TERMO DE REFERÊNCIA OU PROJETO BÁSICO

INTRODUÇÃO

A presente análise tem por objetivo descrever os elementos necessários e suficientes, com nível de precisão adequado, para subsidiar o processo licitatório, demonstrando sua viabilidade e conveniência. Seu conteúdo dependerá da natureza da Solução de TI a ser licitada, sendo mais complexo e minucioso na medida em que a contratação assim exigir. Ele será elaborado com base nas informações constantes do Estudo Técnico preliminar.

1. OBJETO DA CONTRATAÇÃO

A presente licitação tem por objeto o Registro de Preços para contratação de empresa especializada para fornecimento de materiais (elementos de hardware e/ou software) e serviços para a implantação de solução de firewall de próxima geração para a segurança da rede de computadores do IFPI, conforme condições, quantidades e exigências estabelecidas neste instrumento.

2. JUSTIFICATIVA DA CONTRATAÇÃO

Conforme a tecnologia avança, os hackers também avançam e encontram novas maneiras de invadir redes públicas ou privadas para roubar ou sequestrar arquivos e dados pessoais ou corporativos. Os criminosos virtuais atingiram tal ponto de ousadia que chegam a manter estes arquivos reféns até que a pessoa ou corporação pague um resgate pela devolução deles.

Um simples acesso à internet pelos membros do IFPI pode sujeitá-los a riscos de trazerem para a rede local softwares mal-intencionados (malwares) que podem causar interrupção do funcionamento dos computadores e, consequentemente, a interrupção de serviços administrativos executados pelos usuários da rede.

Um sistema de firewall de próxima geração funciona como um filtro eletrônico que examina o tráfego da rede sinalizando quais operações de transmissão e recebimento de dados têm a possibilidade de serem executadas em determinado momento, garantindo a integridade e a segurança dos dados pessoais ou corporativos. Além disso, o firewall evita que os usuários acessem conteúdos ilícitos, protegendo contra ameaças originárias deste tipo de conteúdo.

O firewall de próxima geração, além de impedir que hackers ou softwares

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

mal-intencionados obtenham acesso indevido a uma rede ou computador através da Internet, também impede que um computador propague um software mal-intencionado para outros computadores.

Uma das principais motivações para a execução deste projeto são as ameaças emergentes e muitas vezes direcionadas a ambientes públicos. Tem sido notícia frequente nas mídias, campanhas de ataques do tipo Ransomware a empresas públicas e privadas, que utilizam de uma técnica que criptografa dos dados da vítima, seja servidor ou estação de trabalho, para extorquir financeiramente o alvo solicitando um resgate ou até mesmo fazendo uso indevido das informações ilegalmente obtidas.

Atualmente a solução de firewall do IFPI é muito básica, ou seja, limitada em termos de recursos de identificação de tráfego e tampouco proteção de quaisquer tipos de ameaças que podem vir a causar transtornos ao órgão. Outro ponto a ressaltar é o não atendimento por parte do IFPI ao Marco Civil da Internet. A adequação de um sistema de firewall de próxima geração apresenta-se como ponto crucial para que o Instituto proteja e garanta a integridade da sua rede de dados e de seus usuários.

3. RESULTADOS A SEREM ALCANÇADOS

3.1 Maior visibilidade do tráfego de rede, possibilitando a detecção e proteção em tempo real contra ameaças;

3.2 Controle de utilização da rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;

3.3 Proteção do ambiente de rede contra worms, vírus, malwares entre outras pragas virtuais, atendendo às exigências do Marco Civil da Internet.

3.4 Geração de relatórios dos acessos realizados por IP, grupo ou usuário nas seguintes formas: diário, semanal, mensal ou período selecionado;

3.5 Criação de políticas de proteção da rede de computadores contra ataques de hackers através do bloqueio de programas de compartilhamento de dados (P2P), fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;

3.6 Regras de bloqueio e liberação de portas de serviços TCP e UDP por grupo ou usuário;

3.7 Filtro de conteúdo URL, bloqueando acesso a sites indesejados de conteúdo ilícito e bloqueio de aplicações;

3.8 Administração centralizada de todos os firewalls para melhor gestão de

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

logs e visualização de informações do tráfego da rede (relatórios).

4. ESPECIFICAÇÃO TÉCNICA			
GRUPO	**ITEM**	**DESCRIÇÃO**	**QTD**
1	**1**	**Firewall Virtual tipo 1 com licença de Filtro URL, licenças de proteção contra ameaças conhecidas e desconhecidas e suporte/garantia de 5 anos** **ESPECIFICAÇÕES BÁSICAS** Aquisição de solução de proteção com características de Next Generation Firewall (NGFW) que inclui filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus, spywares e malwares "Zero Day", Filtro de URL, bem como controle de transmissão de dados entre máquinas virtuais e acesso a internet compondo uma plataforma de segurança integrada e robusta para ambientes e datacenters virtualizados. Por plataforma de segurança entende-se appliance virtual de proteção e controle de tráfego compatível com a tecnologia atual de virtualização da instituição (VMware ESXi); **1. CAPACIDADE E QUANTIDADES** 1.1. A plataforma de segurança deve possuir a capacidade e características abaixo ou superior, por appliance virtual: 1.1.1. Suporte a, no mínimo, 600.000 conexões simultâneas; 1.1.2. Suporte a, no mínimo, 15.000 novas conexões por segundo; 1.1.3. Suporte a, no mínimo, 30 (trinta) zonas de segurança; 1.1.4. Estar licenciada para ou suportar sem o uso de licença, 200 (duzentos) clientes de VPN SSL simultâneos; 1.1.5. Estar licenciada para ou suportar sem o uso de licença, 200 (duzentos) túneis de VPN IPSEC simultâneos; 1.2. Por cada appliance virtual que compõe a plataforma de segurança, entende-se o software e as licenças necessárias para o seu funcionamento; 1.3. Por console de gerência e monitoração, entende-se o software e as licenças necessárias para as duas	1

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		funcionalidades; 1.4. Deve ser possível definir interfaces de rede dedicada para gerência do appliance virtual; 1.5. Deve suportar adição de, no mínimo, 2 vCPUs para cada appliance virtual; 1.6. Deve suportar adição de, no mínimo, 8 GB de memória RAM para cada appliance virtual; 1.7. 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. **CARACTERÍSTICAS GERAIS** 1.8. A solução deve consistir de appliance virtual de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), console de gerência e monitoração; 1.9. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões; 1.10. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação; 1.11. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7; 1.12. Os appliances virtuais que executem as funcionalidades de proteção de rede, bem como o console de gerência e monitoração, devem ser do mesmo fabricante; 1.13. O software deverá ser fornecido em sua versão mais atualizada; 1.14. Deve suportar no mínimo 1024 VLANs Tag 802.1q; 1.15. Deve suportar policy based routing ou policy based forwarding; 1.16. Deve suportar roteamento multicast (PIM-SM, PIM-SSM, IGMP v1, v2 e v3); 1.17. Deve suportar DHCP Relay;	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1.18. Deve operar como DHCP Server; 1.19. Deve suportar a criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3; 1.20. O appliance virtual deve ter a capacidade de testar o funcionamento de rotas estáticas e rota default com a definição de um endereço IP de destino que deve estar comunicável através de uma rota. Caso haja falha na comunicação o firewall deve ter a capacidade de usar rota alternativa para estabelecer a comunicação; 1.21. Deve suportar os seguintes tipos de NAT: 1.21.1. Nat dinâmico (Many-to-1); 1.21.2. Nat dinâmico (Many-to-Many); 1.21.3. Nat estático (1-to-1); 1.21.4. NAT estático (Many-to-Many); 1.21.5. Nat estático bidirecional 1-to-1; 1.21.6. Tradução de porta (PAT); 1.21.7. NAT de Origem; 1.21.8. NAT de Destino; 1.21.9. Suportar NAT de Origem e NAT de Destino simultaneamente; 1.21.10. Deve implementar o protocolo ECMP; 1.21.11. Deve implementar balanceamento de link por hash do IP de origem; 1.21.12. Deve implementar balanceamento de link por hash do IP de origem e destino; 1.21.13. Deve implementar balanceamento de link através do método round-robin; 1.21.14. 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, quatro links; 1.21.15. Deve implementar balanceamento de link através de políticas por aplicação e porta de destino ou por serviço e porta de destino; 1.22. Enviar log para sistemas de monitoração externos, simultaneamente; 1.23. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL; 1.24. Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs; 1.25. Deve possuir proteção contra anti-spoofing;	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1.25.1. Deve permitir bloquear sessões TCP que usarem variações do 3-way hand-shake, como 4 way e 5 way split hand-shake, prevenindo desta forma possíveis tráfegos maliciosos; 1.25.2. Dever permitir bloquear conexões que contenham dados no payload de pacotes TCP-SYN e SYN-ACK durante o three-way handshake; 1.25.3. Deve exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver de-criptografia de SSL e SSH; 1.26. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2); 1.26.1. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3); 1.26.2. Suportar a OSPF *graceful restart*; 1.26.3. Deve suportar o protocolo MP-BGP (Multiprotocol BGP) permitindo que o firewall possa anunciar rotas multicast para IPv4 e rotas unicast para IPv6; 1.27. Suportar, no mínimo, as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), NAT64, Identificação de usuários a partir do LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Regras de proteção contra DoS (Denial of Service), De-criptografia SSL e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS e controle de aplicação; 1.28. O appliances virtuais de proteção devem ter a capacidade de operar de forma simultânea mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (l2) e camada 3 (l3); 1.29. Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede; 1.30. Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação; 1.31. Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas; 1.32. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas; 1.33. Suporte a configuração de alta disponibilidade	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		Ativo/Passivo; 1.33.1. Em modo transparente; 1.33.2. Em layer 3; 1.34. A configuração em alta disponibilidade deve sincronizar: 1.34.1. Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede; 1.34.2. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link. 1.35. As funcionalidades de controle de aplicações, VPN IPSec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante. **CARACTERÍSTICAS DE INTEGRAÇÃO COM PLATAFORMA DE VIRTUALIZAÇÃO** 1.36. Segurança e controle de tráfego para ambiente virtualizado deve ser do tipo “host-based”, ou seja, appliance virtual compatível com (VMware ESXi); 1.37. Deve permitir a clonagem (criação de templates), do appliance virtual de forma a suportar automatização do processo de *deployment* de novos appliances dentro de um pool de servidores; 1.38. O *deployment* de novos appliances virtuais deve acompanhar o dinamismo do ambiente virtualizado, ou seja, um novo appliance virtual deve ser criado e configurado automaticamente em novos servidores físicos adicionados ao pool; 1.39. Deve suportar implementação com (standard switch) e (distributed switch); 1.40. Deve controlar o tráfego norte/sul das máquinas virtuais operando como default gateway; 1.41. Deve possuir API aberta que permita integração com tecnologias de orchestração; **CONTROLE POR POLÍTICA DE FIREWALL** 1.42. Deverá suportar controles por zona de segurança. 1.43. Controles de políticas por porta e protocolo.	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1.44. Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações. 1.45. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança. 1.46. Deve suportar a consulta a fontes externas de endereços IP, domínios e URLs podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego de forma automática; 1.47. Deve permitir autenticação segura através de certificado nas fontes externas de endereços IP, domínios e URLs; 1.48. Deve permitir consultar e criar exceção para objetos das listas externas a partir da interface de gerência do próprio firewall; 1.49. Controle de políticas por nome ou código de País (Por exemplo: BR, USA, UK, RUS). 1.50. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound). 1.51. Deve de-criptografar sites e aplicações que utilizam certificados ECC, incluindo Elliptical Curve Digital Signature Algorithm (ECDSA); 1.52. Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2; 1.53. Controle de inspeção e de-criptografia de SSH por política; 1.54. A de-criptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança; 1.55. Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif e reg. 1.56. Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo) 1.57. QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações.	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1.58. Suporte a objetos e regras IPV6. 1.59. Suporte a objetos e regras multicast. 1.60. Deve suportar no mínino três tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão; 1.61. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente. **CONTROLE DE APLICAÇÕES** 1.62. Os appliances virtuais de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades: 1.62.1. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos. 1.62.2. Reconhecer pelo menos 1800 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; 1.62.3. Deve permitir criação de políticas por aplicação aderentes ao negócio da instituição, incluindo, mas não limitado a: 1.62.3.1. Permitir que somente a aplicação SSH seja utilizada pela equipe de suporte baseado em um grupo de usuários do LDAP/AD; 1.62.3.2. Permitir comunicação entre uma máquina virtual (A) e (B) para apenas uma sub-aplicação do Oracle; 1.62.3.3. Permitir que um determinado grupo de usuários do LDAP/AD tenha acesso restrito a uma sub-aplicação customizada do cliente incluída na base de aplicações da solução 1.62.3.4. Permitir que um determinado grupo de usuários do LDAP/AD acesso total a aplicação; 1.62.4. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc; 1.62.5. Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta default ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 389; 1.62.6. Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia proprietária; 1.62.7. 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 ataques mediante a porta 443. 1.62.8. Para tráfego criptografado SSL deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante; 1.62.9. 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, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas; 1.62.10. Deve permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante, incluindo, mas não limitado a Skype. Deve permitir também a criação de políticas de exceção concedendo o acesso a aplicativos como Skype apenas para alguns usuários;	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1.62.11. Deve permitir habilitar aplicações SAAS apenas no modo corporativo e bloqueá-las quando usadas no modo pessoal, tais como: Office 365, Skype, aplicativos google, gmail, etc; 1.62.12. Identificar o uso de táticas evasivas via comunicações criptografadas; 1.62.13. Atualizar a base de assinaturas de aplicações automaticamente; 1.62.14. Reconhecer aplicações em IPv6; 1.62.15. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD; 1.62.16. Os appliances virtuais 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; 1.62.17. Deve ser possível adicionar controle de aplicações em todas as regras de segurança do appliance virtual, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras; 1.62.18. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística; 1.62.19. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas; 1.62.20. 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, mantendo a confidencialidade das aplicações do órgão; 1.62.21. A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos:	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1.62.21.1. HTTP, FTP, SMB, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC, RTSP e File body. 1.62.22. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações; 1.62.23. Deve alertar o usuário quando uma aplicação for bloqueada; 1.62.24. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações; 1.62.25. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/politicas para os mesmos; 1.62.26. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) possuindo granularidade de controle/politicas para os mesmos; 1.62.27. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Gtalk chat e bloquear a transferência de arquivos; 1.62.28. Deve possibilitar a diferenciação de aplicações Proxies (ghostsurf, freegate, etc.) possuindo granularidade de controle/politicas para os mesmos; 1.62.29. Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como: 1.62.29.1. Tecnologia utilizada na aplicações (Client-Server, Browse Based, Network Protocol, etc). 1.62.29.2. Nível de risco da aplicação. 1.62.29.3. Categoria e sub-categoria de aplicações. 1.62.29.4. Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc. **PREVENÇÃO DE AMEAÇAS** 1.63. Para proteção do ambiente contra ataques, os appliances virtuais de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados ou entregue através de composição com outro fabricante. 1.64. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1.65. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante. 1.67.1. Caso o item acima não seja atendido, será aceita carta oficial emitida pelo fabricante garantido a plena funcionalidade da solução por tempo indeterminado, sem nenhum ônus para a CONTRATANTE. 1.66. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo; 1.67. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS e Anti-spyware: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset; 1.68. Deve possuir a capacidade de detectar e prevenir contra ameaças em tráfegos HTTP/2; 1.69. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração; 1.70. Deve suportar granularidade nas politicas de IPS Antivírus e Anti-Spyware, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens. 1.71. Deve permitir o bloqueio de vulnerabilidades. 1.72. Deve permitir o bloqueio de exploits conhecidos. 1.73. Deve incluir proteção contra ataques de negação de serviços. 1.74. Deve suportar a inspeção e criação de regras de proteção de DOS e QOS para o conteúdo de tráfego tunelado pelo protocolo GRE; 1.75. Deverá possuir os seguintes mecanismos de inspeção de IPS: 1.75.1. Análise de padrões de estado de conexões; 1.75.2. Análise de decodificação de protocolo; 1.75.3. Análise para detecção de anomalias de protocolo;	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1.75.4. Análise heurística; 1.75.5. IP Defragmentation; 1.75.6. Remontagem de pacotes de TCP; 1.75.7. Bloqueio de pacotes malformados. 1.76. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc; 1.77. Detectar e bloquear a origem de portscans; com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização; 1.78. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões; 1.79. Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados; 1.80. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS; 1.81. Possuir assinaturas para bloqueio de ataques de buffer overflow; 1.82. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto; 1.83. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e anti-spyware, permitindo a criação de exceções com granularidade nas configurações; 1.84. Permitir o bloqueio de vírus e spywares em, pelo menos os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3; 1.84.1. É permitido uso de software (antivírus de rede), para o bloqueio de vírus e spywares em protocolo SMB de forma a conter malwares se espalhando horizontalmente pela rede; 1.85. Suportar bloqueio de arquivos por tipo; 1.86. Identificar e bloquear comunicação com botnets; 1.87. Deve suportar várias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos);	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1.88. Deve suportar referência cruzada com CVE; 1.89. Registrar no console de monitoração as seguintes informações sobre ameaças identificadas: 1.89.1. O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo appliance virtual; 1.90. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e Antyspyware; 1.91. Deve permitir que na captura de pacotes por assinaturas de IPS e Antispyware seja definido o número de pacotes a serem capturados. Esta captura deve permitir selecionar, no mínimo, 50 pacotes; 1.92. Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos; 1.93. Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3; 1.94. Os eventos devem identificar o país de onde partiu a ameaça; 1.95. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms. 1.96. Proteção contra downloads involuntários usando HTTP de arquivos executáveis maliciosos. 1.97. Rastreamento de vírus em pdf. 1.98. Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.) 1.99. 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 diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança. **ANÁLISE DE MALWARES MODERNOS**	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1.100. Possuir a capacidade de análise de ameaças não conhecidas; 1.101. Devido aos Malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada dever possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante; 1.102. Os appliances virtuais de proteção devem ser capazes de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado; 1.103. Deve possuir a capacidade de diferenciar arquivos analisados em pelo menos duas categorias: malicioso, não malicioso; 1.104. Suportar a análise com pelo menos 100 (cem) tipos de comportamentos maliciosos para a análise da ameaça não conhecida; 1.105. Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows XP, Windows 7 (32 bits) e Windows 7 (64 bits); 1.106. Deve suportar a monitoração de arquivos trafegados na internet (HTTP, FTP, HTTP, SMTP) como também arquivos trafegados internamente nos servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e L3; 1.107. A análise de links em sand-box deve ser capaz de classificar sites falsos na categoria de phishing e atualizar a base de filtro de URL da solução; 1.108. O sistema de análise “In Cloud” ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Anti-spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover informações sobre o usuário infectado (seu endereço ip e seu login de rede); 1.109. O sistema automático de analise "In Cloud" ou	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		local deve emitir relatório com identificação de quais soluções de antivírus existentes no mercado possuem assinaturas para bloquear o malware; 1.110. Deve permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência; 1.111. Deve permitir o download dos malwares identificados a partir da própria interface de gerência; 1.112. Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados; 1.113. Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de malwares de dia zero a partir da própria interface de gerência. **1.114.** Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado; 1.115. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class, Linux (ELF), RAR e 7-ZIP no ambiente de sandbox; 1.116. Deve atualizar a base com assinaturas para bloqueio dos malwares identificados em sand-box com frequência de, pelo menos, 5 minutos. 1.117. Permitir o envio de arquivos e links para análise no ambiente controlado via de forma automática via API. 1.118. Deve permitir o envio para análise em sand-box de malwares bloqueados pelo antivírus da solução; **FILTRO DE URL** 1.119. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL: 1.119.1. 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); 1.119.2. Deve ser possível a criação de politicas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança. 1.119.3. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		integração com serviços de diretório, autenticação via ldap, Active Directory e base de dados local. 1.119.4. Permite popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório; 1.119.5. Suporta a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL; 1.119.6. Deve bloquear o acesso a sites de busca (Google, Bing e Yahoo), caso a opção Safe Search esteja desabilitada. Deve ainda exibir página de bloqueio fornecendo instruções ao usuário de como habilitar a função; 1.119.7. Suporta base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs; 1.119.8. Possui pelo menos 60 categorias de URLs; 1.119.9. A categorização de URL deve analisar toda a URL e não somente até o nível de diretório; 1.119.10. Suporta a criação categorias de URLs customizadas; 1.119.11. Suporta a exclusão de URLs do bloqueio, por categoria; 1.119.12. Permite a customização de página de bloqueio; 1.119.13. Deve proteger contra o roubo de credenciais, usuários e senhas identificadas através da integração com Active Directory submetidos em sites não corporativos. Deve ainda permitir criação de regra onde usuários do Active Directory só possam enviar informações de login para sites autorizados na solução; 1.119.14. Deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas credencias em sites classificados como phishing pelo filtro de URL da solução; 1.119.15. Permite 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 ao usuário continuar acessando o site); 1.119.16. Suporta a inclusão nos logs do produto de informações das atividades dos usuários; 1.119.17. Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For; **IDENTIFICAÇÃO DE USUÁRIOS** 1.120. 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 base de dados local;	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1.121. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários; 1.122. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários; 1.123. Deve implementar a criação de políticas de segurança baseada em atributos específicos do Radius, incluindo, mas não limitado a: baseado no sistema operacional do usuário remoto exigir autenticação padrão Windows e on-time password (OTP) para usuários Android; 1.124. Deve possuir integração com Ldap para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários; 1.124.1.1. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via syslog, para a identificação de endereços IP e usuários; 1.125. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída à internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal); 1.126. Suporte a autenticação Kerberos; 1.127. Deve suportar autenticação via Kerberos para administradores da plataforma de segurança, captive Portal e usuário de VPN SSL; 1.128. Deve possuir suporte à identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços; 1.129. Deve identificar usuários através de leitura do campo x-fowarded-for, populando nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso; 1.130. Deve permitir a criação de políticas de segurança baseadas em usuários de rede com	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		reconhecimento dos mesmos através de leitura do campo x-fowarded-for; 1.131. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD; 1.132. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows. **QOS** 1.133. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming. 1.134. Suportar a criação de políticas de QoS por: 1.134.1. Endereço de origem 1.134.2. Endereço de destino 1.134.3. Por usuário e grupo do LDAP/AD. 1.134.4. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus; 1.134.5. Por porta; 1.135. O QoS deve possibilitar a definição de classes por: 1.135.1. Banda Garantida 1.135.2. Banda Máxima 1.135.3. Fila de Prioridade. 1.136. Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype. 1.137. Suportar marcação de pacotes Diffserv, inclusive por aplicação; 1.138. Deve implementar QOS (traffic-shapping), para pacotes marcados por outros ativos na rede (DSCP). A priorização e limitação do tráfego devem ser efetuadas nos dois sentidos da conexão (inboud e outbound); 1.139. Disponibilizar estatísticas RealTime para classes de QoS.	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1.140. Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário. **FILTRO DE DADOS** 1.141. Permite a criação de filtros para arquivos e dados pré-definidos; 1.142. Os arquivos devem ser identificados por extensão e assinaturas; 1.143. Permite identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (P2P, InstantMessaging, SMB, etc); 1.144. Suportar identificação de arquivos compactados e a aplicação de politicas sobre o conteúdo desses tipos de arquivos; 1.145. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular; 1.146. Permitir listar o número de aplicações suportadas para controle de dados; 1.147. Permitir listar o número de tipos de arquivos suportados para controle de dados; **Geo-localização** 1.148. Suportar a criação de politicas por Geo Localização, permitindo o trafego de determinado Pais/Países sejam bloqueados. 1.149. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos. **VPN** 1.150. Suportar VPN Site-to-Site e Client-to-Site; 1.151. Suportar IPSec VPN; 1.152. Suportar SSL VPN; 1.153. A VPN IPSEc deve suportar:	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1.153.1. 3DES; 1.153.2. Autenticação MD5 e SHA-1; 1.153.3. Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; 1.153.4. Algoritmo Internet Key Exchange (IKEv1 e v2); 1.153.5. AES 128 e 256 (Advanced Encryption Standard) 1.153.6. Autenticação via certificado IKE PKI. 1.154. Deve possuir interoperabilidade com os seguintes fabricantes: 1.154.1. Cisco; 1.154.2. Checkpoint; 1.154.3. Juniper; 1.154.4. Palo Alto Networks; 1.154.5. Fortinet; 1.154.6. Sonic Wall; 1.155. Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de throubleshooting; 1.156. A VPN SSL deve suportar: 1.156.1. Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB; 1.156.2. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente; 1.156.3. Atribuição de endereço IP nos clientes remotos de VPN SSL; 1.156.4. Deve permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL; 1.156.5. Deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário AD/LDAP e grupo de usuário AD/LDAP; 1.156.6. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies; 1.156.7. Atribuição de DNS nos clientes remotos de VPN; 1.156.8. Deve permitir que sejam definidos métodos de autenticação distintos por sistema operacional do dispositivo remoto de VPN (Android, IOS, Mac, Windows); 1.156.9. A solução de VPN deve verificar se o cliente que está conectando é o mesmo para o qual o certificado foi emitido inicialmente. O acesso deve ser bloqueado caso o dispositivo não seja o correto; 1.156.10. Deve haver a opção de ocultar o agente de VPN instalado no cliente remoto, tornando o mesmo invisível para o usuário;	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1.156.11. Deve exibir mensagens de notificação customizada toda vez que um usuário remoto se conectar à VPN. Deve permitir que o usuário desabilite a exibição da mensagem nas conexões seguintes; 1.156.12. Deve avisar ao usuário remoto de VPN quanto a proximidade da expiração de senha LDAP. Deve permitir também a customização da mensagem com informações relevantes para o usuário; 1.156.13. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Anti-spyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL; 1.156.14. A VPN SSL deve suportar proxy arp e uso de interfaces PPPOE; 1.156.15. Suportar autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local; 1.156.16. Deve permitir a distribuição de certificado para o usuário de remoto através do portal de VPN de forma automatizada; 1.156.17. Deve possuir lista de bloqueio para dispositivos em casos quando, por exemplo, o usuário reportar que o dispositivo foi perdido ou roubado; 1.156.18. Permite estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon; 1.156.19. Suporta leitura e verificação de CRL (certificate revocation list); 1.156.20. Permite a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL; 1.156.21. O agente de VPN a ser instalado nos equipamentos desktop e laptops, dever ser capaz de ser distribuído de maneira automática via Microsoft SMS, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN; 1.156.22. O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário, 1.156.23. Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas: 1.156.23.1. Antes do usuário autenticar na estação; 1.156.23.2. Após autenticação do usuário na estação; 1.156.23.3. Sob demanda do usuário; 1.156.24. Deverá manter uma conexão segura com o portal durante a sessão. 1.156.25. O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows XP, Vista	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		Windows 7, Windows 8, Mac OSx; 1.156.26. O portal de VPN deve enviar ao cliente remoto, a lista de gateways de VPN ativos para estabelecimento da conexão, os quais devem poder ser administrados centralmente; 1.156.27. Deve haver a opção do cliente remoto escolher manualmente o gateway de VPN e de forma automática através da melhor rota entre os gateways disponíveis com base no tempo de resposta mais rápido; 1.156.28. Deve possuir a capacidade de identificar se a origem da conexão de VPN é externa ou interna; 1.156.29. O cliente de VPN SSL cliente-to-site também deve suportar dispositivos móveis (IOS e ANDROID); 1.156.30. Deve possuir mecanismos de checagem de conformidade do dispositivo remoto; 1.156.31. Deve ser possível a criação de perfis customizados de conformidade com, no mínimo, as seguintes opções: sistema operacional e patches instalados, antivírus e versão instalada, firewall no host, criptografia do disco, agente de DLP instalado backup de disco, chaves de registros e processos ativos; **Suporte e garantia para a solução de segurança da informação descrita nesta especificação técnica** 1.157. Deve possuir garantia do fabricante no Brasil com validade de 60 (sessenta) meses; 1.158. Durante o prazo de garantia, deve ser possível realizar a atualização de sistema operacional dos equipamentos para obter novas funcionalidades e correção de bugs; 1.159. Os chamados poderão ser abertos diretamente com a contratada ou autorizada oficial do fabricante através de ligação telefônica gratuita (0800) no idioma Português, website e e-mail durante a vigência da garantia (60 meses). O suporte deverá ser na modalidade de 24x7 (24 horas por dia, 7 dias por semana); 1.160. O suporte deverá ter no mínimo o seguinte tempo de resposta para os níveis de severidade abaixo: a. Crítico: Significa que o produto ficou inoperante ou ocorreu falha de grande impacto. Para este nível de severidade o atendimento deve ser imediato e com tempo de resposta de até 1 (uma) hora para resolução total ou encontro de	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		solução temporária de contorno; b. Alta: Impacto moderado no sistema, travamento, ou parada de ambiente parcial. Para este nível de severidade o tempo de resposta deve ser de até 2 (duas) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno; c. Média: Redução de performance do equipamento ou aplicação de solução temporária de contorno bem-sucedida. Para este nível de severidade o tempo de resposta deve ser de até 4 (quatro) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno; d. Baixa: Dúvidas de configuração ou anomalia de baixo impacto. Para este nível de severidade o tempo de resposta deve ser de até 8 (oito) horas em horário comercial.	
	2	**Firewall Virtual tipo 2 com licença de Filtro URL, licenças de proteção contra ameaças conhecidas e desconhecidas e suporte/garantia de 5 anos** **ESPECIFICAÇÕES BÁSICAS** Aquisição de solução de proteção com características de Next Generation Firewall (NGFW) que inclui filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus, spywares e malwares "Zero Day", Filtro de URL, bem como controle de transmissão de dados entre máquinas virtuais e acesso a internet compondo uma plataforma de segurança integrada e robusta para ambientes e datacenters virtualizados; Por plataforma de segurança entende-se appliance virtual de proteção e controle de tráfego compatível com a tecnologia atual de virtualização da instituição (VMware ESXi); **1. CAPACIDADE E QUANTIDADES** 1.1. A plataforma de segurança deve possuir a capacidade e as características abaixo, por appliance virtual: 1.1.1. Suporte a, no mínimo, 200.000 conexões simultâneas; 1.1.2. Suporte a, no mínimo, 10.000 novas conexões por segundo; 1.1.3. Suporte a, no mínimo, 30 (trinta) zonas de segurança; 1.1.4. Estar licenciada para ou suportar sem o uso de licença, 200 (duzentos) clientes de VPN SSL	4

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		simultâneos; 1.1.5. Estar licenciada para ou suportar sem o uso de licença, 300 (trezentos) túneis de VPN IPSEC simultâneos; 1.2. Por cada appliance virtual que compõe a plataforma de segurança, entende-se o software e as licenças necessárias para o seu funcionamento; 1.3. Por console de gerência e monitoração, entende-se o software e as licenças necessárias para as duas funcionalidades; 1.4. Deve ser possível definir interfaces de rede dedicadas para gerência do appliance virtual; 1.5. Deve suportar adição de, no mínimo, 2 vCPUs para cada appliance virtual; 1.6. Deve suportar adição de, no mínimo, 6 GB de memória RAM para cada appliance virtual; 1.7. 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. **CARACTERÍSTICAS GERAIS** 1.8. A solução deve consistir de appliance virtual de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), console de gerência e monitoração; 1.9. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões; 1.10. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação; 1.11. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7; 1.12. Os appliances virtuais que executem as funcionalidades de proteção de rede, bem como a console de gerência e monitoração, devem ser do mesmo fabricante;	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1.13. O software deverá ser fornecido em sua versão mais atualizada; 1.14. Deve suportar 1024 VLANs Tag 802.1q; 1.15. Deve suportar policy based routing ou policy based forwarding; 1.16. Deve suportar roteamento multicast (PIM-SM, PIM-SSM, IGMP v1, v2 e v3); 1.17. Deve suportar DHCP Relay; 1.18. Deve operar como DHCP Server; 1.19. Deve suportar a criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3; 1.20. O appliance virtual deve ter a capacidade de testar o funcionamento de rotas estáticas e rota default com a definição de um endereço IP de destino que deve estar comunicável através de uma rota. Caso haja falha na comunicação o firewall deve ter a capacidade de usar rota alternativa para estabelecer a comunicação; 1.21. Deve suportar os seguintes tipos de NAT: 1.21.1. Nat dinâmico (Many-to-1); 1.21.2. Nat dinâmico (Many-to-Many); 1.21.3. Nat estático (1-to-1); 1.21.4. NAT estático (Many-to-Many); 1.21.5. Nat estático bidirecional 1-to-1; 1.21.6. Tradução de porta (PAT); 1.21.7. NAT de Origem; 1.21.8. NAT de Destino; 1.21.9. Suportar NAT de Origem e NAT de Destino simultaneamente; 1.21.10. Deve implementar o protocolo ECMP; 1.21.11. Deve implementar balanceamento de link por hash do IP de origem; 1.21.12. Deve implementar balanceamento de link por hash do IP de origem e destino; 1.21.13. Deve implementar balanceamento de link através do método round-robin; 1.21.14. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, quatro links; 1.21.15. Deve implementar balanceamento de link através de políticas por aplicação e porta de destino ou por serviço e porta de destino; 1.22. Enviar log para sistemas de monitoração externos, simultaneamente; 1.23. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL; 1.24. Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs; 1.25. Deve possuir proteção contra anti-spoofing; 1.25.1. Deve permitir bloquear sessões TCP que usarem variações do 3-way hand-shake, como 4 way e 5 way split hand-shake, prevenindo desta forma possíveis tráfegos maliciosos; 1.25.2. Dever permitir bloquear conexões que contenham dados no payload de pacotes TCP-SYN e SYN-ACK durante o three-way handshake; 1.25.3. Deve exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver de-criptografia de SSL e SSH; 1.26. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2); 1.26.1. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3); 1.26.2. Suportar a OSPF *graceful restart*; 1.26.3. Deve suportar o protocolo MP-BGP (Multiprotocol BGP) permitindo que o firewall possa anunciar rotas multicast para IPv4 e rotas unicast para IPv6; 1.27. Suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), NAT64, Identificação de usuários a partir do LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Regras de proteção contra DoS (Denial of Service), De-criptografia SSL e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS e controle de aplicação;	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1.28. O appliances virtuais de proteção devem ter a capacidade de operar de forma simultânea mediante o uso de suas interfaces físicas nos seguintes modos: 1.28.1. Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede; 1.28.2. Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação; 1.28.3. Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas; 1.29. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas; 1.30. Suporte a configuração de alta disponibilidade Ativo/Passivo; 1.30.1. Em modo transparente; 1.30.2. Em layer 3; 1.31. A configuração em alta disponibilidade deve sincronizar: 1.31.1. Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede; 1.31.2. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link. 1.32. As funcionalidades de controle de aplicações, VPN IPSec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante. **CARACTERÍSTICAS DE INTEGRAÇÃO COM PLATAFORMA DE VIRTUALIZAÇÃO** 1.33. Segurança e controle de tráfego para ambiente virtualizado deve ser do tipo “host-based”, ou seja, appliance virtual compatível com (VMware ESXi); 1.34. Deve permitir a clonagem (criação de templates), do appliance virtual de forma a suportar automatização do processo de *deployment* de novos appliances dentro de um pool de servidores; 1.35. O *deployment* de novos appliances virtuais deve	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		acompanhar o dinamismo do ambiente virtualizado, ou seja, um novo appliance virtual deve ser criado e configurado automaticamente em novos servidores físicos adicionados ao pool; 1.36. Deve suportar implementação com standard switch e distributed switch; 1.37. Deve controlar o tráfego norte/sul das máquinas virtuais operando como default gateway; 1.38. Deve possuir API aberta que permita integração com tecnologias de orquestração; **CONTROLE POR POLÍTICA DE FIREWALL** 1.39. Deverá suportar controles por zona de segurança. 1.40. Controles de políticas por porta e protocolo. 1.41. Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações. 1.42. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança. 1.43. Deve suportar a consulta a fontes externas de endereços IP, domínios e URLs podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego de forma automática; 1.44. Deve permitir autenticação segura através de certificado nas fontes externas de endereços IP, domínios e URLs; 1.45. Deve permitir consultar e criar exceção para objetos das listas externas a partir da interface de gerência do próprio firewall; 1.46. Controle de políticas por nome ou código de País (Por exemplo: BR, USA, UK, RUS). 1.47. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound). 1.48. Deve de-criptografar sites e aplicações que utilizam certificados ECC, incluindo Elliptical Curve Digital Signature Algorithm (ECDSA);	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1.49. Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2; 1.50. Controle de inspeção e de-criptografia de SSH por política; 1.51. A de-criptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança; 1.52. Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif e reg. 1.53. Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo) 1.54. QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações. 1.55. Suporte a objetos e regras IPV6. 1.56. Suporte a objetos e regras multicast. 1.57. Deve suportar no mínino três tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão; 1.58. Suportar a atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente. **CONTROLE DE APLICAÇÕES** 1.59. Os appliances virtuais de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades: 1.59.1. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos. 1.59.2. Reconhecer pelo menos 1800 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; 1.59.3. Deve permitir criação de políticas por aplicação aderentes ao negócio da instituição, incluindo, mas não limitado a:	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1.59.3.1. Permitir que somente a aplicação SSH seja utilizada pela equipe de suporte baseado em um grupo de usuários do LDAP/AD; 1.59.3.2. Permitir comunicação entre uma máquina virtual (A) e (B) para apenas uma sub-aplicação do Oracle; 1.59.3.3. Permitir que um determinado grupo de usuários do LDAP/AD tenha acesso restrito a uma sub-aplicação customizada do cliente incluída na base de aplicações da solução 1.59.3.4. Permitir que um determinado grupo de usuários do LDAP/AD acesso total a aplicação; 1.59.4. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc; 1.59.5. Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta default ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 389; 1.59.6. Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia proprietária; 1.59.7. 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 ataques mediante a porta 443. 1.59.8. Para tráfego criptografado SSL deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante; 1.59.9. 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, incluindo, mas não	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas; 1.59.10. Deve permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante, incluindo, mas não limitado a Skype. Deve permitir também a criação de políticas de exceção concedendo o acesso a aplicativos como Skype apenas para alguns usuários; 1.59.11. Deve permitir habilitar aplicações SAAS apenas no modo corporativo e bloqueá-las quando usadas no modo pessoal, tais como: Office 365, Skype, aplicativos google, gmail, etc; 1.59.12. Identificar o uso de táticas evasivas via comunicações criptografadas; 1.59.13. Atualizar a base de assinaturas de aplicações automaticamente; 1.59.14. Reconhecer aplicações em IPv6; 1.59.15. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD; 1.59.16. Os appliances virtuais 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; 1.59.17. Deve ser possível adicionar controle de aplicações em todas as regras de segurança do appliance virtual, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras; 1.59.18. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística; 1.59.19. Para manter a segurança da rede eficiente, deve	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas; 1.59.20. 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, mantendo a confidencialidade das aplicações do órgão; 1.59.21. A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos: 1.59.21.1. HTTP, FTP, SMB, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC, RTSP e File body. 1.59.22. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações; 1.59.23. Deve alertar o usuário quando uma aplicação for bloqueada; 1.59.24. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações; 1.59.25. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/políticas para os mesmos; 1.59.26. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) possuindo granularidade de controle/políticas para os mesmos; 1.59.27. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Gtalk chat e bloquear a transferência de arquivos; 1.59.28. Deve possibilitar a diferenciação de aplicações Proxies (ghostsurf, freegate, etc.) possuindo granularidade de controle/políticas para os mesmos; 1.59.29. Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como: 1.59.29.1. Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc). 1.59.29.2. Nível de risco da aplicação. 1.59.29.3. Categoria e sub-categoria de aplicações.	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1.59.29.4. Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc. **PREVENÇÃO DE AMEAÇAS** 1.60. Para proteção do ambiente contra ataques, os appliances virtuais de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados ou entregue através de composição com outro fabricante. 1.61. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware); 1.62. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante. 1.62.1. Caso o item acima não seja atendido, será aceita carta oficial emitida pelo fabricante garantido a plena funcionalidade da solução por tempo indeterminado, sem nenhum ônus para a CONTRATANTE. 1.63. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo; 1.64. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS e Anti-spyware: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset; 1.65. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração; 1.66. Deve suportar granularidade nas políticas de IPS Antivírus e Anti-Spyware, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens. 1.67. Deve permitir o bloqueio de vulnerabilidades. 1.68. Deve permitir o bloqueio de exploits conhecidos. 1.69. Deve incluir proteção contra ataques de negação de serviços.	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1.70. Deve suportar a inspeção e criação de regras de proteção de DOS e QOS para o conteúdo de tráfego tunelado pelo protocolo GRE; 1.71. Deverá possuir os seguintes mecanismos de inspeção de IPS: 1.71.1. Análise de padrões de estado de conexões; 1.71.2. Análise de decodificação de protocolo; 1.71.3. Análise para detecção de anomalias de protocolo; 1.71.4. Análise heurística; 1.71.5. IP Defragmentation; 1.71.6. Remontagem de pacotes de TCP; 1.71.7. Bloqueio de pacotes malformados. 1.72. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc; 1.73. Detectar e bloquear a origem de portscans; com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização; 1.74. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões; 1.75. Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados; 1.76. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS; 1.77. Possuir assinaturas para bloqueio de ataques de buffer overflow; 1.78. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto; 1.79. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e anti-spyware, permitindo a criação de exceções com granularidade nas configurações; 1.80. Permitir o bloqueio de vírus e spywares em, pelo menos os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3; 1.80.1. É permitido uso de software (antivírus de rede), para o bloqueio de vírus e spywares em protocolo SMB	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		de forma a conter malwares se espalhando horizontalmente pela rede; 1.81. Suportar bloqueio de arquivos por tipo; 1.82. Identificar e bloquear comunicação com botnets; 1.83. Deve suportar várias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos); 1.84. Deve suportar referência cruzada com CVE; 1.85. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: 1.85.1. O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo appliance virtual; 1.86. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e Antyspyware; 1.87. Deve permitir que na captura de pacotes por assinaturas de IPS e Antispyware seja definido o número de pacotes a serem capturados. Esta captura deve permitir selecionar, no mínimo, 50 pacotes; 1.88. Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos; 1.89. Os eventos devem identificar o país de onde partiu a ameaça; 1.90. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms. 1.91. Proteção contra downloads involuntários usando HTTP de arquivos executáveis maliciosos. 1.92. Rastreamento de vírus em pdf. 1.93. Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.) 1.94. 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 diferentes de IPS, sendo essas políticas	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		por Usuários, Grupos de usuário, origem, destino, zonas de segurança. **ANÁLISE DE MALWARES MODERNOS** 1.95. Possuir a capacidade de análise de ameaças não conhecidas; 1.96. Devido aos Malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada dever possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante; 1.97. Os appliances virtuais de proteção devem ser capazes de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado; 1.98. Deve possuir a capacidade de diferenciar arquivos analisados em pelo menos duas categorias: malicioso, não malicioso; 1.99. Suportar a análise com pelo menos 100 (cem) tipos de comportamentos maliciosos para a análise da ameaça não conhecida; 1.100. Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows XP, Windows 7 (32 bits) e Windows 7 (64 bits); 1.101. Deve suportar a monitoração de arquivos trafegados na internet (HTTP, FTP, HTTP, SMTP) como também arquivos trafegados internamente nos servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e L3; 1.102. A análise de links em sand-box deve ser capaz de classificar sites falsos na categoria de phishing e atualizar a base de filtro de URL da solução; 1.103. O sistema de análise “In Cloud” ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Anti-spyware	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover informações sobre o usuário infectado (seu endereço ip e seu login de rede); 1.104. O sistema automático de analise "In Cloud" ou local deve emitir relatório com identificação de quais soluções de antivírus existentes no mercado possuem assinaturas para bloquear o malware; 1.105. Deve permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência; 1.106. Deve permitir o download dos malwares indentificados a partir da própria interface de gerência; 1.107. Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados; 1.108. Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de malwares de dia zero a partir da própria interface de gerência. 1.109. Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado; 1.110. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), Linux (ELF), RAR e 7-ZIP no ambiente de sandbox; 1.111. Deve atualizar a base com assinaturas para bloqueio dos malwares identificados em sand-box com frequência de, pelo menos, 5 minutos. 1.112. Permitir o envio de arquivos e links para análise no ambiente controlado via de forma automática via API. 1.113. Deve permitir o envio para análise em sand-box de malwares bloqueados pelo antivírus da solução; **FILTRO DE URL** 1.114. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL: 1.114.1. 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); 1.114.2. Deve ser possível a criação de políticas por	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança. 1.114.3. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via ldap, Active Directory e base de dados local. 1.114.4. Permite popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório; 1.114.5. Suporta a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL; 1.114.6. Deve bloquear o acesso a sites de busca (Google, Bing e Yahoo), caso a opção Safe Search esteja desabilitada. Deve ainda exibir página de bloqueio fornecendo instruções ao usuário de como habilitar a função; 1.114.7. Suporta base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs; 1.114.8. Possui pelo menos 60 categorias de URLs; 1.114.9. A categorização de URL deve analisar toda a URL e não somente até o nível de diretório; 1.114.10. Suporta a criação categorias de URLs customizadas; 1.114.11. Suporta a exclusão de URLs do bloqueio, por categoria; 1.114.12. Permite a customização de página de bloqueio; 1.114.13. Deve proteger contra o roubo de credenciais, usuários e senhas identificadas através da integração com Active Directory submetidos em sites não corporativos. Deve ainda permitir criação de regra onde usuários do Active Directory só possam enviar informações de login para sites autorizados na solução; 1.114.14. Deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas credencias em sites classificados como phishing pelo filtro de URL da solução; 1.114.15. Permite 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 ao usuário continuar acessando o site); 1.114.16. Suporta a inclusão nos logs do produto de informações das atividades dos usuários; 1.114.17. Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For; **IDENTIFICAÇÃO DE USUÁRIOS**	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1.115. 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 base de dados local; 1.116. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários; 1.117. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários; 1.118. Deve implementar a criação de políticas de segurança baseada em atributos específicos do Radius, incluindo, mas não limitado a: baseado no sistema operacional do usuário remoto exigir autenticação padrão Windows e on-time password (OTP) para usuários Android; 1.119. Deve possuir integração com Ldap para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários; 1.120. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via syslog, para a identificação de endereços IP e usuários; 1.121. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída à internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal); 1.122. Suporte a autenticação Kerberos; 1.123. Deve suportar autenticação via Kerberos para administradores da plataforma de segurança, captive Portal e usuário de VPN SSL; 1.124. Deve possuir suporte à identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços; 1.125. Deve identificar usuários através de leitura do	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		campo x-fowarded-for, populando nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso; 1.126. Deve permitir a criação de políticas de segurança baseadas em usuários de rede com reconhecimento dos mesmos através de leitura do campo x-fowarded-for; 1.127. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD; 1.128. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows. **QOS** 1.129. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming. 1.130. Suportar a criação de políticas de QoS por: 1.130.1. Endereço de origem 1.130.2. Endereço de destino 1.130.3. Por usuário e grupo do LDAP/AD. 1.130.4. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus; 1.130.5. Por porta; 1.131. O QoS deve possibilitar a definição de classes por: 1.131.1. Banda Garantida 1.131.2. Banda Máxima 1.131.3. Fila de Prioridade. 1.132. Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype. 1.133. Suportar marcação de pacotes Diffserv, inclusive por aplicação; 1.134. Deve implemetar QOS (traffic-shapping), para	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		pacotes marcados por outros ativos na rede (DSCP). A priorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (inboud e outbound); 1.135. Disponibilizar estatísticas RealTime para classes de QoS. 1.136. Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário. **FILTRO DE DADOS** 1.137. Permite a criação de filtros para arquivos e dados pré-definidos; 1.138. Os arquivos devem ser identificados por extensão e assinaturas; 1.139. Permite identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (P2P, InstantMessaging, SMB, etc); 1.140. Suportar identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos; 1.141. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular; 1.142. Permitir listar o número de aplicações suportadas para controle de dados; 1.143. Permitir listar o número de tipos de arquivos suportados para controle de dados; **Geo-localização** 1.144. Suportar a criação de políticas por Geo Localização, permitindo o trafego de determinado Pais/Países sejam bloqueados. 1.145. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos. **VPN** 1.146. Suportar VPN Site-to-Site e Client-to-Site;	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1.147. Suportar IPSec VPN; 1.148. Suportar SSL VPN; 1.149. A VPN IPSEc deve suportar: 1.149.1. 3DES; 1.149.2. Autenticação MD5 e SHA-1; 1.149.3. Diffie-Hellman Group 1 , Group 2, Group 5 e Group 14; 1.149.4. Algoritmo Internet Key Exchange (IKEv1 e v2); 1.149.5. AES 128 e 256 (Advanced Encryption Standard) 1.149.6. Autenticação via certificado IKE PKI. 1.150. Deve possuir interoperabilidade com os seguintes fabricantes: 1.150.1. Cisco; 1.150.2. Checkpoint; 1.150.3. Juniper; 1.150.4. Palo Alto Networks; 1.150.5. Fortinet; 1.150.6. Sonic Wall; 1.151. Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de throubleshooting; 1.152. A VPN SSL deve suportar: 1.152.1. Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB; 1.152.2. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente; 1.152.3. Atribuição de endereço IP nos clientes remotos de VPN SSL; 1.152.4. Deve permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL; 1.152.5. Deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário AD/LDAP e grupo de usuário AD/LDAP; 1.152.6. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies; 1.152.7. Atribuição de DNS nos clientes remotos de VPN; 1.152.8. Deve permitir que sejam definidos métodos de autenticação distintos por sistema operacional do dispositivo remoto de VPN (Android, IOS, Mac, Windows); 1.152.9. A solução de VPN deve verificar se o client que	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		está conectando é o mesmo para o qual o certificado foi emitido inicialmente. O acesso deve ser bloqueado caso o dispositivo não seja o correto; 1.152.10. Deve haver a opção de ocultar o agente de VPN instalado no cliente remoto, tornando o mesmo invisível para o usuário; 1.152.11. Deve exibir mensagens de notificação customizada toda vez que um usuário remoto se conectar a VPN. Deve permitir que o usuário desabilite a exibição da mensagem nas conexões seguintes; 1.152.12. Deve avisar ao usuário remoto de VPN quanto a proximidade da expiração de senha LDAP. Deve permitir também a customização da mensagem com informações relevantes para o usuário; 1.152.13. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Anti-spyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL; 1.152.14. A VPN SSL deve suportar proxy arp e uso de interfaces PPPOE; 1.152.15. Suportar autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local; 1.152.16. Deve permitir a distribuição de certificado para o usuário de remoto através do portal de VPN de forma automatizada; 1.152.17. Deve possuir lista de bloqueio para dispositivos em casos quando, por exemplo, o usuário reportar que o dispositivo foi perdido ou roubado; 1.152.18. Permite estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon; 1.152.19. Suporta leitura e verificação de CRL (certificate revocation list); 1.152.20. Permite a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL; 1.152.21. O agente de VPN a ser instalado nos equipamentos desktop e laptops, dever ser capaz de ser distribuído de maneira automática via Microsoft SMS, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN; 1.152.22. O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário, 1.152.23. Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas: 1.152.23.1. Antes do usuário autenticar na estação; 1.152.23.2. Após autenticação do usuário na estação;	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1.152.23.3. Sob demanda do usuário; 1.152.24. Deverá manter uma conexão segura com o portal durante a sessão. 1.152.25. O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows XP, Vista Windows 7, Windows 8, Mac OSx; 1.152.26. O portal de VPN deve enviar ao cliente remoto, a lista de gateways de VPN ativos para estabelecimento da conexão, os quais devem poder ser administrados centralmente; 1.152.27. Deve haver a opção do cliente remoto escolher manualmente o gateway de VPN e de forma automática através da melhor rota entre os gateways disponíveis com base no tempo de resposta mais rápido; 1.152.28. Deve possuir a capacidade de identificar se a origem da conexão de VPN é externa ou interna; 1.152.29. O cliente de VPN SSL client-to-site também deve suportar dispositivos móveis (IOS e ANDROID); 1.152.30. Deve possuir mecanismos de checagem de conformidade do dispositivo remoto; 1.152.31. Deve ser possível a criação de perfis customizados de conformidade com, no mínimo, as seguintes opções: sistema operacional e patches instalados, antivírus e versão instalada, firewall no host, criptografia do disco, agente de DLP instalado backup de disco, chaves de registros e processos ativos; **Suporte e garantia para a solução de segurança da informação descrita nesta especificação técnica** 1.153. Deve possuir garantia do fabricante no Brasil com validade de 60 (sessenta) meses; 1.154. Durante o prazo de garantia, deve ser possível realizar a atualização de sistema operacional dos equipamentos para obter novas funcionalidades e correção de bugs; 1.155. Os chamados poderão ser abertos diretamente com a contratada ou autorizada oficial do fabricante através de ligação telefônica gratuita (0800) no idioma Português, website e e-mail durante a vigência da garantia (60 meses). O suporte deverá ser na modalidade de 24x7 (24 horas por dia, 7 dias por semana); 1.156. O suporte deverá ter no mínimo o seguinte tempo de resposta para os níveis de severidade abaixo: a. Crítico: Significa que o produto ficou inoperante ou ocorreu falha de grande impacto. Para este	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		nível de severidade o atendimento deve ser imediato e com tempo de resposta de até 1 (uma) hora para resolução total ou encontro de solução temporária de contorno; b. Alta: Impacto moderado no sistema, travamento, ou parada de ambiente parcial. Para este nível de severidade o tempo de resposta deve ser de até 2 (duas) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno; c. Média: Redução de performance do equipamento ou aplicação de solução temporária de contorno bem-sucedida. Para este nível de severidade o tempo de resposta deve ser de até 4 (quatro) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno; d. Baixa: Dúvidas de configuração ou anomalia de baixo impacto. Para este nível de severidade o tempo de resposta deve ser de até 8 (oito) horas em horário comercial.	
	3	**Firewall tipo 1 com licença de Filtro URL, licenças de proteção contra ameaças conhecidas e desconhecidas e suporte/garantia de 3 anos** **ESPECIFICAÇÕES BÁSICAS** Aquisição de solução de proteção de rede com características de Next Generation Firewall (NGFW) para segurança de informação perimetral que inclui filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus, spywares e malwares "Zero Day", Filtro de URL, bem como controle de transmissão de dados e acesso à internet compondo uma plataforma de segurança integrada e robusta; Por plataforma de segurança entende-se hardware e software integrados do tipo appliance. **1. CAPACIDADE E QUANTIDADES** 1.1. A plataforma de segurança deve possuir a capacidade e as características abaixo, por equipamento: 1.1.1. Throughput de 900 Mbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir; 1.1.2. Throughput de 600 Mbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle	5

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito; 1.1.3. Os throughputs devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, serão considerados inabilitados e sujeitos as sanções previstas em lei; 1.1.4. Os documentos públicos devem comprovar os throughputs aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real (real-word traffic blend); 1.1.5. Não será aceito aceleração de pacotes na placa de rede limitando a análise somente até camada 4. 1.1.6. Suporte a, no mínimo, 120.000 conexões simultâneas; 1.1.7. Suporte a, no mínimo, 5.000 novas conexões por segundo; 1.1.8. Fonte 120/240 AC ou DC; 1.1.9. Disco Solid State Drive (SSD), no mínimo, 240 GB. 1.1.10. No mínimo, 04(quatro) interfaces de rede 10/100/1000 base-TX; 1.1.11. No mínimo,04(quatro) interfaces de rede 1 Gbps SFP; 1.1.12. 1 (uma) interface de rede 1 Gbps dedicada para gerenciamento; 1.1.13. 1 (uma) interface do tipo console ou similar; 1.1.14. Suporte a, no mínimo, 20 (vinte) zonas de segurança; 1.1.15. Estar licenciada para suportar sem o uso de licença, 200 (duzentos) clientes de VPN SSL simultâneos; 1.1.16. Estar licenciada para suportar sem o uso de licença, 200 (duzentos) túneis de VPN IPSEC simultâneos; 1.2. Por cada equipamento que compõe a plataforma de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento; 1.3. Por console de gerência e monitoração, entende-se as	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		licenças de software necessárias para as duas funcionalidades, bem como hardware dedicado para o funcionamento das mesmas; 1.4. O console de gerência e monitoração podem residir no mesmo appliance de proteção de rede, desde que possuam recurso de CPU, memória, interface de rede e sistema operacional dedicados para esta função; 1.5. 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. **CARACTERÍSTICAS GERAIS** 1.6. A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração; 1.7. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões; 1.8. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação; 1.9. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7; 1.10. O hardware e software que executem as funcionalidades de proteção de rede, bem como a console de gerência e monitoração, devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico; 1.11. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19”, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação; 1.12. O software deverá ser fornecido em sua versão mais atualizada; 1.13. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades: 1.13.1. Suporte a 1024 VLAN Tags 802.1q; 1.13.2. Agregação de links 802.3ad e LACP;	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1.13.3. Policy based routing ou policy based forwarding; 1.13.4. Roteamento multicast (PIM-SM); 1.13.5. DHCP Relay; 1.13.6. DHCP Server; 1.13.7. Jumbo Frames; 1.13.8. Suporte a criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3; 1.14. Suportar sub-interfaces ethernet logicas; 1.14.1. Suporte a, no mínimo, 4 (quatro) roteadores virtuais na mesma instancia de firewall; 1.15. O firewall deve ter a capacidade de testar o funcionamento de rotas estáticas e rota default com a definição de um endereço IP de destino que deve estar comunicável através de uma rota. Caso haja falha na comunicação o firewall deve ter a capacidade de usar rota alternativa para estabelecer a comunicação; 1.16. Deve suportar os seguintes tipos de NAT: 1.16.1. Nat dinâmico (Many-to-1); 1.16.2. Nat dinâmico (Many-to-Many); 1.16.3. Nat estático (1-to-1); 1.16.4. NAT estático (Many-to-Many); 1.16.5. Nat estático bidirecional 1-to-1; 1.16.6. Tradução de porta (PAT); 1.16.7. NAT de Origem; 1.16.8. NAT de Destino; 1.16.9. Suportar NAT de Origem e NAT de Destino simultaneamente; 1.16.10. Deve implementar Network Prefix Translation (NPTv6), prevenindo problemas de roteamento assimétrico; 1.16.11. Deve implementar o protocolo ECMP; 1.16.12. Deve implementar balanceamento de link por hash do IP de origem; 1.16.13. Deve implementar balanceamento de link por hash do IP de origem e destino; 1.16.14. Deve implementar balanceamento de link através do método round-robin; 1.16.15. 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, quatro links; 1.16.16. Deve implementar balanceamento de link	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		através de políticas por aplicação e porta de destino ou por serviço e porta de destino; 1.16.17. Deve implementar o protocolo Link Layer Dicovery (LLDP), permitindo que o appliance e outros ativos da rede se comuniquem para identificação da topologia da rede em que estão conectados e a função dos mesmos facilitando o processo de throubleshooting. As informações aprendidas e armazenadas pelo appliance devem ser acessíveis via SNMP; 1.16.18. Enviar log para sistemas de monitoração externos, simultaneamente; 1.16.19. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL; 1.16.20. Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs; 1.16.21. Proteção contra anti-spoofing; 1.16.22. Deve permitir bloquear sessoes TCP que usarem variações do 3-way hand-shake, como 4 way e 5 way split hand-shake, prevenindo desta forma possíveis tráfegos maliciosos; 1.16.23. Dever permitir bloquear conexões que contenham dados no payload de pacotes TCP-SYN e SYN-ACK durante o three-way handshake; 1.16.24. Deve exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver de-criptografia de SSL e SSH; 1.16.25. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2); 1.16.26. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3); 1.16.27. Suportar a OSPF *graceful restart*; 1.16.28. Deve suportar o protocolo MP-BGP (Multiprotocol BGP) permitindo que o firewall possa anunciar rotas multicast para IPv4 e rotas unicast para IPv6; 1.16.29. Suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), NAT64, Identificação de usuários a partir do LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Regras de proteção contra DoS (Denial of Service), De-criptografia SSL e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, IPSEc, VPN SSL, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS, Neighbor Discovery (ND), Recursive DNS Server (RDNSS), DNS Search List (DNSSL) e controle de aplicação; 1.16.30. Os dispositivos de proteção devem ter a	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (l2) e camada 3 (l3); 1.16.30.1. Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede; 1.16.30.2. Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação; 1.16.30.3. Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas; 1.16.31. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas; 1.17. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: 1.17.1. Em modo transparente; 1.17.2. Em layer 3; 1.18. A configuração em alta disponibilidade deve sincronizar: 1.18.1. Sessões; 1.18.2. Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede; 1.18.3. Certificados de-criptografados; 1.18.4. Associações de Segurança das VPNs; 1.18.5. Tabelas FIB; 1.18.6. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link. 1.19. As funcionalidades de controle de aplicações, VPN IPSec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante. **CONTROLE POR POLÍTICA DE FIREWALL** 1.20. Deverá suportar controles por zona de segurança.	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1.21. Controles de políticas por porta e protocolo. 1.22. Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações. 1.23. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança; 1.24. Deve suportar a consulta a fontes externas de endereços IP, domínios e URLs podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego; 1.25. Deve permitir autenticação segura através de certificado nas fontes externas de endereços IP, domínios e URLs; 1.26. Deve permitir consultar e criar exceção para objetos das listas externas a partir da interface de gerência do próprio firewall; 1.27. Controle de políticas por nome ou código de País (Por exemplo: BR, USA, UK, RUS). 1.28. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound). 1.29. Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2; 1.30. Deve de-criptografar sites e aplicações que utilizam certificados ECC, incluindo Elliptical Curve Digital Signature Algorithm (ECDSA); 1.31. Controle de inspeção e de-criptografia de SSH por política; 1.32. A de-criptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança; 1.33. Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg 1.34. Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo) 1.35. QoS baseado em políticas para marcação de	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		pacotes (diffserv marking), inclusive por aplicações. 1.36. Suporte a objetos e regras IPV6. 1.37. Suporte a objetos e regras multicast. 1.38. Deve suportar no mínino três tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão; 1.39. Suportar a atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente. **CONTROLE DE APLICAÇÕES** 1.40. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades: 1.40.1. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos. 1.40.2. Reconhecer pelo menos 1700 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; 1.40.3. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc;- 1.40.4. Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta default ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 389; 1.40.5. Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		proprietária; 1.40.6. 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 ataques mediante a porta 443; 1.40.7. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante; 1.40.8. 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, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas; 1.40.9. Deve permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante, incluindo, mas não limitado a Skype. Deve permitir também a criação de políticas de exceção concedendo o acesso a aplicativos como Skype apenas para alguns usuários; 1.40.10. Deve permitir habilitar aplicações SAAS apenas no modo corporativo e bloqueá-las quando usadas no modo pessoal, tais como: Office 365, Skype, aplicativos google, gmail, etc; 1.40.11. Identificar o uso de táticas evasivas via comunicações criptografadas; 1.40.12. Atualizar a base de assinaturas de aplicações automaticamente; 1.40.13. Reconhecer aplicações em IPv6; 1.40.14. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD; 1.40.15. 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; 1.40.16. Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras; 1.40.17. Deve suportar múltiplos métodos de identificação	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística; 1.40.18. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas; 1.40.19. 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, mantendo a confidencialidade das aplicações do órgão; 1.40.20. A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos: 1.40.20.1. HTTP, FTP, SMB, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC, RTSP e File body. 1.40.21. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações; 1.40.22. Deve alertar o usuário quando uma aplicação for bloqueada; 1.40.23. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações; 1.40.24. Deve permitir criar filtro na tabela de regras de segurança para exibir somente: 1.40.24.1. Regras que permitem passagem de tráfego baseado na porta e não por aplicação, exibindo quais aplicações estão trafegando na mesma, o volume em bytes trafegado por cada a aplicação por, pelo menos, os últimos 30 dias e o primeiro e último registro de log de cada aplicação trafegada por esta determinada regra; 1.40.24.2. Aplicações permitidas em regras de forma desnecessária, pois não há tráfego da mesma na determinada regra; 1.40.24.3. Regras de segurança onde não houve passagem de tráfego nos últimos 90 dias; 1.40.25. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/políticas para os mesmos; 1.40.26. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) possuindo granularidade de controle/políticas para os mesmos; 1.40.27. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Gtalk chat e bloquear a transferência de arquivos; 1.40.28. Deve possibilitar a diferenciação de aplicações	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		Proxies (ghostsurf, freegate, etc.) possuindo granularidade de controle/políticas para os mesmos; 1.40.29. Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como: 1.40.29.1. Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc). 1.40.29.2. Nível de risco da aplicação. 1.40.29.3. Categoria e sub-categoria de aplicações. 1.40.29.4. Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc. **PREVENÇÃO DE AMEAÇAS** 1.41. 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 ou entregue através de composição com outro equipamento ou fabricante. 1.42. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware); 1.43. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante. 1.44. Caso o item acima não seja atendido, será aceita carta oficial emitida pelo fabricante garantido a plena funcionalidade da solução por tempo indeterminado, sem nenhum ônus para a CONTRATANTE. 1.45. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo; 1.46. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS e Antispyware: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset; 1.47. Deve possuir a capacidade de detectar e prevenir contra ameaças em tráfegos HTTP/2; 1.48. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1.49. Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura; 1.50. Deve suportar granularidade nas políticas de IPS Antivírus e Anti-Spyware , possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens. 1.51. Deve permitir o bloqueio de vulnerabilidades. 1.52. Deve permitir o bloqueio de exploits conhecidos. 1.53. Deve incluir proteção contra ataques de negação de serviços. 1.54. Deve suportar a inspeção e criação de regras de proteção de DOS e QOS para o conteúdo de tráfego tunelado pelo protocolo GRE; 1.55. Deverá possuir os seguintes mecanismos de inspeção de IPS: 1.55.1. Análise de padrões de estado de conexões; 1.55.2. Análise de decodificação de protocolo; 1.55.3. Análise para detecção de anomalias de protocolo; 1.55.4. Análise heurística; 1.55.5. IP Defragmentation; 1.55.6. Remontagem de pacotes de TCP; 1.55.7. Bloqueio de pacotes malformados. 1.56. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc; 1.57. Detectar e bloquear a origem de portscans com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização; 1.58. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões; 1.59. Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados; 1.60. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1.61. Possuir assinaturas para bloqueio de ataques de buffer overflow; 1.62. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto; 1.63. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e anti-spyware, permitindo a criação de exceções com granularidade nas configurações; 1.64. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3; 1.64.1. É permitido uso de appliance externo (antivírus de rede), para o bloqueio de vírus e spywares em protocolo SMB de forma a conter malwares se espalhando horizontalmente pela rede; 1.65. Suportar bloqueio de arquivos por tipo; 1.66. Identificar e bloquear comunicação com botnets; 1.67. Deve suportar várias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos); 1.68. Deve suportar referência cruzada com CVE; 1.69. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: 1.69.1. O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo; 1.70. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e Antyspyware; 1.71. Deve permitir que na captura de pacotes por assinaturas de IPS e Antispyware seja definido o número de pacotes a serem capturados. Esta captura deve permitir selecionar, no mínimo, 50 pacotes; 1.72. Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos; 1.73. Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1.74. Os eventos devem identificar o país de onde partiu a ameaça; 1.75. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms. 1.76. Proteção contra downloads involuntários usando HTTP de arquivos executáveis maliciosos. 1.77. Rastreamento de vírus em pdf. 1.78. Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.) 1.79. 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 diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança. **ANÁLISE DE MALWARES MODERNOS** 1.80. Devido aos Malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada dever possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante; 1.81. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado; 1.82. Deve possuir a capacidade de diferenciar arquivos analisados em pelo menos três categorias: malicioso, não malicioso e arquivos não maliciosos, mas com características indesejáveis como softwares que deixa o sistema operacional lento, que alteram parâmetros do sistema, etc.; 1.83. Suportar a análise com pelo menos 100 (cem) tipos de comportamentos maliciosos para a análise da ameaça não conhecida; 1.84. Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		operacional Windows XP, Windows 7 (32 bits) e Windows 7 (64 bits); 1.85. Deve suportar a monitoração de arquivos trafegados na internet (HTTPs, FTP, HTTP, SMTP) como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e L3; 1.86. A análise de links em sand-box deve deve ser capaz de classificar sites falsos na categoria de phishing e atualizar a base de filtro de URL da solução; 1.87. O sistema de análise “In Cloud” ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Anti-spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover informações sobre o usuário infectado (seu endereço ip e seu login de rede); 1.88. O sistema automático de analise "In Cloud" ou local deve emitir relatório com identificação de quais soluções de antivírus existentes no mercado possuem assinaturas para bloquear o malware; 1.89. Deve permitir exportar o resultado das análises de malwares de dia zero em PDF e CSV a partir da própria interface de gerência; 1.90. Deve permitir o download dos malwares identificados a partir da própria interface de gerência; 1.91. Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados; 1.92. Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de malwares de dia Zero a partir da própria interface de gerência. 1.93. Caso a solução seja fornecida em appliance local, deve possuir, no mínimo, 28 ambientes controlados (sand-box) independentes para execução simultânea de arquivos suspeitos; 1.94. Caso seja necessárias licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sand-box), as mesmas devem ser	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		fornecidas em sua totalidade, sem custos adicionais para a contratante; 1.95. Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado; 1.96. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), Linux (ELF), RAR e 7-ZIP no ambiente de sandbox; 1.97. Deve atualizar a base com assinaturas para bloqueio dos malwares identificados em sand-box com frequência de, pelo menos, 5 minutos 1.98. Permitir o envio de arquivos e links para análise no ambiente controlado via de forma automática via API. 1.99. Deve permitir o envio para análise em sand-box de malwares bloqueados pelo antivírus da solução; **FILTRO DE URL** 1.100. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL: 1.100.1. 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); 1.100.2. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança. 1.100.3. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via ldap, Active Directory e base de dados local. 1.100.4. Permite popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório; 1.100.5. Suporta a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL; 1.100.6. Deve bloquear o acesso a sites de busca (Google, Bing e Yahoo), caso a opção Safe Search esteja desabilitada. Deve ainda exibir página de bloqueio fornecendo instruções ao usuário de como habilitar a função; 1.100.7. Suporta base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs; 1.100.8. Possui pelo menos 60 categorias de URLs;	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1.100.9. Deve classificar o nível de risco de URLs em, pelo menos, três níveis: baixo, médio e alto; 1.100.10. Deve possuir categoria especifica para classificar domínios recém registrados (com menos de 30 dias); 1.100.11. A solução deve ter a capacidade de classificar sites em mais de uma categoria, de acordo com a necessidade; 1.100.12. A categorização de URL deve analisar toda a URL e não somente até o nível de diretório; 1.100.13. Suporta a criação categorias de URLs customizadas; 1.100.14. Suporta a exclusão de URLs do bloqueio, por categoria; 1.100.15. Permite a customização de página de bloqueio; 1.100.16. Deve proteger contra o roubo de credenciais, usuários e senhas identificadas através da integração com Active Directory submetidos em sites não corporativos. Deve ainda permitir criação de regra onde usuários do Active Directory só possam enviar informações de login para sites autorizados na solução; 1.100.17. Deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas credencias em sites classificados como phishing pelo filtro de URL da solução; 1.100.18. Permite 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 ao usuário continuar acessando o site); 1.100.19. Suporta a inclusão nos logs do produto de informações das atividades dos usuários; 1.100.20. Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For; **IDENTIFICAÇÃO DE USUÁRIOS** 1.101. 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 base de dados local; 1.102. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários; 1.103. Deve possuir integração com Radius para identificação de usuários e grupos permitindo	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		granularidade de controle/politicas baseadas em usuários e grupos de usuários; 1.104. Deve implementar a criação de políticas de segurança baseada em atributos específicos do Radius, incluindo, mas não limitado a: baseado no sistema operacional do usuário remoto exigir autenticação padrão Windows e on-time password (OTP) para usuários Android; 1.105. Deve possuir integração com Ldap para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários; 1.105.1.1. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via syslog, para a identificação de endereços IP e usuários; 1.106. 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); 1.107. Suporte a autenticação Kerberos; 1.108. Deve suportar autenticação via Kerberos para administradores da plataforma de segurança, captive Portal e usuário de VPN SSL; 1.109. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços; 1.110. Deve identificar usuários através de leitura do campo x-fowarded-for, populando nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso; 1.111. Deve permitir a criação de políticas de segurança baseadas em usuários de rede com reconhecimento dos mesmos através de leitura do campo x-fowarded-for; 1.112. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1.113. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows. **QOS** 1.114. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming. 1.115. Suportar a criação de políticas de QoS por: 1.115.1. Endereço de origem 1.115.2. Endereço de destino 1.115.3. Por usuário e grupo do LDAP/AD. 1.115.4. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus; 1.115.5. Por porta; 1.116. O QoS deve possibilitar a definição de classes por: 1.116.1. Banda Garantida 1.116.2. Banda Máxima 1.116.3. Fila de Prioridade. 1.117. Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype. 1.118. Suportar marcação de pacotes Diffserv, inclusive por aplicação; 1.119. Deve implemetar QoS (traffic-shapping), para pacotes marcados por outros ativos na rede (DSCP). A priorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (inboud e outbound); 1.120. Disponibilizar estatísticas RealTime para classes de QoS. 1.121. Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário. **FILTRO DE DADOS** 1.122. Permite a criação de filtros para arquivos e	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		dados pré-definidos; 1.123. Os arquivos devem ser identificados por extensão e assinaturas; 1.124. Permite identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (P2P, InstantMessaging, SMB, etc); 1.125. Suportar identificação de arquivos compactados e a aplicação de politicas sobre o conteúdo desses tipos de arquivos; 1.126. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular; 1.127. Permitir listar o número de aplicações suportadas para controle de dados; 1.128. Permitir listar o número de tipos de arquivos suportados para controle de dados; **Geo-localização** 1.129. Suportar a criação de politicas por Geo Localização, permitindo o trafego de determinado Pais/Países sejam bloqueados. 1.130. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos. **VPN** 1.131. Suportar VPN Site-to-Site e Client-to-Site; 1.132. Suportar IPSec VPN; 1.133. Suportar SSL VPN; 1.134. A VPN IPSEc deve suportar: 1.134.1. DES e 3DES; 1.134.2. Autenticação MD5 e SHA-1; 1.134.3. Diffie-Hellman Group 1 , Group 2, Group 5 e Group 14; 1.134.4. Algoritmo Internet Key Exchange (IKEv1 e v2); 1.134.5. AES 128 e 256 (Advanced Encryption Standard) 1.134.6. Autenticação via certificado IKE PKI.	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1.135. Deve possuir interoperabilidade com os seguintes fabricantes: 1.135.1. Cisco; 1.135.2. Checkpoint; 1.135.3. Juniper; 1.135.4. Palo Alto Networks; 1.135.5. Fortinet; 1.135.6. Sonic Wall; 1.136. Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de throubleshooting; 1.137. A VPN SSL deve suportar: 1.137.1. O usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB; 1.137.2. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente; 1.137.3. Atribuição de endereço IP nos clientes remotos de VPN SSL; 1.137.4. Deve permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL; 1.137.5. Deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário AD/LDAP e grupo de usuário AD/LDAP; 1.137.6. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies; 1.137.7. Atribuição de DNS nos clientes remotos de VPN; 1.137.8. Deve permitir que seja definido métodos de autenticação distintos por sistema operacional do dispositivo remoto de VPN (Android, IOS, Mac, Windows); 1.137.9. A solução de VPN deve verificar se o client que está conectando é o mesmo para o qual o certificado foi emitido inicialmente. O acesso deve ser bloqueado caso o dispositivo não seja o correto; 1.137.10. Deve possuir lista de bloqueio para dispositivos que forem reportados com roubado ou perdido pelo usuário; 1.137.11. Deve haver a opção de ocultar o agente de VPN instalado no cliente remoto, tornando o mesmo invisível para o usuário; 1.137.12. Deve exibir mensagens de notificação customizada toda vez que um usuário remoto se conectar a VPN. Deve permitir que o usuário desabilite a exibição da mensagem nas conexões	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		seguintes; 1.137.13. Deve avisar ao usuário remoto de VPN quanto a proximidade da expiração de senha LDAP. Deve permitir também a customização da mensagem com informações relevantes para o usuário; 1.137.14. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL; 1.137.15. A VPN SSL deve suportar proxy arp e uso de interfaces PPPOE; 1.137.16. Suportar autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local; 1.137.17. Deve permitir a distribuição de certificado para o usuário de remoto através do portal de VPN de forma automatizada; 1.137.18. Deve possuir lista de bloqueio para dispositivos em casos quando, por exemplo, o usuário reportar que o dispositivo foi perdido ou roubado; 1.137.19. Permite estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon; 1.137.20. Suporta leitura e verificação de CRL (certificate revocation list); 1.137.21. Permite a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL; 1.137.22. O agente de VPN a ser instalado nos equipamentos desktop e laptops, dever ser capaz de ser distribuído de maneira automática via Microsoft SMS, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN; 1.137.23. O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário; 1.137.24. Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas: 1.137.24.1. Antes do usuário autenticar na estação; 1.137.24.2. Após autenticação do usuário na estação; 1.137.24.3. Sob demanda do usuário; 1.137.25. Deve manter uma conexão segura com o portal durante a sessão. 1.137.26. O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows XP, Vista Windows 7, Windows 8, Mac OSx; 1.137.27. O portal de VPN deve enviar ao cliente remoto, a lista de gateways de VPN ativos para estabelecimento da conexão, os quais devem poder	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		ser administrados centralmente; 1.137.28. Deve haver a opção do cliente remoto escolher manualmente o gateway de VPN e de forma automática através da melhor rota entre os gateways disponíveis com base no tempo de resposta mais rápido; 1.137.29. Deve possuir a capacidade de identificar se a origem da conexão de VPN é externa ou interna; **Suporte e garantia para a solução de segurança da informação descrita nesta especificação técnica** 1.138. Deve possuir garantia do fabricante no Brasil com validade de 36 (trinta e seis) meses; 1.139. Durante o prazo de garantia, deve ser possível realizar a atualização de sistema operacional dos equipamentos para obter novas funcionalidades e correção de bugs; 1.140. A garantia deve incluir envio de peças ou equipamentos de reposição nos locais especificados neste edital, obedecendo a modalidade NBD (Next Business Day); 1.141. Os chamados poderão ser abertos diretamente com a contratada ou autorizada oficial do fabricante através de ligação telefônica gratuita (0800) no idioma Português, website e e-mail durante a vigência da garantia (36 meses). O suporte deverá ser na modalidade de 24x7 (24 horas por dia, 7 dias por semana); 1.142. O suporte deverá ter no mínimo o seguinte tempo de resposta para os níveis de severidade abaixo: a. Crítico: Significa que o produto ficou inoperante ou ocorreu falha de grande impacto. Para este nível de severidade o atendimento deve ser imediato e com tempo de resposta de até 1 (uma) hora para resolução total ou encontro de solução temporária de contorno; b. Alta: Impacto moderado no sistema, travamento, ou parada de ambiente parcial. Para este nível de severidade o tempo de resposta deve ser de até 2 (duas) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno; c. Média: Redução de performance do equipamento ou aplicação de solução temporária de contorno bem-sucedida. Para este nível de severidade o tempo de resposta deve ser de até 4 (quatro) horas, em horário comercial, para	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		resolução total ou encontro de solução temporária de contorno; d. Baixa: Dúvidas de configuração ou anomalia de baixo impacto. Para este nível de severidade o tempo de resposta deve ser de até 8 (oito) horas em horário comercial.	
	4	**Software de gestão centralizada para NGFW com suporte/garantia de 3 anos** O software deve atender aos requisitos abaixo: 1.1. Deve possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos. 1.2. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança. 1.3. Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios e funções. 1.4. O gerenciamento centralizado poderá ser entregue como appliance físico ou virtual. Caso seja entregue em appliance fisíco deve ser compatível com rack 19 polegadas e possuir todos acessórios necessários para sua instalação. Caso seja entregue em appliance virtual dever ser compatível com VMware ESXi; 1.5. Deve permitir controle global de políticas para todos os equipamentos que compõe a plataforma de segurança; 1.6. Deve suportar organizar os dispositivos administrados em grupos: os sistemas virtuais devem ser administrados como dispositivos individuais, os grupos podem ser geográficos, por funcionalidade (por exemplo, IPS), e distribuição; 1.7. Deve implementar sistema de hierarquia entre os firewalls gerenciados, onde seja possível aplicar configurações de forma granular em grupos de firewalls; 1.8. Deve implementar a criação de perfis de usuários com acesso à plataforma de gerenciamento com definição exata de quais informações e de quais firewalls e grupos de firewalls o usuário terá acesso referente a logs e relatórios;	1

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1.9. Deve permitir a criação de objetos e políticas compartilhadas; 1.10. Deve consolidar logs e relatórios de todos os dispositivos administrados; 1.11. Deve permitir que exportar backup de configuração automaticamente via agendamento; 1.12. Deve permitir que a configuração dos firewalls seja importada de forma automática na plataforma de gerenciamento centralizado e que possa ser usada em outros firewalls e grupos de firewalls; 1.13. Deve mostrar os status dos firewalls em alta disponibilidade a partir da plataforma de gerenciamento centralizado; 1.14. Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento; 1.15. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta; 1.16. Deve permitir substituir o certificado de fábrica no acesso HTTPS a gerência do firewall como possibilidade de uso de certificado criado localmente na própria solução ou importado de fonte externa; 1.17. Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows ou Linux; 1.18. O gerenciamento deve permitir/possuir: 1.18.1. Criação e administração de políticas de firewall e controle de aplicação; 1.18.2. Criação e administração de políticas de IPS, Antivírus e Anti-Spyware; 1.18.3. Criação e administração de políticas de Filtro de URL; 1.18.4. Monitoração de logs; 1.18.5. Ferramentas de investigação de logs; 1.18.6. Debugging; 1.18.7. Captura de pacotes. 1.19. Acesso concorrente de administradores; 1.20. Deve permitir que administradores concorrentes façam modificações, valide configurações e reverta	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		configurações do firewall simultaneamente e que cada administrador consiga aplicar apenas as suas alterações de forma independente das realizadas por outro administrador; 1.21. Deve mostrar ao administrador do firewall a hora e data do último login e tentativas de login com falha para acessos a partir da interface gráfica e CLI. 1.22. Deve possuir mecanismo de busca global na solução onde possa se consultar por string tais como: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas, endereços IPs, permitindo a localização e uso dos mesmo na configuração do dispositivo; 1.23. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos; 1.24. Deve permitir usar palavras chaves e cores para facilitar identificação de regras; 1.25. Deve permitir monitorar via SNMP falhas de hardware, inserção ou remoção de fontes, discos e coolers, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN cliente-to-site, porcentagem de utilização em referência ao número total suportado/licenciado e número de sessões estabelecidas, estatísticas/taxa de logs, uso de disco, período de retenção dos logs e status do envio de logs para soluções externas; 1.26. Deve suportar também o monitoramento dos seguintes recursos via SNMP: IP fragmentation, TCP state e dropped packets; 1.27. Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores; 1.28. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações; 1.29. Autenticação integrada ao Microsoft Active Directory ou servidor Radius; 1.30. Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados; 1.31. Deve atribuir sequencialmente um número a	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		cada regra de firewall, NAT, QOS e regras de DOS; 1.32. Criação de regras que fiquem ativas em horário definido; 1.33. Criação de regras com data de expiração; 1.34. Backup das configurações e rollback de configuração para a última configuração salva; 1.35. Suportar Rollback de Sistema Operacional para a última versão local; 1.36. Habilidade de upgrade via SCP, TFTP e interface de gerenciamento; 1.37. Deve possuir mecanismo de análise de impacto na política de segurança antes de atualizar a base com novas aplicações disponibilizadas pelo fabricante; 1.38. Validação de regras antes da aplicação; 1.39. Deve implementar mecanismo de validação de configurações antes da aplicação das mesmas permitindo identificar erros, tais como: rota de destino inválida, regras em *shadowing* etc. 1.39.1. É permitido o uso de appliance externo para permitir a validação de regras antes da aplicação. 1.40. Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing); 1.40.1. É permitido o uso de appliance externo para permitir a validação de políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing); 1.41. Deve possibilitar a visualização e comparação de configurações Atuais, configuração anterior e configurações antigas. 1.42. Deve permitir auditar regras de segurança exibindo quadro comparativo das alterações de uma regra em relação a versão anterior; 1.43. Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors) 1.44. Geração de logs de auditoria detalhados,	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		informando a configuração realizada, o administrador que a realizou e o horário da alteração; 1.45. Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado; 1.46. Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição; 1.47. Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus e Anti-Spware), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes; 1.48. Deve permitir a criação de *Dash-Boards* customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS, antivírus, anti-spyware, malwares "Zero Day"detectados em sand-box e tráfego bloqueado; 1.49. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança; 1.50. Dever permitir a visualização dos logs de malwares modernos, tráfego (IP de origem, destino, usuário e porta), aplicação, IPS, antivírus, anti-spyware, Filtro de URL e filtro de arquivos em uma única tela; 1.51. Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Spware), etc; 1.52. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e Anti-Spware), e URLs que passaram pela solução; 1.53. Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime; 1.54. Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso; 1.55. Deve possuir relatório de visibilidade e uso sobre aplicativos (SaaS). O relatório também deve mostrar os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		informação do usuário responsável pelo acesso; 1.56. Os relatórios de visibilidade e uso sobre aplicativos (SaaS) devem poder ser extraídos por grupo de usuários apresentando o uso e consumo de aplicações por grupo de usuário; 1.57. Deve ser possível exportar os logs em CSV; 1.58. Deverá ser possível acessar o equipamento a aplicar configurações durante momentos onde o trafego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada. 1.59. Rotação do log; 1.60. Deve permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado; 1.61. Deve permitir fazer o envio de logs para soluções externas de forma granular podendo selecionar quais campos dos logs serão enviados incluindo, mas não limitado a: tipo de ameaça, usuário, aplicação, etc; 1.62. Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto): 1.62.1. Situação do dispositivo e do cluster; 1.62.2. Principais aplicações; 1.62.3. Principais aplicações por risco; 1.62.4. Administradores autenticados na gerência da plataforma de segurança; 1.62.5. Número de sessões simultâneas; 1.62.6. Status das interfaces; 1.62.7. Uso de CPU; 1.63. Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados: 1.63.1. Resumo gráfico de aplicações utilizadas; 1.63.2. Principais aplicações por utilização de largura de banda de entrada e saída; 1.63.3. Principais aplicações por taxa de transferência de bytes; 1.63.4. Principais hosts por número de ameaças identificadas; 1.63.5. Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Spware), de rede vinculadas a este tráfego;	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1.63.6. Deve permitir a criação de relatórios personalizados; 1.64. Em cada critério de pesquisa do log deve ser possível incluir múltiplas entradas (ex. 10 redes e IP's distintos; serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa; 1.65. Gerar alertas automáticos via: 1.65.1. Email; 1.65.2. SNMP; 1.65.3. Syslog; 1.66. A plataforma de segurança deve permitir através de API-XML (Application Program Interface) a integração com sistemas existentes no ambiente da contratante de forma a possibilitar que aplicações desenvolvidas na contratante possam interagir em RealTime com a solução possibilitando assim que regras e políticas de segurança de possam ser modificadas por estas aplicações com a utilização de scripts em linguagens de programação como Perl ou PHP. **Suporte e garantia para a solução de segurança da informação descrita nesta especificação técnica** 1.67. Deve possuir garantia do fabricante no Brasil com validade de 36 (trinta e seis) meses; 1.68. Durante o prazo de garantia, deve ser possível realizar a atualização de sistema operacional dos equipamentos para obter novas funcionalidades e correção de bugs; 1.69. Os chamados poderão ser abertos diretamente com a contratada ou autorizada oficial do fabricante através de ligação telefônica gratuita (0800) no idioma Português, website e e-mail durante a vigência da garantia (36 meses). O suporte deverá ser na modalidade de 24x7 (24 horas por dia, 7 dias por semana); 1.70. O suporte deverá ter no mínimo o seguinte tempo de resposta para os níveis de severidade abaixo: a. Crítico: Significa que o produto ficou inoperante ou ocorreu falha de grande impacto. Para este nível de severidade o atendimento deve ser imediato e com tempo de resposta de até 1 (uma) hora para resolução total ou encontro de solução temporária de contorno; b. Alta: Impacto moderado no sistema, travamento, ou parada de ambiente parcial. Para este nível	

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		de severidade o tempo de resposta deve ser de até 2 (duas) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno; c. Média: Redução de performance do equipamento ou aplicação de solução temporária de contorno bem-sucedida. Para este nível de severidade o tempo de resposta deve ser de até 4 (quatro) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno; d. Baixa: Dúvidas de configuração ou anomalia de baixo impacto. Para este nível de severidade o tempo de resposta deve ser de até 8 (oito) horas em horário comercial.	
	5	**Treinamento oficial para solução de firewall** 5.1. Deverá disponibilizar voucher (s) para treinamento oficial do fabricante; 5.2. O treinamento deve ser ministrado abrangendo teoria e prática de implantação, configuração, administração e solução de problemas no ambiente deste órgão, bem como assuntos teóricos relacionados; 5.3. Deve conter no mínimo a seguinte ementa: ● Arquitetura e Plataforma; ● Configuração Inicial; ● Configuração Interface; ● Políticas de Segurança e NAT; ● Identificação de Aplicações; ● Identificação de Conteúdo Básico; ● Filtro URL; ● Decriptografia; ● Prevenção de ameaças desconhecidas; ● Identificação de Usuário; ● VPN; ● Monitoramento e Relatórios; ● Alta Disponibilidade (redundância); 5.4. O tempo dedicado a cada solução deve ser proporcional à complexidade da administração de cada uma; 5.5. A duração do curso será de, no máximo, 5 dias em horário comercial; 5.6. Deve ser emitido um único certificado de conclusão cobrindo todo o curso, sendo um para cada participante; 5.7. O treinamento deverá ser ministrado pelo próprio	3

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		fabricante ou por um parceiro nacional, capacitado, certificado e autorizado pelo fabricante a ministrar treinamentos oficiais. 5.8. O treinamento deve estar disponível nas modalidades online e/ou presencial nas instalações do fabricante ou autorizada; 5.9. A contratada fornecerá os materiais didáticos para ministrar o curso; 5.10. Não será necessário considerar na proposta os custos de deslocamento, hospedagem e alimentação. Esses custos serão de responsabilidade da contratante;	
	6	**Instalação de solução Firewall de Próxima Geração** 6.1. Prestar serviços de instalação e configuração, que compreendem, entre outros, os seguintes procedimentos: 6.1.1. Reunião de alinhamento para criação do escopo do projeto previamente a instalação; 6.1.2. Instalação e configuração de 2 (dois) firewalls em Alta Disponibilidade (ativo/passivo) nas dependências do IFPI; 6.1.3. Análise da topologia e arquitetura da rede , considerando todos equipamentos já existentes instalados; 6.1.4. Análise do acesso à Internet , sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos; 6.1.5. Migração das regras de Firewall existentes e aplicáveis à solução ofertada , considerando a adequação às políticas de camada 7; 6.1.6. Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução; 6.1.7. Instalação física de todos os equipamentos adquiridos no local determinado pela equipe de Informática; 6.1.8. Configuração do sistema de Firewall , VPN, IPS, Filtro URL, Antivírus e Anti malware de acordo com as exigências levantadas; 6.1.9. Instalação e configuração do sistema de gerenciamento centralizado; 6.1.10. Repasse no formato hands-on de 4 horas para o DTI após validação da migração; 6.1.11. Deve haver geração de relatório com as configurações efetuadas e as decisões tomadas em formato legível e tecnicamente fundamentado.	10
	7	**Banco de horas - suporte técnico**	150

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		1. Deve ser considerado pacote com 150 horas de serviço de suporte técnico para ajustes e configuração da solução ofertada neste edital; 2. O suporte técnico deve ser prestado pela Contratada ou Subcontratada, com técnicos que deverão possuir certificado do fabricante para garantir a qualidade do atendimento; 3. O atendimento de chamados para suporte técnico será realizado dentro do horário comercial, das 08h00 às 18h00, salvo casos onde haja parada no ambiente devido falha crítica, que demande janelas de manutenção; 4. Parte do pacote de horas poderá ser utilizado a critério do IFPI para repasse de informação no formato de treinamento para a equipe da Contratante; 5. Deverá registrar todos os chamados de suporte técnico para posterior entrega de relatório para a Contratante;	

5. JUSTIFICATIVA COMPATIBILIDADE

Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), estes equipamentos, por questões de compatibilidade, gerência, suporte e garantia, devem ser do mesmo fabricante dos equipamentos deste grupo/lote.

6. CONDIÇÕES GERAIS

Condições de Entrega

- O prazo de entrega de produtos deverá ocorrer em até no máximo 90 (noventa) dias corridos a partir da data de assinatura do contrato;
- A entrega deve ser agendada com antecedência mínima de 24 horas, sob o risco de não ser autorizada;
- Para itens de software, poderá ser fornecido sem mídia de instalação, desde que seja indicado local para download do arquivo de instalação;

Habilitação e Qualificação do Fornecedor

- Deve ser apresentado atestado de capacidade técnica comprovando que a licitante é apta a instalar, configurar, prestar suporte técnico e ministrar

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

treinamentos das soluções referente a este edital;

- A empresa deverá possuir no mínimo 1 (um) profissional pertencente ao quadro de funcionários da empresa com certificação técnica oficial do fabricante, compatível com o(s) objeto(s) deste processo. Tal comprovação deverá ser enviada durante a fase de habilitação.

Padronização

- Conforme disposto no item I do artigo 15 da lei 8.666, de 21 de junho de 1993 (I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), estes equipamentos, por questões de compatibilidade, gerência, suporte e garantia, devem ser do mesmo fabricante dos equipamentos deste grupo/lote;

Condições de aceite

- Somente serão aceitos equipamentos novos e sem uso. Não serão aceitos equipamentos remanufaturas, NFR (Not For Resale) ou de demonstração. Os equipamentos deverão ser entregues nas caixas lacradas pelo fabricante, não sendo aceitos equipamentos com caixas violadas;
- O aceite do bem somente será dado após comprovação da entrega e o efetivo cumprimento de todas as exigências da presente especificação técnica;
- Será consultado diretamente no site do fabricante do equipamento manuais e toda documentação pública disponível para comprovação do pleno atendimento aos requisitos deste edital. Em caso de dúvida ou divergência na comprovação da especificação técnica, este órgão poderá solicitar amostra do equipamento ofertado, sem ônus ao processo, para comprovação técnica de funcionalidades. Esta amostra deverá ocorrer em até 15 (quinze) dias úteis após a solicitação deste órgão. Para a amostra, a empresa deverá apresentar o mesmo modelo do equipamento ofertado no certame, com técnico certificado na solução para configuração e comprovação dos itens pendentes, nas dependências deste órgão (conforme itens 1.1.1 e 1.1.2, TC-006.806/2006-4, Acórdão nº 838/2006-TCU-2ª Câmara);

Adesão a Ata de Registro de Preços

- Os órgãos/entidades que não participaram do procedimento licitatório, quando desejarem poderão fazer uso da Ata de Registro de Preços, devendo consultar a este órgão para manifestação sobre a possibilidade de adesão;
- Conforme o Decreto no 7.892/2013, o somatório de todas as contratações adicionais, entendidas como aquelas realizadas por órgãos não participantes da presente Ata de Registro de Preços, não poderá ultrapassar o quíntuplo da quantidade total registrada para cada item na ata de registro de preços para o órgão gerenciador e órgãos participantes;
- As aquisições ou contratações adicionais a que se refere este subitem não poderão exceder, por órgão ou entidade, a cem por cento dos quantitativos dos itens do instrumento convocatório e registrados na ata de registro de preços para o órgão gerenciador e órgãos participantes;
- O limite estabelecido no item anterior não afeta os quantitativos registrados pelo órgão gerenciador e órgãos participantes, como também a possibilidade prevista no § 1o, art. 65, da Lei n. 8.666/93, para os quantitativos efetivamente contratados.

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

Para os quantitativos não contratados, fica vedado efetuar acréscimos, conforme o § 1o, do art.12, do Decreto no 7.832/2013.

7. DEVERES E RESPONSABILIDADES DA CONTRATANTE

7.1. Receber o objeto no prazo e condições estabelecidas no Edital e seus anexos;

7.2. Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo;

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

7.4. Acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através de comissão/servidor especialmente designado;

7.5. Efetuar o pagamento à Contratada no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no Edital e seus anexos;

7.6. Notificar a Contratada por escrito da ocorrência de eventuais imperfeições no curso da execução dos serviços, fixando prazo para a sua correção;

7.7. Proporcionar a Contratada condições e facilidades que estejam ao seu alcance para que esta possa executar o objeto contratual de forma satisfatória;

7.8. Aplicar à Contratada as penalidades cabíveis, quando for o caso e conforme legislação vigente, garantindo o contraditório e a ampla defesa;

7.9. Manter arquivado junto ao processo administrativo ao qual estará vinculado o Edital, toda a documentação a ele referente, apensando processos de Fiscalização e Penalizações decorrentes da contratação;

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

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

8. DEVERES E RESPONSABILIDADES DA CONTRATADA

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

8.2. Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Termo de Referência e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, fabricante, modelo, procedência e prazo de garantia ou validade;

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

8.4. Substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste Termo de Referência, o objeto com avarias ou defeitos;

8.5. Responsabilizar-se pela contratação ou ônus de eventual garantia estendida, caso a garantia do fabricante seja inferior ao requerido para os itens;

8.6. Comunicar à Contratante, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

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

8.8. Indicar preposto para representá-la durante a execução do contrato;

8.9. Utilizar empregados habilitados e com conhecimentos básicos dos serviços a serem executados, em conformidade com as normas e determinações em vigor;

8.10. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento da contratação;

8.11. Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas na legislação específica, cuja inadimplência não transfere responsabilidade à Contratante;

8.12. Solucionar todos os problemas técnicos e/ou legais que surgirem durante a execução dos serviços contratados;

8.13. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento ao objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do § 1º do art. 57 da Lei nº 8.666, de 1993;

8.14. Cumprir as normas brasileiras relativas à matéria;

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

8.15. Tratar com urbanidade, celeridade e presteza os servidores do IFPI encaminhados para atendimento;

8.16. Assegurar a cobertura de garantia de qualidade com assistência técnica qualificada, on-site, seguindo-se os padrões dos fabricantes e utilizando-se mão-de-obra devidamente qualificada e certificada nos equipamentos adquiridos;

8.17. Responder por danos materiais e/ou morais causados, por pessoal encarregado da execução dos serviços, a discentes, docentes, e demais servidores do IFPI, decorrente de dolo ou culpa. Todas as providências judiciais ou extrajudiciais para solução de questões vinculadas e danos causados a terceiros serão de responsabilidade da Contratada e tomadas em seu próprio nome e às suas expensas.

9. DA VISTORIA

9.1. Para o correto dimensionamento e elaboração de sua proposta, o licitante PODERÁ realizar a vistoria nas instalações do local de onde serão executados os serviços, acompanhado por servidor designado para esse fim, em dia útil, de segunda a sexta-feira, das 08 horas às 11 horas e das 14 horas às 16 horas, devendo o agendamento ser efetuado previamente pelo telefone (86) 3131-1414 ou através do e-mail dti@ifpi.edu.br após confirmação do órgão licitante, ou presencialmente no endereço: IFPI Reitoria – Diretoria de Tecnologia da Informação, localizado na Av. Pres. Jânio Quadros, número 330, bairro Santa Isabel, Teresina, Piauí, CEP 64053-390.

9.2. O prazo para vistoria iniciar-se-á no dia útil seguinte ao da publicação do Edital, estendendo-se até o segundo dia útil anterior à data prevista para a abertura da sessão pública.

9.3. Para a vistoria, o licitante, ou o seu representante, deverá estar devidamente identificado.

9.4. A Licitante poderá optar por não realizar a visita técnica, mas, deverá, obrigatoriamente, apresentar junto a sua documentação de habilitação uma declaração de conhecimento prévio da área onde serão executados o fornecimento e instalação dos equipamentos. Dessa forma, caso venha ser a vencedora, não poderá alegar em nenhuma hipótese o desconhecimento dos locais da realização do fornecimento e instalação dos materiais e suas peculiaridades como justificativa para se eximir das obrigações assumidas em consequência do presente certame.

10. ATESTADOS DE CAPACIDADE TÉCNICA

10.1. Deve(m) ser fornecido(s) Atestado(s) de Capacidade Técnica emitido por pessoas jurídicas de direito público ou privado, impresso em papel timbrado, com os dados do responsável pela informação atestada, comprovando que a licitante forneceu, instalou, configurou e prestou suporte técnico a equipamento de características semelhantes aos especificados neste edital, além de informar, sempre que possível, quantidade, valores e demais dados técnicos, com

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

qualidade satisfatória.

10.2. A administração poderá fazer diligências para comprovação do conteúdo dos atestados.

10.3. Não serão aceitas declarações genéricas de catálogos, manuais ou internet.

10.4. Os atestados deverão ser apresentados em seu original ou cópia devidamente autenticada.

11. FORMA E PRESTAÇÃO DOS SERVIÇOS

11.1. Os serviços serão executados conforme discriminado:

11.1.1. Os serviços a serem prestados são de natureza técnica.

11.1.2. A versão dos produtos disponibilizada deve ser a última disponível no mercado na data de sua entrega.

11.1.3. Os produtos devem vir acompanhados de manuais completos e originais com instruções de instalação e configuração e manuais completos e originais com instruções de uso do produto e de todas as suas funcionalidades.

11.1.4. Os equipamentos e softwares que compõem a solução, objetos do presente Termo, deverão ser entregues no seguinte endereço:

IFPI - Reitoria, localizado na Av. Pres. Jânio Quadros, número 330, bairro Santa Isabel, Teresina, Piauí, CEP 64053-390.

12. ESTIMATIVA DE PREÇO

GRUPO	Id	Bem/serviço	Quant	Valor Unitário Estimado
1	1	FIREWALL VIRTUAL TIPO 1 COM LICENÇA DE FILTRO URL, LICENÇAS DE PROTEÇÃO CONTRA AMEAÇAS CONHECIDAS E DESCONHECIDAS E SUPORTE / GARANTIA DE 5 ANOS	1	R$ 179.688,52
	2	FIREWALL VIRTUAL TIPO 2 COM LICENÇA DE FILTRO URL, LICENÇAS DE PROTEÇÃO CONTRA AMEAÇAS CONHECIDAS E DESCONHECIDAS E SUPORTE / GARANTIA DE 5 ANOS	4	R$ 89.582,09
	3	FIREWALL TIPO 1 COM LICENÇA DE FILTRO URL, LICENÇAS DE PROTEÇÃO CONTRA AMEAÇAS CONHECIDAS E DESCONHECIDAS E	5	R$ 220.602,94

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

		SUPORTE / GARANTIA DE 3 ANOS		
	4	SOFTWARE DE GESTÃO CENTRALIZADA PARA NGFW COM SUPORTE/GARANTIA DE 3 ANOS	1	R$ 181.182,77
	5	TREINAMENTO OFICIAL PARA SOLUÇÃO DE FIREWALL	3	R$ 20.641,45
	6	INSTALAÇÃO DE SOLUÇÃO DE FIREWALL DE PRÓXIMA GERAÇÃO	10	R$ 27.160,96
	7	BANCO DE HORAS – SUPORTE TÉCNICO	150	R$ 213,97
		VALOR TOTAL		**R$ 2.187.844,28**

13. ENTREGA

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

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

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

13.4. Os produtos deverão ser entregues na reitoria do Instituto Federal do Piauí, UASG 158146, localizado na Av. Pres. Jânio Quadros, número 330, bairro Santa Isabel, Teresina, Piauí, CEP 64053-390, contato (86) 3131-1414, sem custas para o contratante, em prazo não superior a 30 (trinta) dias, contados após o recebimento da Nota de Empenho.

13.5 A entrega do(s) produto(s) deverá ser efetuada de Segunda a Sexta, no horário das 08h às 12h e das 14h às 17h, nos dias úteis, de acordo com a necessidade e mediante solicitação, devendo a CONTRATADA, com antecedência mínima de 24 (vinte e quatro) horas, marcar data e horário para a entrega pelo telefone;

13.6. Os pedidos de materiais a serem adquiridos, pelo Registro de Preços, serão efetuados por Nota de Empenho, devidamente numerada em ordem sequencial por pedido, datada e assinada, por servidor designado pela autoridade competente;

13.7. A entrega dos materiais deverá ser efetuada de acordo com o respectivo

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

Contrato e/ou Ata de Registro de Preços, sempre acompanhada do respectivo documento fiscal;

13.8. Não serão pagos os materiais entregues em locais diferentes do mencionado no item 13.4. ou a pessoas não autorizadas;

13.9. Os serviços serão realizados nas dependências da CONTRATANTE, por meio da supervisão e fiscalização da Diretoria de Tecnologia da Informação do Instituto Federal do Piauí;

13.10. Os serviços deverão ser executados de forma cuidadosa, criteriosa e apropriados de modo a evitar danos materiais, pessoais e ambientais;

13.11. Os equipamentos e softwares que compõem a solução, objetos do presente Termo, deverão ser entregues no prazo máximo de 30 (trinta) dias corridos após a assinatura do contrato;

13.12. O prazo de instalação para Solução é de até 15 (quinze) dias corridos, contados a partir do aceite definitivo dos equipamentos;

13.13. A licitante vencedora e seus funcionários deverão observar, rigorosamente, todas as normas e procedimentos de segurança implementados no ambiente de Tecnologia da Informação do IFPI;

13.14. Será exigida da licitante vencedora que cada profissional que venha a prestar serviços assine um termo de compromisso, pelo qual se compromete a manter sigilo e a confidencialidade de todos os dados e informações de que venha a ter conhecimento no exercício de suas atribuições, o qual deverá ser entregue à Fiscalização do contrato;

13.15. A licitante vencedora deverá manter sigilo absoluto a respeito de quaisquer dados, informações, códigos-fonte e artefatos, contidos em documentos e mídias, de que venha a ter conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos, independentemente da classificação de sigilo conferida pelo IFPI a tais documentos;

13.16. O IFPI se reserva o direito de proceder a levantamento e/ou confirmação de informações pertinentes à idoneidade de qualquer profissional que venha a ser indicado para a prestação dos serviços.

14. RECEBIMENTO

14.1. De acordo com o Art. 5o, III da Instrução Normativa no 01 de 19 de janeiro de 2010, da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão, os bens devem ser, preferencialmente, acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e armazenamento.

14.2. Os bens serão recebidos provisoriamente no ato da entrega, por servidor

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

público indicado pela contratante, para efeito de posterior verificação da sua conformidade com as especificações constantes no Termo de Referência e nas especificações constantes na proposta.

14.3. Os equipamentos poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta da licitante vencedora, devendo ser substituídos no prazo de 10 (dez) dias corridos, a contar da notificação da contratada, devendo está arcar com todas as custas para a entrega de equipamento similar ou de superior qualidade ao IFPI, sem prejuízo da aplicação das penalidades legais e aquelas previstas neste instrumento.

14.4. Nos casos de sinais externos de avaria de transporte ou de mau funcionamento do equipamento, verificados na inspeção do mesmo, este deverá ser substituído por outro com as mesmas características, no prazo de até 30 (trinta) dias corridos, a contar da data de realização da inspeção;

14.5. Os equipamentos serão recebidos definitivamente no prazo de até 45 (quarenta e cinco) dias corridos, contados do recebimento provisório, após a verificação da qualidade e quantidade dos equipamentos, bem como sua adequação às especificações técnicas, e consequente aceitação mediante termo circunstanciado.

14.5.1. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da contratada pelos prejuízos resultantes da incorreta execução do contrato.

14.5.2. Na hipótese de a verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo.

15. DO ACOMPANHAMENTO E DA FISCALIZAÇÃO DO CONTRATO

15.1 A execução do contrato será acompanhada e fiscalizada por intermédio de fiscal especialmente designado pela Administração, nos termos do art. 67, da Lei no 8.666/93. Verificados ainda os apontamentos no Modelo de Gestão.

16. DA FORMALIZAÇÃO E VIGÊNCIA

16.1. O contrato de fornecimento deverá ter vigência de 12 (doze) meses, a contar da data de assinatura do mesmo, podendo ser prorrogado por iguais e sucessivos períodos, até o limite de 60 (sessenta) meses, conforme previsto no art. 57, inciso II da Lei no 8.666/93 e alterações, com vistas à obtenção de preços e condições mais vantajosas para a Administração.

17. SANÇÕES

17.1. Comete infração administrativa nos termos da Lei no 8.666, de 1993 e da Lei no 10.520, de 2002, a Contratada que:

a) Não assinar a ata de registro de preços quando convocado dentro do prazo de validade da proposta, não aceitar/retirar a nota de empenho ou não assinar o termo de contrato decorrente da ata de registro de preços;
b) Apresentar documentação falsa;
c) Deixar de entregar os documentos exigidos no certame;
d) Inexecução total ou parcial de qualquer das obrigações assumidas em decorrência da contratação;

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

e) Ensejar o retardamento da execução do objeto;
f) Fraudar na execução do contrato;
g) Comportar-se de modo inidôneo;
h) Cometer fraude fiscal;
i) Não mantiver a proposta.

17.2. A Contratada que cometer qualquer das infrações discriminadas no subitem acima ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

a) Advertência por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a Contratante;
b) Multa moratória de 0,03% (três centésimos por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias; decorridos 30 (trinta) dias de atraso a CONTRATANTE poderá optar pela rescisão do contrato, em razão da inexecução total.

c) Multa compensatória de 10% (dez por cento) sobre o valor total do contrato, no caso de inexecução total do objeto. Multa de 10% (dez por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do licitante;
d) Em caso de inexecução parcial, a multa compensatória, no mesmo percentual do subitem acima, será aplicada de forma proporcional à obrigação inadimplida;
e) Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;
f) Impedimento de licitar e contratar com a União com o consequente descredenciamento no SICAF pelo prazo de até cinco anos;
g) Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados;
h) Impedimento de licitar e de contratar com a União e descredenciamento no SICAF, pelo prazo de até cinco anos;
17.3. A penalidade de multa pode ser aplicada cumulativamente com a sanção de impedimento.
17.4. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto na Lei no 8.666, de 1993, e subsidiariamente na Lei no 9.784, de 1999. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.
17.5. As sanções por atos praticados no decorrer da contratação estão previstas no Termo de Referência.
17.6. 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 licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.
17.7. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei no 8.666, de 1993, as empresas e os profissionais que:
a) Tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;
b) Tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;
c) Demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.
SUBCLÁUSULA PRIMEIRA – A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à Contratada, observando-se o procedimento previsto na Lei no 8.666, de 1993, e subsidiariamente a Lei no 9.784, de 1999.
SUBCLÁUSULA SEGUNDA – A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

o dano causado à Administração, observado o princípio da proporcionalidade.
SUBCLÁUSULA TERCEIRA – As penalidades serão obrigatoriamente registradas no SICAF.
17.8. A não observância pela CONTRATADA quanto aos prazos estabelecidos neste termo para apresentação das informações que caracterizam o início da prestação dos serviços de suportes resulta na sujeição da CONTRATADA às sanções abaixo definidas:
17.8.2. Advertência: Atraso injustificado em até sete dias corridos;
17.8.1. Multa: Atraso injustificado em período maior de sete dias corridos. O valor da multa a ser aplicado será calculado conforme abaixo:
VM = [(NDA – 7) * VC* 0,1] / 30
VM = Valor da multa;
NDA = Número de dias (corridos) atrasados;
VC = Valor anual da prestação do serviço de suporte;
O valor máximo da multa será equivalente a 30 dias de atrasos. A partir deste momento, e de forma acumulativa, se aplica a penalidade de impedimento de licitar e contratar com a União, Estados, Distrito Federal ou Municípios, conforme Art 7o da Lei n.o 10.520.

18. DAS PENALIDADES

18.1 A recusa ou o não cumprimento do objeto contratado dentro do prazo estabelecido pela Administração sem motivo justificado caracteriza o descumprimento da obrigação assumida sujeita a CONTRATADA à aplicação de advertência ou multa de até 5% do valor do contrato, que deverá ser recolhida no prazo de 15 (quinze) dias contados da comunicação oficial.
18.2 A aplicação de quaisquer das penalidades previstas neste instrumento será, obrigatoriamente registrada no SICAF e precedida de regular processo administrativo, no qual será assegurado o contraditório e a ampla defesa.

19. DO REAJUSTE

19.1. O contrato será reajustado com base no Índice de Custo da Tecnologia da Informação (ICTI), conforme Portaria nº 6.432 de 11 de julho de 2018 do Ministério do Planejamento, Desenvolvimento e Gestão/Secretaria de Tecnologia da Informação e Comunicação.

20. DO PAGAMENTO

20.1. O pagamento será efetuado pela Contratante no prazo de 30 dias, contados do recebimento da Nota Fiscal/Fatura.

20.1.1. Os pagamentos decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da Lei 8.666, de 1993, deverão ser efetuados no prazo de até 5 (cinco) dias úteis, contados da data da apresentação da Nota Fiscal/Fatura, nos termos do art. 5º, § 3º, da Lei nº 8.666, de 1993.

20.2. A emissão da Nota Fiscal/Fatura será precedida do recebimento definitivo do serviço, conforme este Termo de Referência.
20.3. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 29 da Lei nº 8.666, de 1993.

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

20.4 O setor competente para proceder o pagamento deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

20.4.1 o prazo de validade;
20.4.2 a data da emissão;
20.4.3 os dados do contrato e do órgão contratante;
20.4.4 o período de prestação dos serviços;
20.4.5 o calor a pagar; e

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

20.4.6 eventual destaque do valor de retenções tributárias cabíveis.

20.5. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante;

20.6. Nos termos do item 1, do Anexo VIII-A da Instrução Normativa SEGES/MP nº 05, de 2017, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:

20.6.1. não produziu os resultados acordados;

20.6.2. deixou de executar as atividades contratadas, ou não as executou com a qualidade mínima exigida;

20.6.3 deixou de utilizar os materiais e recursos humanos exigidos para a execução do serviço, ou utilizou-os com qualidade ou quantidade inferior à demandada.

20.7. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

20.8. Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital

20.9. Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da contratante.

20.10. Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018.

20.11. Não havendo regularização ou sendo a defesa considerada improcedente, a contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

20.12. Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.

20.13. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao SICAF.

20.13.1. Será rescindido o contrato em execução com a contratada inadimplente no SICAF, salvo por motivo de economicidade, segurança nacional ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da contratante.

20.14. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável, em especial a prevista no artigo 31 da Lei 8.212, de 1993, nos termos do item 6 do Anexo XI da IN SEGES/MP n. 5/2017, quando couber.

20.15. É vedado o pagamento, a qualquer título, por serviços prestados, à empresa privada que tenha em seu quadro societário servidor público da ativa do órgão contratante, com fundamento na Lei de Diretrizes Orçamentárias vigente.

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

EM = I x N x VP, sendo:

EM = Encargos moratórios;

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

VP = Valor da parcela a ser paga.

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

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

$I = (TX) \qquad I = \frac{(6 / 100)}{365}$ I = 0,00016438
TX = Percentual da taxa anual = 6%

21. DISPOSIÇÕES GERAIS

21.1. O IFPI/Reitoria reserva-se ao direito de solicitar quaisquer dos itens registrados no presente Termo de referência em qualquer momento, inexistindo obrigação de contratação total imediata.

Equipe de Planejamento da Contratação		
Rafael Morais da Cunha	Paulo Alex dos Santos Maranhão	Leonardo de Macedo Carvalho

Integrante Requ s tante

Rafael Mora s da Cunha
Matr cula: 2178256

Integrante Tecn co

Paulo Alex dos Santos Maranhao
Matr cula: 1263948

Integrante Adm n strat vo

Leonardo de Macedo Carvalho
Matr cula: 1808241

Aprovo. Encaminha-se à DEPLIC – Departamento de Licitações, para abertura de processo administrativo e iniciação de procedimento licitatório, segundo o art. 38 da Lei n° 8.666,

Autor dade Competente da Area Adm n strat va

Paulo Borges da Cunha
Matr cula: 1288003

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br

Teresina- PI, 20 de julho de 2020.

Avenida Presidente Jânio Quadros, 330 – Santa Isabel – Teresina – PI CEP. 64.053-390
Fone: (086)3131 1414/ dti@ifpi.edu.br / endereço eletrônico: www.ifpi.edu.br