endpoint Detection and Response – EDR de acordo com as especificações no item 14. SOLUÇÃO DE PROTEÇÃO AVANÇADA DE ENDPOINT (EPP/EDR).

**16.7.** Toda a solução implantada deverá abranger as interconexões entre os pontos de rede da Es Gás com o centro de operações e as agências, conforme item 3.1 DIAGRAMA ATUAL DA REDE.

**16.8.** A implantação deverá seguir o cronograma definido na Tabela abaixo:

**Cronograma de entrega**

| <b>Etapas</b> | <b>Intervalo</b>  | <b>Descrição</b>  |
|---------------|---|---|
| <b>1</b>      | 0   | Data indicada pelo Gestor de TI na Autorização para Início dos Serviços   |
| <b>2</b>      | Até 45 dias   | Instalação dos equipamentos de hardware e softwares necessários para prestação dos serviços;<br>Configuração das regras de detecção e prevenção;<br>Entrega de documentação do serviço; |
| <b>3</b>      | 15 dias úteis a partir do aceite técnico da etapa 2           | Operação Assistida dos ativos implementados e de toda conectividade de rede.  |
| <b>4</b>      | Em até 30 dias contados a partir do aceite técnico da etapa 2 | Transferência de conhecimento – Hands-On para a equipe de segurança da Es Gás.  |

**16.9. Operação Assistida**

16.9.1. A operação assistida, citada na etapa 3, em cronograma de entrega, consiste na permanência de mais um profissional da CONTRATADA, para atender as solicitações, operar o sistema e solucionar todas as dúvidas e problemas que possam ocorrer com a solução instalada;

16.9.2. O horário de permanência do profissional citado deverá ser o mesmo do expediente do CONTRATANTE, de segunda-feira à sexta-feira, das 9h às 18h;

16.9.3. O profissional deverá estar identificado com crachá da CONTRATADA durante sua permanência nas dependências do

CONTRATANTE.

**16.10.** Transferência de conhecimento (Hands-On)

16.10.1. Deverá ser fornecido um acompanhamento técnico para uma turma de até 5 participantes nas dependências da ES Gás:

16.10.1.1. O acompanhamento deverá abranger uma capacitação em formato Hands-On para os profissionais de segurança da Es Gás e contemplar os seguintes tópicos:

16.10.1.1.1. Conceitos sobre segurança cibernética, IPS, correlação de eventos, gestão de vulnerabilidades e ameaças atuais;

16.10.1.1.2. Todas as funcionalidades especificadas neste termo de referência;

16.10.1.1.3. Público-alvo: Equipe Técnica da ES Gás;

16.10.1.1.4. Carga horária mínima: 40 horas.

**16.11.** Serviços de Suporte da solução por profissionais especializados (N3)

Sob Demanda.

16.11.1. Os serviços de suporte sob demanda caracterizam-se por serviços que contemplem as atividades de nível especializado e operacional para configuração e operação de toda a solução objeto deste termo que poderão ser consumidos sob demanda, de acordo com as necessidades da ES GÁS.

16.11.2. Os atendimentos se darão por meio de horas técnicas

contratadas.



## **17. PRAZO**

O contrato terá vigência de 24 (vinte e quatro) meses, desdobrando-se de acordo com as características de cada serviço e entregas a serem realizadas.

## **18. RESPONSABILIDADES DA CONTRATADA**

- 18.1.** Manter, durante toda a execução do Contrato, todas as condições estabelecidas no EDITAL e em seus ANEXOS, e assim como em relação às demais exigências contratuais.
- 18.2.** Responsabilizar-se pelo integral cumprimento do contrato, arcar com os eventuais prejuízos causados a ES Gás ou a terceiros, provocados por ineficiência no fornecimento dos produtos, respondendo integralmente pelo ônus decorrente, o que não exclui nem diminui a responsabilidade pelos danos que se evidenciarem, independentemente do controle e fiscalização exercidos pela ES Gás.
- 18.3.** Fornecer as devidas notas fiscais/faturas, nos termos da lei e cumprir todas as obrigações fiscais decorrentes da execução do Contrato, responsabilizando-se por quaisquer infrações fiscais daí advindas.
- 18.4.** Prestar as informações e esclarecimentos relativos ao objeto desta contratação, que venham a ser solicitados pelos agentes designados pela ES Gás.
- 18.5.** A CONTRATADA não poderá cobrar valores adicionais ao valor do contrato, tais como custos de deslocamento, alimentação, transporte, alojamento, trabalho aos sábados, domingos, feriados ou em horário noturno, bem com qualquer outro valor adicional.
- 18.6.** Observar durante a realização do trabalho e nos produtos a serem entregues todas as leis, decretos, normas, portarias, instruções normativas, enfim todas as normas a que esteja submetido a ES Gás.
- 18.7.** É de responsabilidade da CONTRATADA fornecer todos os recursos materiais, humanos e de informática (software, hardware) necessários à execução dos serviços previstos neste Memorial Descritivo.

- 18.8.** A CONTRATADA deverá formalizar Acordo de Nível de Serviços com a CONTRATANTE.
- 18.9.** A CONTRATADA deverá manter canal para comunicação, de maneira a receber e protocolar solicitações de suporte, alteração, dúvidas e/ou customização.
- 18.10.** A CONTRATADA deverá garantir, junto aos serviços de manutenção e sustentação, a atualização (releases) de versões da solução fornecida.
- 18.11.** A CONTRATADA deverá, quando da solicitação da CONTRATANTE para execução de manutenção, emitir número/código de referência da solicitação, que deve servir como identificação em todos os contatos e acordos realizados entre ambos.
- 18.12.** A CONTRATADA deverá, quando da entrega de sistema ou ajustes, disponibilizar versão em área de transferência escolhida da CONTRATANTE.

## **19.SUBCONTRATAÇÃO**

Será permitida a subcontratação de até 25% (vinte e cinco por cento) do objeto contratual. É vedada a subcontratação de empresa participante do certame.

## 20. PLANILHA DE PREÇOS UNITÁRIOS

As linhas de serviço a serem precificadas no ANEXO I, Planilha de Preços Unitários (PPU), foram definidas conforme segue:

### 20.1. Item 01.00 Aquisição de Appliance de Segurança (Hardware):

| Item | Descrição   | Métrica  | Quantidade |
|------|---|----------|------------|
| 1    | Appliance Next Generation Firewall FortiGate 60F (NGFW01) | Unitário | 2          |
| 2    | Appliance Next Generation Firewall FortiGate 40F (NGFW02) | Unitário | 2          |

### 20.2. Item 02.00 Software:

| Item | Descrição  | Métrica   | Quantidade |
|------|--|-----------|------------|
| 1    | Licenciamento - Gerenciamento dos Firewalls                                | 24 meses  | 4          |
| 2    | Licenciamento de solução de proteção avançada de endpoint EPP/EDR (2 anos) | Endpoints | 200        |

### 20.3. Item 03.00 Serviços de Implantação:

| Item  | Descrição   | Métrica   | Quantidade |
|-------|---|-----------|------------|
| 03.01 | Serviço de Implantação da Solução de Firewalls e Segurança Next Generation Firewall (NGFW)                          | Unitário  | 4          |
| 03.02 | Reconfiguração da Rede: Serviço de Configuração: Switches (10); Access Points (04); Firewalls (02); Roteadores (02) | Unitário  | 10         |
| 03.03 | Implantação da solução de Endpoint Protection EPP/EDR   | Endpoints | 200        |

### 20.4. O item 04.00 Serviços Complementares – Sob Demanda

| Item | Descrição  | Métrica      | Quantidade |
|------|--|--------------|------------|
| 1    | Serviços de Suporte da solução por profissionais especializados (N3) Sob Demanda | Hora técnica | 500        |

## **21. CRITÉRIOS DE MEDIÇÃO**

- 21.1.** Os serviços serão medidos e pagos conforme Planilha de Preços Unitários – PPU, de acordo com o andamento dos trabalhos.
- 21.2.** Todos os demais custos associados, como deslocamentos, estadias, treinamentos, reuniões, SAC, entre outros devem ser considerados no valor global do projeto.

## **22. VISITA TÉCNICA**

- 22.1.** A ES Gás disponibilizará aos licitantes visita técnica com o objetivo de apresentar o ambiente operacional e os principais sistemas que serão integrados à solução contratada.
- 22.2.** A licitante poderá realizar visita técnica e obter, para sua própria utilização, por sua exclusiva responsabilidade, conta e risco, toda a informação necessária para elaboração de sua proposta e eventual execução do contrato.
- 22.3.** Todos os custos associados com a visita presencial, assim como quaisquer outras despesas com a elaboração da proposta, serão arcados pela licitante. A licitante que optar pela vistoria presencial deverá agendar data e horário junto à Coordenação de TI da ES Gás por meio do telefone (27) 3347 8974 ou e-mail [flavio.pires@esgas.com.br](mailto:flavio.pires@esgas.com.br).
- 22.4.** A visita técnica poderá ser realizada até o terceiro dia útil anterior à data de abertura das propostas.
- 22.5.** Após a realização de visita técnica, a licitante receberá uma declaração de realização do procedimento devidamente assinada pelo responsável por seu acompanhamento.

## **23. CONDIÇÕES DE PAGAMENTO**

- 23.1.** Os valores referentes à Aquisição de Equipamentos: - CAPEX, serão pagos conforme política, vigente, da CONTRANTE.

- 23.2.** O valor a ser pago pelo CONTRATANTE à CONTRATADA pelos itens relativos aos serviços prestados, terá seu consumo apurado mensalmente, de acordo com a utilização mensurada na Planilha de Preços Unitários condicionada ao aceite da equipe técnica da ES Gás.
- 23.3.** Os valores devidos, OPEX, serão pagos até o dia 30 do mês subsequente, mediante a apresentação dos competentes Documentos de Cobrança (Nota Fiscal/Fatura), acompanhados dos documentos de comprovação de regularidade fiscal, boletim de medição e relatório mensal de gastos, devidamente aprovado pela área técnica do CONTRATANTE.
- 23.4.** A CONTRATADA deverá encaminhar o relatório mensal até o 5º (quinto) dia útil de cada mês, com o detalhamento de consumo dos serviços e dos impostos devidos, para aprovação pela área técnica do CONTRATANTE antes do envio do respectivo Documento de Cobrança para pagamento.
- 23.5.** A área técnica do CONTRATANTE analisará o relatório e terá o prazo de até 3 (três) dias úteis para aprová-lo ou manifestar a recusa.
- 23.6.** Os documentos de cobrança somente poderão ser emitidos pela CONTRATADA e entregues ao CONTRATANTE para pagamento após a aprovação do boletim de medição e relatório de consumo mensal pela área técnica do CONTRATANTE.
- 23.7.** As informações constantes dos documentos de cobrança deverão ser as mesmas consignadas neste Instrumento, sem o que não será liberado o respectivo pagamento.
- 23.8.** O pagamento será efetuado preferencialmente por meio de boleto, ou na sua falta, através de depósito bancário, em banco, agência e conta corrente indicados pela CONTRATADA, observando-se a situação tributária desta, obedecidas as disposições legais vigentes.
- 23.9.** O competente Documento Fiscal para pagamento do objeto deve ser emitido no mês seguinte ao da prestação do serviço e encaminhado ao CONTRATANTE, no máximo, até o dia 15 (quinze) do mês de emissão, observando-se os dados do local da prestação do serviço para fins de faturamento.

- 23.10.** Os valores devem ser especificados separadamente nos Documentos Fiscais, não sendo aceitas informações de valores globais.
- 23.11.** Nos documentos de cobrança deverão ser indicados, obrigatoriamente, o número deste CONTRATO e os dados bancários para fins de pagamento (banco, agência e conta corrente), viabilizando, assim, a devida quitação.
- 23.12.** Se os documentos de cobrança apresentarem quaisquer divergências com relação a dados ou valores estabelecidos neste CONTRATO, a CONTRATADA terá o prazo de até 3 (três) dias úteis para proceder à sua substituição, prorrogando-se, igualmente, o prazo para pagamento pelo CONTRATANTE.
- 23.13.** O CONTRATANTE não se responsabilizará por quaisquer atrasos no pagamento quando decorrentes de falhas por parte da CONTRATADA no atendimento ao previsto em qualquer das cláusulas do presente CONTRATO.
- 23.14.** Os valores porventura devidos pela CONTRATADA ao CONTRATANTE, provenientes de possíveis penalidades a ela aplicadas ou quaisquer outros débitos atribuídos à sua responsabilidade em decorrência deste CONTRATO, serão deduzidos de eventuais créditos daquela junto a este, respeitado, no entanto, seu direito ao contraditório e à ampla defesa.
- 23.15.** A CONTRATADA deve garantir a qualidade de todos os equipamentos e serviços entregues, por exemplo: SISTEMAS aderentes às especificações e sem erros de codificação.
- 23.16.** A CONTRATADA deve garantir a constante atualização tecnológica de seus funcionários, mantendo-os sempre capacitados, certificados e reciclados nas tecnologias em uso, bem como em boas práticas na área segurança da informação.

## **24. GARANTIA**

- 24.1.** A CONTRATADA deverá oferecer garantia total aos equipamentos adquiridos neste objeto em 24 meses.
- 24.2.** A GARANTIA compreende desde a reposição de peças até a substituição do equipamento na hipótese de apresentar sucessivos defeitos.
- 24.3.** Em caso de indisponibilidade total de qualquer um dos equipamentos, será aceito o tempo máximo de 24 horas corridas para que a CONTRATADA efetue a substituição ou reparo do equipamento defeituoso.
- 24.4.** Entende-se como sucessivos defeitos aqueles:
- 24.4.1. problemas de natureza distinta que ocorrerem três vezes durante o ano.
  - 24.4.2. problemas de mesma natureza que ocorrerem duas vezes num período de 6 meses.
- 24.5.** A garantia para os serviços prestados será obrigatória e seu prazo será de 90 dias, a contar da data de assinatura do Termo de Recebimento Definitivo dos serviços pela ES Gás.
- 24.6.** Durante o prazo de garantia, todos os eventuais erros ou falhas identificados deverão ser corrigidos pela CONTRATADA, sem ônus para a ES Gás.
- 24.7.** Os vícios ocultos, identificados após a entrega de dado módulo ou a finalização do contrato deverão ser sanados pela CONTRATADA, sem ônus para a ES Gás.
- 24.8.** O prazo de garantia deverá ser respeitado pela CONTRATADA mesmo após o término do prazo de vigência do contrato.
- 24.9.** Funcionalidades desenvolvidas ou ajustadas pela CONTRATADA serão mantidas por ela no escopo do suporte técnico.

## **25. MECANISMOS FORMAIS DE COMUNICAÇÃO**

- 25.1.** Os serviços serão solicitados por meio de chamado técnico ou por meio de contato direto ao serviço de suporte avançado especializado nível 3. No final de cada atendimento deverá ser emitido e enviado para a TI da ES Gás o relatório de atendimento técnico, ou ordem de serviço (OS) do atendimento realizado.
- 25.2.** Os documentos de gestão a serem utilizados na execução e de serviços sob demanda serão definidos conforme Metodologia de Trabalho e estão sujeitos a aprovação e controle pela equipe da ES Gás.
- 25.3.** Toda execução dos serviços especializados sob demanda de responsabilidade da CONTRATADA, deverão ser administrados pelo Gerente de Projetos, Coordenador Técnico, ou preposto do contrato.
- 25.4.** Caberá ao preposto da CONTRATADA fornecer informações de controle e acompanhamento da execução dos serviços contratados, bem como responsabilizar-se pelo fiel cumprimento dos chamados técnicos.
- 25.5.** O preposto da CONTRATADA deverá coordenar as atividades necessárias ao atendimento das demandas primando pela qualidade dos serviços prestados.

## **26. ACEITE, ALTERAÇÃO E CANCELAMENTO**

- 26.1.** A ES Gás efetuará o recebimento do objeto contratado, provisoriamente, para efeito de posterior verificação da conformidade do objeto com a especificação, e definitivamente, após a verificação da qualidade e quantidade do objeto de acordo com o contrato.
- 26.2.** Em caso de rejeição total/parcial do objeto contratado, substituição ou demais hipóteses de descumprimento de outras obrigações contratuais, avaliadas na etapa de recebimento, sujeitarão a CONTRATADA à aplicação das sanções administrativas cabíveis.
- 26.3.** Recebimento Provisório:
- 26.4.** A ES Gás receberá provisoriamente o objeto contratado, mediante emissão de termo circunstanciado assinado pelas partes, em até 5 (cinco) dias úteis após a entrega do objeto.



**26.5.** O recebimento provisório caberá ao gestor do contrato especialmente designado para acompanhamento e fiscalização do contrato decorrente desta proposição.

**26.6. Recebimento Definitivo:**

25.6.1. A ES Gás efetuará o recebimento definitivo do objeto contratado após a verificação da qualidade e quantidade do objeto fornecido e se atende aos requisitos estabelecidos no contrato.

25.6.2. Ocorrendo problemas durante a execução desta etapa, eles serão informados à CONTRATADA, que deverá providenciar a correção do problema, promovendo a substituição dos itens identificados, que fazem parte da contratação.

25.6.3. Uma vez verificado o funcionamento do item contratado e entregue, com os termos contratuais, a ES Gás efetuará o recebimento definitivo, mediante emissão de termo circunstanciado, em até 10 (dez) dias úteis após a emissão do termo de recebimento provisório.

25.6.4. O recebimento definitivo caberá ao usuário final, ao coordenador de projetos da área a ser validada e o gestor do contrato especialmente designado para acompanhamento e fiscalização do contrato decorrente desta proposição.

25.6.5. O objeto contratado será rejeitado caso esteja em desacordo com as especificações constantes deste Memorial Descritivo, devendo a ES Gás apontar, por escrito, esta ocorrência, onde detalhará as razões para deixar de emitir o termo de recebimento definitivo e indicará as falhas e pendências verificadas.

25.6.6. O recebimento definitivo do objeto não exclui nem reduz a responsabilidade da CONTRATADA com relação ao funcionamento e configurações divergentes do especificado, durante todo o seu período de garantia.

25.6.7. O recebimento definitivo é condição indispensável para o pagamento da Ordem de Serviço.

## **27. ANEXOS**

Anexo I – Planilha de Preços Unitários – PPU.

Anexo II – Diagramas de Rede por Localidade.