



## TERMO DE REFERÊNCIA

### 1. INTRODUÇÃO

#### 1.1. CONSIDERAÇÕES INICIAIS

1.2. Este termo de referência tem por objetivos:

- a) Caracterizar o objeto a ser contratado;
- b) Estabelecer método de planejamento gerencial das atividades;
- c) Estabelecer nível de qualidade desejado para a aquisição;
- d) Estabelecer os critérios de entrega, pagamento e demais condições a serem observadas durante o cumprimento do Contrato.

### 2. DO OBJETO.

2.1. O presente Termo de Referência tem por objetivo a **CONTRATAÇÃO DE SOLUÇÃO DE SEGURANÇA DA INFORMAÇÃO, INCLUINDO A LOCAÇÃO DE 1 (UM) EQUIPAMENTO FIREWALL DE PRÓXIMA GERAÇÃO (NEXT GENERATION FIREWALL – NGFW), ACOMPANHADO DE SUPORTE TÉCNICO ESPECIALIZADO E LICENCIAMENTO COMPLETO POR 5 (CINCO) ANOS, A SER UTILIZADO NA INFRAESTRUTURA DE REDE DO CONSÓRCIO PÚBLICO DA REGIÃO POLINORTE – CIM POLINORTE**, nas condições, quantidades, características e prazo abaixo definidos.

### 3. DA JUSTIFICATIVA E OBJETIVO DA CONTRATAÇÃO.

3.1. A necessidade da **CONTRATAÇÃO DE SOLUÇÃO DE SEGURANÇA DA INFORMAÇÃO, INCLUINDO A LOCAÇÃO DE 1 (UM) EQUIPAMENTO FIREWALL DE PRÓXIMA GERAÇÃO (NEXT GENERATION FIREWALL – NGFW), ACOMPANHADO DE SUPORTE TÉCNICO ESPECIALIZADO E LICENCIAMENTO COMPLETO POR 5 (CINCO) ANOS, A SER UTILIZADO NA INFRAESTRUTURA DE REDE DO CONSÓRCIO PÚBLICO DA REGIÃO POLINORTE – CIM POLINORTE**, é **proteger redes e dispositivos contra acessos não autorizados e tráfego malicioso**, atuando como um porteiro digital que filtra pacotes de dados, bloqueando ameaças (vírus, hackers) e impedindo a saída de dados sensíveis, sendo essencial para a segurança cibernética, privacidade e integridade de informações em ambientes pessoais e corporativos.

3.2. Após pesquisa no mercado identificamos que firewall pode ser tanto um sistema quanto um equipamento, ou até mesmo uma combinação de ambos. Um **firewall** é um sistema de segurança de rede que monitora e controla o tráfego de dados de entrada e saída, agindo como uma barreira entre uma rede interna confiável (como sua casa ou escritório) e redes externas não confiáveis (como a internet), bloqueando acessos não autorizados e ameaças com base em regras predefinidas, podendo ser de hardware, software ou ambos. Ele filtra pacotes de dados, permitindo ou negando a passagem

#### CONSÓRCIO PÚBLICO DA REGIÃO POLINORTE

Alegre, Aracruz, Cariacica, Ibiraçu, Fundão, João Neiva, Linhares, Santa Teresa, São Roque do Canaã, Santa Leopoldina, Sooretama, Rio Bananal e Viana.

Rua: Martins Pescadores, S/N, Bairro Ericina, Ibiraçu – ES – Cep: 29.670-000  
Tel: (27) 98125-0110 / (27) 98125-0143 – <http://www.cimpolinorte.es.gov.br/>



com base em endereços IP, portas ou tipos de programas, protegendo informações sensíveis de visitantes indesejados e ataques cibernéticos.

3.3. Como sistema: Um firewall de software é um aplicativo que protege um único dispositivo, como um computador ou smartphone. Ele pode estar integrado ao sistema operacional ou ser instalado separadamente.

3.4. Como equipamento: Um firewall de hardware é um dispositivo físico dedicado, comum em redes corporativas, que protege uma rede inteira.

3.5. Um firewall para hardware atua como uma solução de gatekeeper e antivírus para seu servidor. Ele fica logo atrás do roteador e pode ser configurado para analisar o tráfego de entrada, filtrando ameaças específicas à medida que elas chegam ao dispositivo.

3.6. Um firewall para hardware é um dispositivo físico muito parecido com um servidor que filtra o tráfego que vai para um computador. Embora um usuário normalmente conecte um cabo de rede diretamente em um computador ou servidor, com um firewall para hardware, o cabo é conectado primeiro ao firewall. O firewall fica entre a rede externa e o servidor, proporcionando uma solução antivírus e uma barreira rígida contra invasões.

3.7. Um firewall para hardware oferece vários benefícios:

- Pode ser usado para controlar com inteligência o tráfego que chega ao seu servidor
- Pode ser configurado com regras específicas para todo o tráfego
- Pode aliviar a carga sobre outros recursos do servidor. Por exemplo, você pode desativar firewalls para software, o que pode liberar a memória e a potência necessária do processador

3.8. Os firewalls para hardware modernos podem examinar dados em ambas as direções. Semelhante ao mecanismo para examinar o tráfego de entrada, o firewall aplica um conjunto de permissões aos dados de saída também. Dessa forma, ele pode capturar dados incorporados na codificação criada para usar seu computador para espalhar código malicioso para outros computadores na internet.

3.9. Vantagens dos firewalls físicos

- Controle de rede de dispositivo único: um único firewall para hardware oferece proteção para cada computador conectado ao servidor, reduzindo o tempo e os recursos necessários para instalar o software em cada computador.
- Atualizações simultâneas e atualizações de proteção para todos os computadores na rede: atualize suas configurações de proteção uma vez e todos os computadores na rede se beneficiam ao mesmo tempo. Isso garante que todos os dispositivos estejam protegidos contra comprometimento e evita que as equipes de TI atualizem cada computador manualmente, confiando que cada computador estará livre e pronto para uma atualização automática ou confiando que cada usuário tomará as medidas apropriadas para implementar uma atualização.



- Proteção constante: firewalls para hardware permanecem em funcionamento, a menos que você opte por desativá-los. Sem planos de pagamento mensal ou potencial para flutuações na memória do computador ou potência de processamento, não há chance de perder a proteção e expor perigosamente seu servidor.
- Melhor segurança: como os firewalls para hardware têm seu próprio sistema operacional separado, eles são menos propensos a alguns dos ataques que os firewalls de software podem sofrer quando um computador é comprometido.
- Prevenção contra ameaças de alcançar unidades internas: proteja todas as facetas do seu computador contra invasões potencialmente prejudiciais e caras. Uma barreira física entre as unidades internas do seu computador e o código malicioso de entrada interrompe as ameaças antes que elas penetrem no seu computador.
- Os firewalls em hardwares oferecem proteção confiável enquanto economizam memória e capacidade de processamento, tornando-os uma solução poderosa para empresas. Com muitos dispositivos recebendo dados do mesmo servidor, um único firewall físico pode proporcionar segurança valiosa e conveniente para muitos dispositivos ao mesmo tempo, economizando tempo e esforço da equipe de TI.

3.10. Assim conclui-se que a opção de sistema de firewall combinada com hardware é a solução mais segura e economicamente viável para o CIM Polinorte, por não ocupar espaço no servidor de rede e reduzir o trabalho de TI, visto que não temos esse profissional em nosso quadro de pessoal.

#### 4. DO CRITÉRIO DE JULGAMENTO.

4.1. O critério de julgamento será o de MENOR PREÇO GLOBAL, pois trata-se da contratação de um único objeto.

#### 5. DA FUNDAMENTAÇÃO LEGAL.

5.1. Esta contratação observará as normas e procedimentos administrativos constantes no Art. 75 da Lei nº 14.133/21, que dispõe sobre o valor máximo para realizar a Dispensa de Licitação, e também baseada na Lei nº 11.107, de 6 de abril de 2005, que Dispõe sobre normas gerais de contratação de consórcios públicos e dá outras providências.

5.2. Vale ressaltar que os valores máximos previstos na Lei 14.133/21 são duplicados para contratações realizadas por consórcio público. Assim, este consórcio público poderá utilizará como limites os valores inferiores a R\$ 100.000,00 para serviços e compras, previsto no Art. 75 da Lei nº 14.133/21.

#### 6. DAS ESPECIFICAÇÕES E QUANTIDADES

##### CONSÓRCIO PÚBLICO DA REGIÃO POLINORTE

Alegre, Aracruz, Cariacica, Ibirapu, Fundão, João Neiva, Linhares, Santa Teresa, São Roque do Canaã, Santa Leopoldina, Sooretama, Rio Bananal e Viana.

Rua: Martins Pescadores, S/N, Bairro Ericina, Ibirapu – ES – Cep: 29.670-000  
Tel: (27) 98125-0110 / (27) 98125-0143 – <http://www.cimpolinorte.es.gov.br/>



6.1 A demanda em questão se trata do FORNECIMENTO DE SOLUÇÃO DE SEGURANÇA DA INFORMAÇÃO, portanto, refere-se à contratação de serviço de natureza contínua, estima-se que será necessária a contratação por 12 meses consecutivos.

ITEM	DESCRIÇÃO	UND DE MEDIDA	QUANT.
01	FORNECIMENTO DE SOLUÇÃO DE SEGURANÇA DA INFORMAÇÃO, INCLUINDO A LOCAÇÃO DE 1 (UM) EQUIPAMENTO FIREWALL DE PRÓXIMA GERAÇÃO (NEXT GENERATION FIREWALL – NGFW), ACOMPANHADO DE SUPORTE TÉCNICO ESPECIALIZADO E LICENCIAMENTO COMPLETO POR 5 (CINCO) ANOS, A SER UTILIZADO NA INFRAESTRUTURA DE REDE DO CONSÓRCIO PÚBLICO DA REGIÃO POLINORTE – CIM POLINORTE	MÊS	12

## 7. DA DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

7.1. O serviço será prestado mensalmente e deverá ser executado na Sede da Contratada, localizada na Rua Martins Pescadores, S/N, Bairro Ericina, Ibiraçu/ES, CEP: 29.670-000.

### 7.2. CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DO FIREWALL

- Deve suportar, no mínimo, 27 (vinte e sete) Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote;
- Deve suportar, no mínimo, 3 (tres) milhões de conexões simultâneas;
- Deve suportar, no mínimo, 124.000 (cento e vinte quatro mil) novas conexões por segundo;
- Deve Suportar, no mínimo, 25 (vinte e cinco) Gbps de throughput VPN IPSec;
- Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 200 (duzentos) túneis de VPN IPSEC Site-to-Site simultâneos;
- Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 2.500 (dois mil e quinhentos) túneis de clientes VPN IPSEC simultâneos;
- Deve suportar, no mínimo, 4,5 (quatro vírgula cinco) Gbps de throughput de IPS;
- Deve suportar, no mínimo, 2,6 (dois vírgula seis) Gbps throughput de Inspeção SSL;
- Deve suportar, no mínimo, 2,2 (dois vírgula dois) Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS e AntiMalware.

#### CONSÓRCIO PÚBLICO DA REGIÃO POLINORTE

Alegre, Aracruz, Cariacica, Ibiraçu, Fundão, João Neiva, Linhares, Santa Teresa, São Roque do Canaã, Santa Leopoldina, Sooretama, Rio Bananal e Viana.

Rua: Martins Pescadores, S/N, Bairro Ericina, Ibiraçu – ES – Cep: 29.670-000  
Tel: (27) 98125-0110 / (27) 98125-0143 – <http://www.cimpolinorte.es.gov.br/>



- Deve possuir, pelo menos, 8 (oito) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;
- Deve possuir, pelo menos, 2 (duas) interfaces com suporte a conectores SFP+ de 10 Gigabit Ethernet;
- Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para gerenciamento;
- Deve estar homologado pela ANATEL.

## 7.2. Características gerais para os equipamentos de NGFW

A solução deve consistir em plataforma de proteção de rede baseada em appliance físico com funcionalidades de Next Generation Firewall (NGFW), não sendo permitido appliances virtuais ou solução open source (produto montado);

Todos os equipamentos NGFW devem ser do mesmo fabricante para garantir compatibilidade com a gestão centralizada;

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

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

O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

Para telnet e ssh, deve haver opção de configurar a interface de origem ao executar o acesso remoto;

Os dispositivos de proteção de rede devem possuir suporte a Vlans;

Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

Deve suportar BGP, OSPF, RIP e roteamento estático;

Para BGP (IPv4 e IPv6), deve suportar o anúncio apenas quando determinadas condições forem atendidas;

Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;

Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;

Deve suportar DHCP em IPv4 e IPv6;

### CONSÓRCIO PÚBLICO DA REGIÃO POLINORTE

Alegre, Aracruz, Cariacica, Ibirapu, Fundão, João Neiva, Linhares, Santa Teresa, São Roque do Canaã, Santa Leopoldina, Sooretama, Rio Bananal e Viana.

Rua: Martins Pescadores, S/N, Bairro Ericina, Ibirapu – ES – Cep: 29.670-000  
Tel: (27) 98125-0110 / (27) 98125-0143 – <http://www.cimpolinorte.es.gov.br/>



- Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
- Deve suportar tabelas independentes de roteamento, por contexto de firewall;
- Deve suportar NAT dinâmico (Many-to-Many);
- Deve suportar NAT estático (1-to-1);
- Deve suportar NAT estático bidirecional 1-to-1;
- Deve suportar Tradução de porta (PAT);
- Deve suportar NAT de Origem;
- Deve suportar NAT de Destino;
- Deve suportar NAT de Origem e NAT de Destino simultaneamente;
- Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
- Deve suportar NAT64;
- Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;
- Enviar log para sistemas de monitoração externos;
- Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;
- Proteção anti-spoofing;
- Deve haver suporte ao protocolo ICAP, inclusive de forma segura (SSL);
- Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
- Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;
- A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs e Tabelas FIB;
- O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;



Controle, inspeção e decriptografia de SSL para tráfego de Saída (Outbound);

A solução deve suportar integração nativa com Let's Encrypt, para obtenção de certificados válidos, de forma automática;

Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;

Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;

A solução de firewall deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXI, Cisco ACI e Kubernetes;

A solução de firewall deve permitir integração com threat feeds externos. Suportar ao menos listas de IPs, hashes de malwares e domínios;

Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via Teams e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;

Deve possuir integração com soluções de NAC, para autenticação SSO no firewall de elementos registrados no NAC e execução de políticas de compliance na VPN;

### 7.3. Políticas

Deverá suportar controles por zonas de segurança;

Deverá suportar controles de políticas por porta e protocolo;

Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;

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

Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);

Controle, inspeção e decriptografia de SSL por política para tráfego de saída (Outbound);

Deve decriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;

#### CONSÓRCIO PÚBLICO DA REGIÃO POLINORTE

Alegre, Aracruz, Cariacica, Ibiraçu, Fundão, João Neiva, Linhares, Santa Teresa, São Roque do Canaã, Santa Leopoldina, Sooretama, Rio Bananal e Viana.

Rua: Martins Pescadores, S/N, Bairro Ericina, Ibiraçu – ES – Cep: 29.670-000  
Tel: (27) 98125-0110 / (27) 98125-0143 – <http://www.cimpolinorte.es.gov.br/>





Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;

Suporte a objetos e regras IPV6;

Suporte a objetos e regras multicast;

Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

#### **7.4. Controle de Aplicações**

Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

Reconhecer pelo menos 3000 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;

Para tráfego criptografado SSL, deve decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação;

Identificar o uso de táticas evasivas via comunicações criptografadas;

Atualizar a base de assinaturas de aplicações automaticamente;

#### **CONSÓRCIO PÚBLICO DA REGIÃO POLINORTE**

Alegre, Aracruz, Cariacica, Ibiraçu, Fundão, João Neiva, Linhares, Santa Teresa, São Roque do Canaã, Santa Leopoldina, Sooretama, Rio Bananal e Viana.

Rua: Martins Pescadores, S/N, Bairro Ericina, Ibiraçu – ES – Cep: 29.670-000  
Tel: (27) 98125-0110 / (27) 98125-0143 – <http://www.cimpolinorte.es.gov.br/>





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

Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;

Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;

O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

Deve alertar o usuário quando uma aplicação for bloqueada;

Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;

Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc);

Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);

Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, vendor e popularidade;

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

Deve permitir forçar o uso de portas específicas para determinadas aplicações;

## 7.5. Prevenção de ameaças

Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;

Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

### CONSÓRCIO PÚBLICO DA REGIÃO POLINORTE

Alegre, Aracruz, Cariacica, Ibirapu, Fundão, João Neiva, Linhares, Santa Teresa, São Roque do Canaã, Santa Leopoldina, Sooretama, Rio Bananal e Viana.

Rua: Martins Pescadores, S/N, Bairro Ericina, Ibirapu – ES – Cep: 29.670-000  
Tel: (27) 98125-0110 / (27) 98125-0143 – <http://www.cimpolinorte.es.gov.br/>



Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e quarentenar IP do atacante por um intervalo de tempo;

As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;

Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

Deve permitir o bloqueio de vulnerabilidades;

Deve permitir o bloqueio de exploits conhecidos;

Deve incluir proteção contra-ataques de negação de serviços;

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

Detectar e bloquear a origem de portscans;

Bloquear ataques efetuados por worms conhecidos;

Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

Possuir assinaturas para bloqueio de ataques de buffer overflow;

Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

Deve permitir ao administrador adicionar um tempo mínimo para que assinaturas de IPS sejam ativadas;

Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, IMAP, SMTP e POP3;

#### **CONSÓRCIO PÚBLICO DA REGIÃO POLINORTE**

Alegre, Aracruz, Cariacica, Ibirapu, Fundão, João Neiva, Linhares, Santa Teresa, São Roque do Canaã, Santa Leopoldina, Sooretama, Rio Bananal e Viana.

Rua: Martins Pescadores, S/N, Bairro Ericina, Ibirapu – ES – Cep: 29.670-000  
Tel: (27) 98125-0110 / (27) 98125-0143 – <http://www.cimpolinorte.es.gov.br/>



Identificar e bloquear comunicação com botnets;

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

Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;

Os eventos devem identificar o país de onde partiu a ameaça;

Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;

Dentre as análises efetuadas, a solução deve suportar antivírus, query na nuvem, emulação de código, sandboxing e verificação de call-back;

A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado;

## 7.6. Filtro de URLs

Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;

Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;



A identificação pela base do Active Directory deve permitir SSO, de forma que os usuários não precisem logar novamente na rede para navegar pelo firewall;

Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

Possuir categorias de URLs previamente definidas pelo fabricante e atualizáveis a qualquer tempo;

Possuir pelo menos 60 categorias de URLs;

Deve possuir a função de exclusão de URLs do bloqueio;

Permitir a customização de página de bloqueio;

Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;

### 7.7. Identificação de usuários

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

Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior;

Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;

Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;

#### CONSÓRCIO PÚBLICO DA REGIÃO POLINORTE

Alegre, Aracruz, Cariacica, Ibiraçu, Fundão, João Neiva, Linhares, Santa Teresa, São Roque do Canaã, Santa Leopoldina, Sooretama, Rio Bananal e Viana.

Rua: Martins Pescadores, S/N, Bairro Ericina, Ibiraçu – ES – Cep: 29.670-000  
Tel: (27) 98125-0110 / (27) 98125-0143 – <http://www.cimpolinorte.es.gov.br/>



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

Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

Deve suportar o envio e recebimento de credenciais via RADIUS;

Deve suportar SAML como método para autenticação na navegação de Internet e para VPN;

### **7.8. Geolocalização**

Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;

Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

### **7.9. VPN Client to Site**

Recurso de VPN Client to Site deve considerado para os equipamentos NFGW dos tipos 4, 5 e Concentrador.

Suportar IPSec VPN;

Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN;

Atribuição de DNS nos clientes remotos de VPN, inclusive com DNS split tunnel;

Suportar autenticação via AD/LDAP, certificado e base de usuários local;

Suportar leitura e verificação de CRL (certificate revocation list);

A VPN SSL deve permitir aos usuários remotos a troca de senha no Active Directory;

A VPN SSL deve permitir a customização da tela em sessões RDP;

O agente de VPN client-to-site deve ser compatível com pelo menos: Windows, Linux e Mac OS;

### **7.10. Recursos Gerais de SD-WAN**

#### **CONSÓRCIO PÚBLICO DA REGIÃO POLINORTE**

Alegre, Aracruz, Cariacica, Ibirapu, Fundão, João Neiva, Linhares, Santa Teresa, São Roque do Canaã, Santa Leopoldina, Sooretama, Rio Bananal e Viana.

Rua: Martins Pescadores, S/N, Bairro Ericina, Ibirapu – ES – Cep: 29.670-000  
Tel: (27) 98125-0110 / (27) 98125-0143 – <http://www.cimpolinorte.es.gov.br/>



A solução de SD-WAN poderá ser entregue no mesmo equipamento do NGFW desde que atenda todos os requisitos solicitados neste certame.

Caso o equipamento de NGFW não atenda os requisitos de SD-WAN, serão aceitas soluções com composição de equipamento específico para SD-WAN desde que atenda todos os quesitos deste certame e tenha os throughputs de rede equivalentes ou superiores aos solicitados pro NGFW.

Todas as funcionalidades e recursos de SD-WAN aqui especificados deverão ser entregues localmente na solução, isto é, o plano de controle em sua totalidade deverá ser local, não sendo aceitas plataformas de SD-WAN baseadas em nuvem.

A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;

Deve ser possível criar políticas que definam os seguintes critérios para match:

1. Endereços de origem;
2. Grupos de usuários;

Endereços de destino;

DSCP;

Aplicação de camada 7 utilizada (O365 Exchange, AWS, Dropbox e etc);

A solução deverá ser capaz de monitorar e identificar falhas mediante a associação de health check, permitindo testes de resposta por ping, http, tcp/udp echo, dns, tcp-connect e twamp;

A solução de SD-WAN deve suportar health check ativo, passivo e misto, com o objetivo de medir latência, jitter e latência de cada caminho, separadamente:

1. Deve suportar ao menos 10 tabelas independentes de roteamento, por firewall;
2. Ativo: criação manual de health check, definindo o destino a ser medido e o protocolo;
3. Passivo: uso do tráfego real para as medições;
4. Misto: Passivo quando há tráfego do usuário e, na ausência dele, chaveamento para o método ativo;



O SD-WAN deverá balancear o tráfego das aplicações entre múltiplos links simultaneamente, inclusive 4G;

A solução deve permitir a configuração e uso de várias interfaces SD-WAN. Cada uma com seus links;

O SD-WAN deverá analisar o tráfego em tempo real e realizar o balanceamento dos pacotes de um mesmo fluxo (sessão) entre múltiplos links simultaneamente;

Deve possuir suporte ao MOS (Mean Opinion Score), para calcular a qualidade de chamadas de voz, considerando jitter, perda de pacote e codec utilizado;

Deverá ser permitida a criação de políticas de roteamento com base nos seguintes critérios: latência, jitter, perda de pacote, banda ocupada ou todos ao mesmo tempo;

A solução de SD-WAN deve possibilitar o uso de túneis VPN dinâmicos, entre pontas remotas, para aplicações sensíveis. Uma vez que as pontas se trocam informações entre si, é feito by-pass do hub;

Deve permitir a segmentação de várias VRFs sobre um único túnel SD-WAN;

Deve permitir a duplicação e deduplicação de pacotes entre dois ou mais links, de forma seletiva, objetivando uma melhor experiência de uso de aplicações de negócio;

A solução deve permitir a definição do roteamento para cada aplicação;

Diversas formas de escolha do link devem estar presentes, incluindo: melhor link, menor custo e definição de níveis máximos de qualidade a serem aceitos para que tais links possam ser utilizados em um determinado roteamento de aplicação;

Deve possibilitar a definição do link de saída para uma aplicação específica;

Deve implementar balanceamento de link por hash do IP de origem;

Deve implementar balanceamento de link por hash do IP de origem e destino;

Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;

Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais; A solução de SD-WAN deve possuir suporte a Policy based routing ou policy based forwarding;

#### **CONSÓRCIO PÚBLICO DA REGIÃO POLINORTE**

Alegre, Aracruz, Cariacica, Ibiraçu, Fundão, João Neiva, Linhares, Santa Teresa, São Roque do Canaã, Santa Leopoldina, Sooretama, Rio Bananal e Viana.

Rua: Martins Pescadores, S/N, Bairro Ericina, Ibiraçu – ES – Cep: 29.670-000  
Tel: (27) 98125-0110 / (27) 98125-0143 – <http://www.cimpolinorte.es.gov.br/>





Para IPv4, deve suportar roteamento estático e dinâmico (BGP e OSPF);

Deve possuir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões. A solução deve realizar os ajustes dinâmicos na relação perda de pacote x envio de pacotes redundantes;

Deve ser possível habilitar o FEC para tráfegos específicos. Ex: apenas para aplicações sensíveis a perda de pacote;

Deve permitir a customização dos timers para detecção de queda de link, bem como tempo necessário para retornar com o link para o balanceamento após restabelecido;

A solução de SD-WAN deve suportar nativamente conectores com clouds públicas. Pelo menos: Azure, AWS e GCP;

Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, Facebook, etc), impactando no bom uso das aplicações de negócio, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de shaping. Dentre as tratativas possíveis, a solução deve contemplar:

Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem, endereço de destino, usuário e grupo de usuários, aplicações e porta;

O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;

O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como Youtube, Facebook etc;

Deve ainda possibilitar a marcação de DSCP, a fim de que essa informação possa ser utilizada ao longo do backbone para fins de reserva de banda;

O QoS deve possibilitar a definição de fila de prioridade;

Além de possibilitar a definição de banda máxima e garantida por aplicação, deve também suportar o match em categorias de URL, IPs de origem e destino, logins e portas;

A capacidade de agendar intervalos de tempo em que as políticas de shaping/QoS serão válidas é mandatória. Ex: regra de controle de banda mais permissivas durante o horário de almoço;

#### **CONSÓRCIO PÚBLICO DA REGIÃO POLINORTE**

Alegre, Aracruz, Cariacica, Ibiraçu, Fundão, João Neiva, Linhares, Santa Teresa, São Roque do Canaã, Santa Leopoldina, Sooretama, Rio Bananal e Viana.

Rua: Martins Pescadores, S/N, Bairro Ericina, Ibiraçu – ES – Cep: 29.670-000  
Tel: (27) 98125-0110 / (27) 98125-0143 – <http://www.cimpolinorte.es.gov.br/>



Deve possibilitar a definição de bandas distintas para download e upload;

A solução de SD-WAN deve prover estatísticas em tempo real a respeito da ocupação de banda (upload e download) e performance do health check (packet loss, jitter e latência);

A solução de SD-WAN deve suportar health check ativo, passivo e misto:

1. Ativo: criação manual de health check, definindo o destino a ser medido e o protocolo;
2. Passivo: uso do tráfego real para as medições;
3. Misto: Passivo quando há tráfego do usuário e, na ausência dele, chaveamento para o método ativo;

A solução de SD-WAN deve suportar IPv6;

Deve possibilitar roteamento distinto a depender do grupo de usuário selecionado na regra de SD-WAN;

Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

O SD-WAN deverá possuir serviço de Firewall Stateful;

A solução SD-WAN deverá fornecer criptografia AES de 128 bits ou AES de 256 bits em sua VPN;

A solução SD-WAN deverá simplificar a implantação de túneis criptografados de site para site;

Deve ser capaz de bloquear acesso às aplicações;

Deve suportar NAT dinâmico bem como NAT de saída;

Deve suportar balanceamento de tráfego por sessão e pacote;

Suportar VPN IPsec Site-to-Site;

A VPN IPSEC deve suportar criptografia 3DES, AES128, AES192 e AES256 (Advanced Encryption Standard);

A VPN IPSEC deve suportar Autenticação MD5, SHA1, SHA256, SHA384 e SHA512;

A VPN IPSEC deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Group 15 até 21 e Group 27 até 31;

A VPN IPSEC deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);

#### **CONSÓRCIO PÚBLICO DA REGIÃO POLINORTE**

Alegre, Aracruz, Cariacica, Ibirapu, Fundão, João Neiva, Linhares, Santa Teresa, São Roque do Canaã, Santa Leopoldina, Sooretama, Rio Bananal e Viana.

Rua: Martins Pescadores, S/N, Bairro Ericina, Ibirapu – ES – Cep: 29.670-000  
Tel: (27) 98125-0110 / (27) 98125-0143 – <http://www.cimpolinorte.es.gov.br/>



A VPN IPSEc deve suportar Autenticação via certificado IKE PKI;

Deve suportar o uso de DDNS, para casos em que uma ou ambas as pontas possuam IPs dinâmicos;

O recurso de DDNS deve suportar IPv4 e IPv6;

Deve suportar VPN dial up, no caso da ponta remota não possui IP estático na WAN;

Deve possuir suporte e estar licenciamento para uso de VRFs, em IPv4 e IPv6;

A solução de SD-WAN pode ser fornecida em composição com o firewall, desde que atenda aos mesmos requisitos de performance.

Essa especificação é o mínimo desejado, sendo aceitas especificações superiores.

## 8. DO PRAZO DE EXECUÇÃO

8.1. A entrega/Instalação do equipamento, bem como o início da execução do serviço dar-se-á no prazo máximo de 15 (quinze) dias consecutivos após o recebimento da Ordem de Fornecimento/Serviço que será expedida pelo CIM Polinorte;

## 9. DO ACOMPANHAMENTO E FISCALIZAÇÃO.

9.1. O CIM POLINORTE designará, formalmente, um servidor para acompanhar a entrega do objeto, conforme este Termo de Referência, bem como para atestar o recebimento provisório e definitivo;

9.2 A execução do contrato acompanhada por um servidor e/ou comissão, previamente designados pelo CIM POLINORTE, para proceder à fiscalização, que deverá atestar o fornecimento, para cumprimento das normas estabelecidas nos arts. 62 e 63 da Lei nº 4.320/1964;

9.3 O fiscal anotará todas as ocorrências relacionadas com a execução do Contrato em registro próprio, determinando o que for necessário à regularização das faltas ou defeitos observados, conforme Termo de Referência;

9.4. As decisões e providências que ultrapassarem a competência da Comissão deverão ser solicitadas a seus superiores em tempo hábil para adoção das medidas convenientes;

9.5. Não obstante a CONTRATADA seja a única e exclusiva responsável por todos os produtos fornecidos, a Administração reserva-se o direito de, sem que de qualquer forma restrinja a plenitude desta responsabilidade, exercer a mais ampla e completa fiscalização sobre os produtos e o serviço de garantia, diretamente ou por prepostos designados;

### CONSÓRCIO PÚBLICO DA REGIÃO POLINORTE

Alegre, Aracruz, Cariacica, Ibirapu, Fundão, João Neiva, Linhares, Santa Teresa, São Roque do Canaã, Santa Leopoldina, Sooretama, Rio Bananal e Viana.

Rua: Martins Pescadores, S/N, Bairro Ericina, Ibirapu – ES – Cep: 29.670-000  
Tel: (27) 98125-0110 / (27) 98125-0143 – <http://www.cimpolinorte.es.gov.br/>



9.6. A fiscalização será exercida no interesse exclusivo do CIM POLINORTE e não exclui nem reduz a responsabilidade da CONTRATADA por qualquer inconsistência.

9.7. A fiscalização será exercida por servidor lotado no CIM POLINORTE, formalmente designado, para o acompanhamento da contratação e entrega dos produtos.

## **10. DO PRAZO DE VIGÊNCIA DO CONTRATO**

10.1. O prazo de vigência do contrato será de 12 (doze) meses, contado do dia posterior à data de sua assinatura e sua eficácia dar-se-á a partir da data de sua publicação resumida na Imprensa Oficial do Estado.

10.2. Conforme o Art. 108 da Lei 14.133/21, a Administração poderá celebrar contratos com prazo de até 10 (dez) anos nas hipóteses previstas nas alíneas “f” e “g” do inciso IV e nos incisos V, VI, XII e XVI do caput do art. 75 desta Lei.

10.3. Os contratos de serviços contínuos poderão ser prorrogados sucessivamente, respeitada a vigência máxima decenal, desde que haja previsão em edital e que a autoridade competente ateste que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com o contratado ou a extinção contratual sem ônus para qualquer das partes.

## **11. DAS CONDIÇÕES E DOS PRAZOS DE PAGAMENTO.**

11.1. Os pagamentos serão efetuados mediante o fornecimento ao CIM POLINORTE de NOTA FISCAL ELETRÔNICA bem como os documentos de regularidade fiscal exigidos para a habilitação no procedimento licitatório. Estes documentos depois de conferidos e visados, serão encaminhados para processamento e pagamento no prazo de 30 (trinta) dias úteis após a respectiva apresentação e ateste definitivo do objeto;

11.2. A Nota fiscal deverá conter todas as informações referente ao número de processo e objeto de contratação, bem como o número da conta bancária para pagamento de despesa.

## **12. DAS OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATADA E CONTRATANTE.**

### **12.1 Compete à Contratada:**

12.1.1. Entregar os materiais de acordo com as condições e prazos propostos;

12.1.2. Providenciar a imediata correção das deficiências apontadas pelo setor competente do Contratante;

### **CONSÓRCIO PÚBLICO DA REGIÃO POLINORTE**

Alegre, Aracruz, Cariacica, Ibirapu, Fundão, João Neiva, Linhares, Santa Teresa, São Roque do Canaã, Santa Leopoldina, Sooretama, Rio Bananal e Viana.

Rua: Martins Pescadores, S/N, Bairro Ericina, Ibirapu – ES – Cep: 29.670-000  
Tel: (27) 98125-0110 / (27) 98125-0143 – <http://www.cimpolinorte.es.gov.br/>



12.1.3. Manter, durante toda a execução do Contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação, conforme dispõe o Art. 62 Lei Nº 14.133/21.

12.1.4. Substituir o produto, quando do surgimento de eventuais defeitos verificados, durante o período da garantia oferecida pelo fabricante, atendendo no prazo máximo de 48 horas as solicitações nesse sentido;

## 12.2. Compete à Contratante:

12.2.1 Efetuar o pagamento à empresa Contratada, em até 30 (trinta) dias após a certificação das Notas Fiscais, de acordo com as condições de preço e pagamento estabelecidos no Termo de Referência.

## 13. DA DOTAÇÃO ORÇAMENTÁRIA

13.1. Os recursos para cobrir as despesas do objeto desta contratação correrão a conta do orçamento próprio deste Consórcio para o exercício financeiro de 2025.

- Projeto/Atividade: 01101.0412200042.012 - MANUTENCAO DE ATIVIDADES DE ADMINISTRAÇÃO DA SEDE DO POLINORTE DO ES.

## 14. DA APRESENTAÇÃO DAS PROPOSTAS.

14.1. Nos preços propostos deverão estar incluídos, além do lucro, todas as despesas e custos, como por exemplo: transportes, tributos de qualquer natureza e todas as despesas, diretas ou indiretas, relacionadas com o fornecimento do objeto da presente licitação.

## 15. DA HABILITAÇÃO

15.1. Encerrada a etapa de cotação de preços, a agente de contratação verificará se a empresa provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no [art. 14 da Lei nº 14.133/2021](#), especialmente quanto à existência de sanção que impeça a participação no certame ou da futura contratação mediante a consulta aos seguintes cadastros:

- a) Cadastro Nacional de Empresas Inidôneas e Suspensas – CEIS, mantido pela Controladoria Geral da União (<http://www.portaltransparencia.gov.br/sancoes/ceis>);
- b) Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça ([www.cnj.jus.br/improbidade\\_adm/consultar\\_requerido.php](http://www.cnj.jus.br/improbidade_adm/consultar_requerido.php)).

### CONSÓRCIO PÚBLICO DA REGIÃO POLINORTE

Alegre, Aracruz, Cariacica, Ibirapu, Fundão, João Neiva, Linhares, Santa Teresa, São Roque do Canaã, Santa Leopoldina, Sooretama, Rio Bananal e Viana.

Rua: Martins Pescadores, S/N, Bairro Ericina, Ibirapu – ES – Cep: 29.670-000  
Tel: (27) 98125-0110 / (27) 98125-0143 – <http://www.cimpolinorte.es.gov.br/>



c) Certidão Negativa de Licitante Inidôneo, expedida pelo Tribunal de Contas da União (<https://contas.tcu.gov.br/ords/f?p=INABILITADO:CERTIDAO:0:>).

d) Cadastro de Fornecedores do Estado do Espírito Santo – CRC/ES (<https://www.siga.es.gov.br/sgc/faces/pub/sgc/tabbasicas/FornecedoresSancionadosPageList.jspx?opcao=todos>).

## 15.2. HABILITAÇÃO JURÍDICA

a) Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial, tratando-se de sociedade empresária;

b) O representante da empresa (representante legal ou procurador) responsável pela assinatura do Contrato, deverá identificar-se apresentando cópia de documento oficial de identificação que contenha foto.

c) Os documentos acima deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

d) Deverá estar prevista no estatuto ou contrato social da licitante a autorização para empreender atividades compatíveis com o objeto desta Licitação.

## 15.3. REGULARIDADE FISCAL, SOCIAL E TRABALHISTA

a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas do Ministério da Fazenda (CNPJ);

b) Prova de inscrição no Cadastro de Contribuintes Estadual (com situação ativa) ou Municipal, relativo ao domicílio ou sede da proponente, pertinente ao seu ramo de atividade e compatível com o objeto do certame.

c) Certidão Conjunta Negativa de Débitos ou Positiva com efeito de Negativa, relativa a Tributos Federais (inclusive às contribuições sociais) e à Dívida Ativa da União;

d) Certidão de regularidade de débito com a Fazenda Estadual expedida pela Secretaria de Estado da Fazenda, da sede ou do domicílio do licitante, ou outra equivalente, na forma da lei;

e) Certidão de regularidade de débito com a Fazenda Municipal da sede ou do domicílio do licitante relativa aos tributos incidentes sobre o objeto desta licitação;

f) Certidão de regularidade de débito para com o Fundo de Garantia por Tempo de Serviço (FGTS);

### CONSÓRCIO PÚBLICO DA REGIÃO POLINORTE

Alegre, Aracruz, Cariacica, Ibirapu, Fundão, João Neiva, Linhares, Santa Teresa, São Roque do Canaã, Santa Leopoldina, Sooretama, Rio Bananal e Viana.

Rua: Martins Pescadores, S/N, Bairro Ericina, Ibirapu – ES – Cep: 29.670-000  
Tel: (27) 98125-0110 / (27) 98125-0143 – <http://www.cimpolinorte.es.gov.br/>



g) Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

h) Caso o licitante seja considerado isento dos tributos municipais relacionados ao objeto licitatório, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda do seu domicílio ou sede, ou outra equivalente, na forma da lei;

i) Declaração de que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7º, XXXIII, da Constituição (Anexo IV);

## 16. DA QUALIFICAÇÃO TÉCNICA.

16.1. A empresa classificada, deverá apresentar junto com a proposta comercial, a ficha técnica respectiva a marca e modelo do equipamento ofertado.

16.2. Será exigida a apresentação de **Atestado (s) de Capacidade Técnica** em nome da empresa licitante, fornecido (s) por empresa, órgãos ou entidades da Administração Pública ou Privada, que comprove (m) a aptidão para o desempenho de atividade pertinente e compatível em características e quantidades indicadas;

16.2.1. O(s) atestado(s) deve(m) ser emitido(s) em papel timbrado da empresa contratante, assinado por seu representante legal, contendo a identificação do nome por extenso, discriminando o teor da contratação e os dados da empresa contratada;

16.2.2. O Consórcio CIM POLINORTE poderá promover diligências para averiguar a veracidade das informações constantes nos documentos apresentados, caso julgue necessário, estando sujeita à inabilitação, a licitante que apresentar documentos em desacordo com as informações obtidas pela Equipe de Pregão, além de incorrer nas sanções previstas na Lei nº 14.133/21.

## 17. DAS PENALIDADES/SANÇÕES ADMINISTRATIVAS

17.1. Comete infração administrativa o fornecedor que cometer quaisquer das infrações previstas no art. 155 da Lei nº 14.133, de 2021, quais sejam:

17.1.1. Dar causa à inexecução parcial deste Termo;

17.1.2. Dar causa à inexecução parcial que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

### CONSÓRCIO PÚBLICO DA REGIÃO POLINORTE

Alegre, Aracruz, Cariacica, Ibiraçu, Fundão, João Neiva, Linhares, Santa Teresa, São Roque do Canaã, Santa Leopoldina, Sooretama, Rio Bananal e Viana.

Rua: Martins Pescadores, S/N, Bairro Ericina, Ibiraçu – ES – Cep: 29.670-000  
Tel: (27) 98125-0110 / (27) 98125-0143 – <http://www.cimpolinorte.es.gov.br/>





17.1.3. Dar causa à inexecução total deste Termo;

17.1.4. Deixar de entregar a documentação exigida para a contratação;

17.1.5. Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

17.1.6. Não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

17.1.7. Ensejar o retardamento da execução ou da entrega do objeto da licitação/ contratação sem motivo justificado;

17.1.8. Apresentar declaração ou documentação falsa exigida para a contratação;

17.1.9. Fraudar a dispensa de licitação ou praticar ato fraudulento na execução do Processo;

17.1.10. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

17.1.11. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os fornecedores, em qualquer momento da dispensa;

17.1.12. Praticar atos ilícitos com vistas a frustrar os objetivos desta contratação;

17.1.13. Serão aplicadas ao responsável pelas infrações administrativas previstas nesta Lei as seguintes sanções:

17.1.13.1. Advertência pela falta do subitem 16.1.1 deste Aviso de Contratação Direta, quando não se justificar a imposição de penalidade mais grave;

17.1.13.2. Multa de 5% (por cento) sobre o valor estimado do (s) item (s) prejudicado (s) pela conduta do fornecedor, por qualquer das infrações dos subitens 16.1.1 a 16.1.12;

17.1.13.3. Declaração de inidoneidade para licitar ou contratar, que impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos;

17.2. Na aplicação das sanções serão considerados:

- a) A natureza e a gravidade da infração cometida;
- b) As peculiaridades do caso concreto;
- c) As circunstâncias agravantes ou atenuantes;

#### CONSÓRCIO PÚBLICO DA REGIÃO POLINORTE

Alegre, Aracruz, Cariacica, Ibirapu, Fundão, João Neiva, Linhares, Santa Teresa, São Roque do Canaã, Santa Leopoldina, Sooretama, Rio Bananal e Viana.

Rua: Martins Pescadores, S/N, Bairro Ericina, Ibirapu – ES – Cep: 29.670-000  
Tel: (27) 98125-0110 / (27) 98125-0143 – <http://www.cimpolinorte.es.gov.br/>



- d) Os danos que dela provierem para a Administração Pública;
- e) A implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

17.3. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor de pagamento eventualmente devido pela Administração ao contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente;

17.4. A aplicação das sanções previstas neste Aviso de Contratação Direta, em hipótese alguma, a obrigação de reparação integral do dano causado à Administração Pública;

17.5. A penalidade de multa pode ser aplicada cumulativamente com as demais sanções;

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

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

17.8. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao fornecedor/adjudicatário, observando-se o procedimento previsto na Lei nº 14.133, de 2021, e subsidiariamente na Lei nº 9.784, de 1999.

## 18. DAS DISPOSIÇÕES FINAIS

18.1. O CONSÓRCIO CIM POLINORTE/ES reserva para si o direito de não aceitar ou receber qualquer serviço em desacordo com o previsto no Termo de Referência, ou em desconformidade com as normas legais ou técnicas pertinentes ao objeto;

18.2. Naquilo que for omissa o presente Termo de Referência, reger-se-á pela lei nº 14.133/21.

### CONSÓRCIO PÚBLICO DA REGIÃO POLINORTE

Alegre, Aracruz, Cariacica, Ibirapu, Fundão, João Neiva, Linhares, Santa Teresa, São Roque do Canaã, Santa Leopoldina, Sooretama, Rio Bananal e Viana.

Rua: Martins Pescadores, S/N, Bairro Ericina, Ibirapu – ES – Cep: 29.670-000  
Tel: (27) 98125-0110 / (27) 98125-0143 – <http://www.cimpolinorte.es.gov.br/>



18.3. A execução dos serviços será efetuada mediante expedição, pelo CONSÓRCIO CIM POLINORTE/ES, da **“Ordem de Fornecimento”**, que deverá conter a identificação do órgão requisitante, indicação expressa dos números do contrato, do processo, do contrato, bem como a identificação da CONTRATADA.

18.4. Fica eleito o Foro da Comarca de Ibiraçu/ES, para dirimir possíveis litígios decorrentes deste procedimento licitatório;

18.5. Quaisquer dúvidas quanto às especificações, favor entrar em contato através do telefone (27) 3257-1772 ou e-mail [cotacao@cimpolinorte.es.gov.br](mailto:cotacao@cimpolinorte.es.gov.br).

## 19. RESPONSÁVEIS PELA ELABORAÇÃO DO TERMO DE REFERÊNCIA

19.1. O presente Termo de Referência foi elaborado por Max Mauro Otoni Laurete Responsável Técnico Contratado - CIM Polinorte.

**Max Mauro Otoni Laurete**  
Responsável Técnico Contratado  
CIM Polinorte

### CONSÓRCIO PÚBLICO DA REGIÃO POLINORTE

Alegre, Aracruz, Cariacica, Ibiraçu, Fundão, João Neiva, Linhares, Santa Teresa, São Roque do Canaã, Santa Leopoldina, Sooretama, Rio Bananal e Viana.

Rua: Martins Pescadores, S/N, Bairro Ericina, Ibiraçu – ES – Cep: 29.670-000  
Tel: (27) 98125-0110 / (27) 98125-0143 – <http://www.cimpolinorte.es.gov.br/>

**CONSÓRCIO PÚBLICO DA REGIÃO POLINORTE**

Alegre, Aracruz, Cariacica, Ibiraçu, Fundão, João Neiva, Linhares, Santa Teresa,  
São Roque do Canaã, Santa Leopoldina, Sooretama, Rio Bananal e Viana.

Rua: Martins Pescadores, S/N, Bairro Ericina, Ibiraçu – ES – Cep: 29.670-000  
Tel: (27) 98125-0110 / (27) 98125-0143 – <http://www.cimpolinorte.es.gov.br/>