



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

TERMO DE REFERÊNCIA

1. OBJETO

Contratação de empresa especializada para fornecimento de solução de segurança de perímetro Firewall/UTM, solução de segurança para a camada de servidores físicos e virtuais, e serviços técnicos de monitoramento e suporte especializado nas soluções de segurança (servidores físicos, virtuais e de perímetro - Firewall/UTM), através de uma Central de Monitoramento de Redes e Serviços (NOC) localizada nas dependências da CONTRATADA. A prestação deste serviço compreende o gerenciamento proativo de eventos, através do monitoramento de métricas de disponibilidade, capacidade e performance de ativos de rede, servidores e serviços de TI, baseado nas melhores práticas de mercado.

2. DA JUSTIFICATIVA

Em 2013 o INEA adquiriu equipamentos do tipo firewall para proteção de segurança da informação que visa o bloqueio de acessos não autorizados a ativos de rede bem como ativos de informação críticas a organização, desta forma é possível permitir somente a transmissão e recepção de dados autorizados evitando tentativas e acessos indevidos.

Conforme contrato atual, o período de garantia, suporte do fabricante e licenças dos softwares embutidos na solução foi de 36 meses a partir da ativação dos produtos, ocorrida em 29/07/2014. Portanto, o período de garantia, suporte do fabricante e licenças dos softwares embutidos expiraram em 28/07/2017.

Devido à necessidade de aumento na velocidade dos links de internet e MPLS para conexão entre o INEA e suas superintendências e as recentes ameaças avançadas como Ransomwares, que geraram impactos graves em diversos órgãos governamentais e empresas privadas no Brasil, se faz necessário além da aquisição uma solução de firewall/UTM mais robusta para atender o aumento de demanda de tráfegos de dados, a aquisição de solução de segurança na camada de servidores, para proteger a rede do INEA contra ameaças de vírus, malwares e vulnerabilidades de softwares.





GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

A aquisição de soluções integradas de segurança na rede perimetral e de camada de servidores são de suma importância pela inexistência dentro do INEA, de uma solução que proteja os dados contidos na rede, que irá permitir a realização de:

- criação de filtros para bloqueio dos conteúdos impróprios como: pornografia, vídeos impróprios, arquivos maliciosos entre outros;
- proteger a rede contra worms, vírus, malware entre outras pragas virtuais;
- geração de relatórios dos acessos realizados por IP, grupo ou usuário nas seguintes formas: diário, semanal, mensal ou período selecionado;
- criação de políticas de proteção da rede de computadores contra: ataques de hackers através do bloqueio de programas de compartilhamento de dados (P2P), bloqueio mensagens instantâneas, fechamento de portas não utilizadas controlando a banda de internet a fim de evitar abusos em sua utilização;
- Regras de bloqueio e liberação de serviços e portas TCP e UDP por grupo ou usuário;
- Limitação de banda por serviços, tais como: servidor web, streaming, internet etc.;
- Monitoramento do link de dados;
- Bloqueio de vulnerabilidades do sistema operacional e aplicações de mercado, por conta de patches que não podem ser atualizados com frequência ou por sua liberação em tempo hábil pelos fabricantes.
- Prover visibilidade dessas possíveis ações de atacantes, com funcionalidades de inspeção de logs e monitoramento contínuo.



3. DESCRIÇÃO DOS PRODUTOS

3.1. Solução de Segurança de Perímetro - Firewall/UTM

3.1.1. Características gerais

- 3.1.1.1. Os produtos de hardware ofertados deverão ser novos, nunca terem sido utilizados e não terem sido descontinuados, ou seja, devem constar na linha atual de comercialização e suporte do fabricante;
- 3.1.1.2. A solução deverá utilizar a tecnologia de firewall Stateful Packet Inspection com Deep Packet Inspection (suportar a inspeção da área de dados do pacote) para filtragem de tráfego IP;
- 3.1.1.3. Deverá ter hardware e software que executem as funcionalidades de proteção de rede devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;
- 3.1.1.4. Todo o ambiente deverá ser gerenciado através de uma única interface sem a necessidade de produtos de terceiros para compor a solução;
- 3.1.1.5. Deverá oferecer as funcionalidades de backup/restore tanto da configuração quanto do firmware/sistema operacional através da interface gráfica, assim como permitir ao administrador agendar procedimentos de backups da configuração em determinado dia e hora. O appliance deve armazenar no mínimo 02 (duas) versões distintas do sistema operacional, sendo possível escolher qual versão será inicializada; de backups da configuração em determinado dia e hora;
- 3.1.1.6. Deverá suportar a definição de VLAN no firewall, conforme padrão IEEE 802.1q e ser possível criar sub-interfaces lógicas associadas a VLANs e estabelecer regras de filtragem (Stateful Firewall) entre elas;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE - SEA
INSTITUTO ESTADUAL DO AMBIENTE - INEA

- 3.1.1.7. A solução deverá suportar configuração de link-aggregation de interfaces suportando o protocolo 802.3ad para aumento de throughput;
- 3.1.1.8. A solução deverá suportar configuração de port-redundancy de interfaces para a alta disponibilidade de interfaces;
- 3.1.1.9. Os dispositivos de proteção deverão 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);
 - ✓ Modo sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
 - ✓ Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
 - ✓ 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;
 - ✓ Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.
- 3.1.1.10. Deverá suportar arquitetura de armazenamento de logs redundante, permitindo a configuração de equipamentos distintos;
- 3.1.1.11. Os produtos ofertados deverão vir acompanhados de todos os cabos e acessórios necessários à completa instalação e operação dos mesmos;
- 3.1.1.12. Os produtos ofertados deverão vir acompanhados de documentação impressa ou em mídia DVD/CD ou via download, em



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

idioma português ou inglês, contendo orientações para configuração e operação do produto fornecido;

- 3.1.1.13. A Solução deverá ser em appliance com no máximo 2U de altura, com kit de montagem em rack de 19”;
- 3.1.1.14. Não serão permitidas soluções baseadas em sistemas operacionais abertos como Free BSD, Debian ou mesmo Linux;
- 3.1.1.15. O equipamento deverá ser baseado em hardware desenvolvido com esta finalidade, ou seja, de um firewall não sendo baseado em plataforma X86 ou equivalente;
- 3.1.1.16. O equipamento deverá ter o mínimo de 8 GB de memória RAM para maior confiabilidade do sistema;
- 3.1.1.17. O equipamento deverá ter armazenamento em SSD de no mínimo 64 Gb;
- 3.1.1.18. Sistema Operacional do Tipo “Harderizado” não serão aceitos. Apenas os que forem armazenados em memória flash;
- 3.1.1.19. Todas as funcionalidades descritas deverão funcionar no mesmo appliance, sem a necessidade de composição de um ou mais produtos;
- 3.1.1.20. A plataforma deverá ser otimizada para análise de conteúdo de aplicações em camada 7;
- 3.1.1.21. A solução deverá suportar monitoramento através de SNMP v2 e v3;
- 3.1.1.22. O equipamento deverá ter fonte de alimentação redundante com chaveamento automático entre 110/240V;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE - SEA
INSTITUTO ESTADUAL DO AMBIENTE - INEA

- 3.1.1.23. Deverá possuir redundância do sistema de refrigeração do produto (Fan) redundante, com no mínimo três ventiladores operando em modo “hot swappable”;
- 3.1.1.24. Deverá possuir pelo menos quatro interfaces de 10 GbE SFP+ ou UTP;
- 3.1.1.25. Deverá possuir pelo menos quatro interfaces de 1 GbE SFP;
- 3.1.1.26. Deverá suportar dezesseis interfaces 10/100/1000 GbE. Todas operando em modo autosense e em modo half/full duplex, com inversão automática de polaridade configuráveis pelo administrador do firewall para atendendo os segmentos de segurança e rede para:
- ✓ Segmento WAN, ou externo;
 - ✓ Segmento WAN, secundário com possibilidade de ativação de recurso para redundância de WAN com balanceamento de carga e WAN Failover por aplicação. O equipamento deverá suportar no mínimo balanceamento de 4 links utilizando diferentes métricas pré-definidas pelo sistema;
 - ✓ Segmento LAN ou rede interna;
 - ✓ Segmento LAN ou rede interna podendo ser configurado como DMZ (Zona desmilitarizada);
 - ✓ Segmento LAN ou rede interna ou Porta de sincronismo para funcionamento em alta disponibilidade;
 - ✓ Possuir uma interface de rede dedicada operando em 1Gbps para o gerenciamento do produto. Seu processamento deverá ser de forma isolada ao processamento dos demais tráfegos que passam pelo produto;
 - ✓ Possuir uma interface do tipo console ou similar;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- ✓ Segmento ou Zona exclusiva para controle de dispositivos Wireless dedicado, com controle e configuração destes dispositivos.

3.1.1.27. O equipamento deverá ter a VPN SSL licenciada para, no mínimo, dois usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para no mínimo, 1000 (Mil) usuários;

3.1.1.28. Deverá suportar 6000 túneis de VPN IPSEC simultâneos;

3.1.1.29. Deverá suportar, no mínimo, 3500 Mbps de throughput de VPN IPSEC;

3.1.1.30. Deverá ter Performance de Firewall SPI (Stateful Packet Inspection) igual ou superior a 6.200 Mbps;

3.1.1.31. Deverá ter Performance de todos os serviços ativos UTM (Gateway Antivírus, Gateway Anti Spyware, IDS, IPS e Filtro de Conteúdo) deverá ser de 1700 Mbps ou superior. Caso o fornecedor não possa comprovar este item em documentações públicas, o mesmo poderá comprovado através de testes em bancada com gerador de pacotes;

3.1.1.32. O equipamento deverá ter a capacidade de analisar tráfegos criptografados HTTPS/SSL onde o mesmo deverá ser decriptografado de forma transparente a aplicação, verificado possíveis ameaças e então re-criptografado enviado juntamente ao seu destino caso este não contenha ameaças ou vulnerabilidades;

3.1.1.33. Deverá ter Performance de Inspeção (decriptografia e criptografia) de trafego criptografado (SSL) de no mínimo 800 Mbps, os throughputs devem ser comprovados por documento de domínio público do fabricante. Caso o fornecedor não possa comprovar este item em documentações públicas, deve ser comprovado através de testes em bancada com gerador de pacotes (custos destes testes pagos pela



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

CONTRATADA). Não serão aceitos declarações ou cartas de fabricantes para atendimento a este item;

- 3.1.1.34. Deverá ter Performance de IPS igual ou superior 3400 Mbps;
- 3.1.1.35. Deverá ter Performance para inspeção de Anti-Malware integrado no mesmo appliance: 1.7 Gbps ou superior;
- 3.1.1.36. Não serão permitidas soluções baseadas em redirecionamento de tráfego para dispositivos externos ao appliance para análise de arquivos ou pacotes de dados. A atualização das assinaturas deverá ocorrer de forma automática sem há necessidade de intervenção humana;
- 3.1.1.37. A solução de Gateway Antivírus deverá suportar análise de pelo menos os protocolos, CIFS, NETBIOS, HTTP, FTP, IMAP, SMTP e POP3;
- 3.1.1.38. Não serão permitidas soluções baseadas em redirecionamento de tráfego para dispositivos externos ao appliance para análise de arquivos ou pacotes de dados;
- 3.1.1.39. A atualização das assinaturas deverá ocorrer de forma automática sem a necessidade de intervenção humana;
- 3.1.1.40. 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, o fornecedor será considerado inabilitados. Todos os custos oriundos do teste de bancada serão por conta do fornecedor;
- 3.1.1.41. Não serão aceitas cartas ou declarações de fabricantes para atendimento aos valores de performance solicitados;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- 3.1.1.42. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e/ou end-of-sale ou situação semelhante;
- 3.1.1.43. Capacidade mínima de conexões suportadas em modo firewall deverá ser de no mínimo ou superior 4.000.000 conexões;
- 3.1.1.44. Capacidade mínima de conexões suportadas em modo DPI (análise profunda de pacotes com os serviços IPS, Anti-Malware (Anti-Virus e Anti-Spyware) deverá ser de no mínimo a 1.500.000 conexões;
- 3.1.1.45. Capacidade mínima de conexões suportadas em modo DPI SSL (tráfego Criptografado) de 37.000 conexões;
- 3.1.1.46. Suportar no mínimo 40.000 novas conexões por segundo;
- 3.1.1.28. Performance de VPN IPSEC (3DES & AES 256) deverá ser de 3.5 Gbps ou superior;

3.1.2. Funcionalidades de Firewall

A solução deverá ter as seguintes funcionalidades:

- 3.1.2.1. Possibilitar o controle sobre aplicações de forma granular com criação de políticas sobre o fluxo de dados de entrada, saída ou ambos;
- 3.1.2.2. Possibilitar aplicações de regras e políticas por usuário e por grupo;
- 3.1.2.3. Associar suas ações a endereçamento IP baseados em sub-redes;
- 3.1.2.4. Permitir a filtragem de e-mails pelo seu conteúdo, através da definição de palavras-chave e a sua forma de pesquisa;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- 3.1.2.5. Prover matriz de horários que possibilite o bloqueio de serviços com granularidade baseada em hora, minutos, dia, dias da semana, mês e ano que a ação deverá ser tomada.
- 3.1.2.6. Permitir a utilização de políticas de segurança associadas as políticas Anti Malware, IPS/IDS e filtro de Conteúdo em diferentes segmentos e diferentes combinações podendo ser aplicadas inclusive em sub-interfaces estruturadas em Vlans, por sua vez associadas a diferentes zonas de segurança.
- 3.1.2.7. Possuir flexibilidade para liberar aplicações da inspeção profunda de pacotes, ou seja, excluir a aplicação da checagem de recursos como Anti Malwares, IPS entre outros.
- 3.1.2.8. Prover controle e gerenciamento de banda para a tecnologia VoIP sobre diferentes segmentos de rede/segurança com inspeção profunda de segurança sobre este serviço.
- 3.1.2.9. Prover mecanismo contra-ataques de falsificação de endereços (IP Spoofing) através da especificação da interface de rede pela qual uma comunicação deve se originar;
- 3.1.2.15. Prover servidor DHCP Interno suportando múltiplos escopos de endereçamento para a mesma interface e a funcionalidade de DHCP Relay;
- 3.1.2.16. Prover a capacidade de encaminhamento de pacotes UDPs multicast/broadcast entre diferentes interfaces e zonas de segurança como DHCP Relay, suportando os protocolos e portas:
- ✓ Time service—UDP porta 37
 - ✓ DNS—UDP porta 53
 - ✓ DHCP—UDP portas 67 e 68



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE - SEA
INSTITUTO ESTADUAL DO AMBIENTE - INEA

- ✓ Net-Bios DNS—UDP porta 137
- ✓ Net-Bios Datagram—UDP porta 138
- ✓ Wake On LAN—UDP porta 7 e 9
- ✓ mDNS—UDP porta 5353

3.1.2.18. Implementar mecanismo de sincronismo de horário através do protocolo NTP. Para tanto o appliance deve realizar a pesquisa em pelo menos 03 servidores NTP distintos, com a configuração do tempo do intervalo de pesquisa;

3.1.2.19. Possuir mecanismo que permita que a conversão de endereços (NAT) seja feita de forma dependente do destino de uma comunicação, possibilitando que uma máquina, ou grupo de máquinas, tenham seus endereços convertidos para endereços diferentes de acordo com o endereço destino;

3.1.2.20. Suporte a Jumbo Frames;

3.1.2.21. Implementar sub-interfaces ethernet lógicas;

3.1.2.22. Suportar os seguintes tipos de NAT:

- ✓ Nat dinâmico (Many-to-1);
- ✓ Nat dinâmico (Many-to-Many);
- ✓ Nat estático (1-to-1);
- ✓ NAT estático (Many-to-Many);
- ✓ Nat estático bidirecional 1-to-1;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- ✓ Tradução de porta (PAT);
- ✓ NAT de origem;
- ✓ NAT de destino.

3.1.2.23. Suportar NAT de origem e NAT de destino simultaneamente;

3.1.2.24. Possuir gerenciamento de tráfego de entrada ou saída, por serviços, endereços IP e regra de firewall, permitindo definir banda mínima garantida e máxima permitida em porcentagem (%) para cada regra definida.

3.1.2.25. Implementar 802.1p e classe de serviços CoS (Class of Service) de DSCP (Differentiated Services Code Points);

3.1.2.26. Permitir remarcação de pacotes utilizando TOS e/ou DSCP;

3.1.2.27. Suporte a policy based routing (PBR), com a capacidade de roteamento por endereço de origem, endereço de destino, serviço, interface ou todas as opções simultâneas.

3.1.2.28. Suporte ao protocolo de roteamento multicast (PIM-SM);

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

3.1.2.30. Suportar Equal Cost Multi-Path (ECMP);

3.1.2.31. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

3.1.2.32. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3, RIPng);



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE - SEA
INSTITUTO ESTADUAL DO AMBIENTE - INEA

- 3.1.2.33. A solução deve suportar integralmente o padrão IPv6, assim como criação de regras com objetos que utilizem endereços IPv4 e IPv6;
- 3.1.2.34. Deve suportar no mínimo as seguintes funcionalidades ou protocolos para o padrão de endereçamento IPv6: Tunel 6 to 4, regras de acesso, objetos de endereço, limitador de conexões IPv6, monitor de conexões, DHCP, gerenciamento HTTPS via IPv6, NAT IPv6, proteção contra ataques do tipo IP Spoofing para IPv6, captura de pacotes IPv6, interface VLAN com endereço IPv6, VPN SSL com o uso do IPv6, controle de URL, Anti-Malware e antivírus, controle de aplicação, IPS, IKEv2, ICMP6, SNMP, alta disponibilidade, RFC 1981 Path MTU Discovery for IPv6, RFC 2460 IPv6 specification, RFC 2464 Transmission of IPv6 Packets over Ethernet Networks;
- 3.1.2.35. Possuir suporte ao protocolo SNMP versões 2 e 3;
- 3.1.2.36. Possui suporte a log via syslog;
- 3.1.2.37. Possuir mecanismo para possibilitar a aplicação de correções e atualizações para o firewall remotamente através da interface gráfica;
- 3.1.2.38. Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall;
- 3.1.2.39. Permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e as máquinas mais acessadas em um dado momento;
- 3.1.2.40. Permitir a visualização de estatísticas do uso de CPU do appliance o através da interface gráfica remota em tempo real.

3.1.3. Funcionalidades de Alta Disponibilidade

A solução deverá ter as seguintes funcionalidades:



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE - SEA
INSTITUTO ESTADUAL DO AMBIENTE - INEA

- 3.1.3.1. A solução deve ser entregue operando em alta disponibilidade (HA) no modo Ativo/Standby com as implementações de Failover;
- 3.1.3.2. Possuir mecanismo de Alta Disponibilidade operando em modo Ativo/Standby com as implementações de Failover;
- 3.1.3.3. Não serão permitidas soluções de cluster (HA) que façam com que o(s) equipamento(s) reinicie(m) após qualquer modificação de parâmetro/configuração realizada pelo administrador;
- 3.1.3.4. O recurso de Alta Disponibilidade deverá ser suportado em modo Bridge;
- 3.1.3.5. A solução deve ter capacidade de fazer monitoramento físico das interfaces dos membros do cluster;
- 3.1.3.6. A solução deve operar em alta disponibilidade implementando monitoramento lógico de um host na rede, para verificar a existência de problemas lógicos na rede e possibilitar Failover;
- 3.1.3.7. A solução deve permitir o uso de endereço MAC virtual para evitar problemas de expiração de tabela ARP em caso de Failover;
- 3.1.3.8. A solução deve possibilitar a sincronização de todas as configurações realizadas na caixa principal do cluster, incluindo - mas não limitado a objetos, regras, rotas, VPNs e políticas de segurança;
- 3.1.3.9. A solução deve permitir visualizar no equipamento principal, o status da comunicação entre o peers do cluster, status de sincronização das configurações, status atual equipamento do equipamento standby.

3.1.4. Funcionalidades de VPN (Virtual Private Network)

A solução deverá ter as seguintes funcionalidades:





GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- 3.1.4.1. Criptografia 3DES, AES 128 e AES 256;
- 3.1.4.2. Autenticação com MD5, SHA-1, SHA-256 e SHA-384;
- 3.1.4.3. Diffie-Hellman: Grupo 2 (1024 bits), Grupo 5 (1536 bits) e Grupo 14 (2048 bits);
- 3.1.4.4. Algoritmo Internet Key Exchange (IKE);
- 3.1.4.5. Autenticação via certificado IKE PKI;
- 3.1.4.6. Deve possuir interoperabilidade com outros fabricantes de acordo com o padrão IPSEC através de RFC's;
- 3.1.4.7. A solução deve suportar VPNs L2TP, incluindo suporte para iPhone, Windows phone, Android com suporte a cliente L2TP;
- 3.1.4.8. Solução deve suportar VPNs baseadas em políticas e VPNs baseadas em roteamento estático e dinâmico.
- 3.1.4.9. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.
- 3.1.4.10. Solução deve incluir a capacidade de estabelecer VPNs com outros firewalls que utilizam IP públicos dinâmicos;
- 3.1.4.11. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do circuito primário;
- 3.1.4.12. Permitir que seja criado políticas de roteamentos estáticos utilizando IPs de origem, destino, serviços e a própria VPN como parte encaminhadora deste tráfego sendo este visto pela regra de



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

roteamento, como uma interface simples de rede para encaminhamento do tráfego.

3.1.4.13. Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet.

3.1.5. Funcionalidades de Prevenção de Intrusão

A solução deverá ter as seguintes funcionalidades:

3.1.5.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio appliance de firewall, onde sua console de gerência deverá residir na mesma console centralizada dos appliances de segurança, com suporte a pelo menos 3.000 assinaturas;

3.1.5.2. A solução de IPS deverá possuir os seguintes mecanismos de detecção: assinaturas e trabalhar em conjunto com o controle de aplicações;

3.1.5.3. A solução de IPS deve fazer a inspeção de todo o pacote, independentemente do tamanho;

3.1.5.4. A solução de IPS deve fazer a inspeção de todo o tráfego de forma bidirecional, analisando qualquer tamanho de pacote sem degradar a performance do equipamento solicitada neste edital;

3.1.5.5. Possuir capacidade de remontagem de pacotes para identificação de ataques;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- 3.1.5.6. O mecanismo de inspeção deve receber e implementar em tempo real atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance;
- 3.1.5.7. Para cada proteção de segurança, deve ser possível consultar informações no site do fabricante.
- 3.1.5.8. A ferramenta de log deve possuir a capacidade de criar uma regra de exceção a partir do log visualizado na grência centralizada;
- 3.1.5.9. As regras de exceção devem possuir: origem, destino e serviço;
- 3.1.5.10. A solução deve ser capaz de inspecionar tráfego HTTPS.
- 3.1.5.11. Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;
- 3.1.5.12. A solução de IPS deve possuir política capaz de definir o modo de operação (bloqueio ou detecção);
- 3.1.5.13. O módulo de IPS deve possuir assinaturas voltadas para ambientes de servidores de SMTP, Web e DNS;
- 3.1.5.14. O mecanismo de inspeção deve receber e implementar em tempo real atualizações de novas assinaturas sem a necessidade de reiniciar o appliance;
- 3.1.5.15. Para cada proteção, ou para todas as proteções suportadas, deve incluir a opção de adicionar exceções baseado na origem e destino;
- 3.1.5.16. A solução deve ser capaz de detectar e bloquear ataques nas camadas de rede e aplicação, protegendo pelo menos os seguintes serviços: Aplicações web, serviços de e-mail, DNS, FTP, SQL Injection, ataques a sistemas operacionais e VOIP;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- 3.1.5.17. Deve incluir proteção contra worms;
- 3.1.5.18. Deve incluir uma tela de visualização situacional a fim de monitorar graficamente a quantidade de alertas de diferentes severidades e a evolução ao longo do tempo dispondo o sumário quantitativo das ameaças analisadas;
- 3.1.5.19. A solução deve possuir esquema de atualização de assinaturas através de um click;
- 3.1.5.20. Atualização de modo offline, onde poder ser baixado na base do fabricante e posteriormente fazer o upload do arquivo na solução;
- 3.1.5.21. A solução deve suportar importar certificados de servidor para inspeções de tráfego seguro HTTP (HTTPS) de entrada. Depois de importar esses certificados, a solução deve permitir o IPS para Inspeção segura HTTP(HTTPS);
- 3.1.5.22. A solução deverá ser capaz de inspecionar e proteger apenas hosts internos;
- 3.1.5.23. A solução deverá possuir proteções para sistemas SCADA;
- 3.1.5.24. Solução deverá permitir que o administrador bloqueie facilmente o tráfego de entrada e/ou saída com base em países, sem a necessidade de gerir manualmente os ranges de endereços IP dos países que deseja bloquear;
- 3.1.5.25. Possibilitar operação em modo de detecção baseado em base de assinaturas SNORT;
- 3.1.5.26. O Sistema de detecção e proteção de intrusão deverá estar orientado à proteção de redes;
- 3.1.5.27. Possuir tecnologia de detecção baseada em assinatura;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- 3.1.5.28. Possuir capacidade de remontagem de pacotes para identificação de ataques;
- 3.1.5.29. Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas à webserver para que seja usado para proteção específica de Servidores Web;
- 3.1.5.30. Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;
- 3.1.5.31. Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos sem intervenção do administrador
- 3.1.5.32. Reconhecimento de padrões;
- 3.1.5.33. Análise de protocolos;
- 3.1.5.34. Detecção de anomalias;
- 3.1.5.35. Detecção de ataques de RPC (Remote procedure call);
- 3.1.5.36. Proteção contra ataques DNS (Domain Name System);
- 3.1.5.37. Proteção contra ataques de ICMP (Internet Control Message Protocol);
- 3.1.5.38. Suportar reconhecimento de ataques de DDoS, reconnaissance, exploits e evasion;

3.1.6. Funcionalidades de Filtro de Conteúdo

A solução deverá ter as seguintes funcionalidades:





GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE - SEA
INSTITUTO ESTADUAL DO AMBIENTE - INEA

- 3.1.6.1. Para prover maior visibilidade e controle dos acessos dos usuários do ambiente, deve ser incluído um módulo de filtro de URL integrado no firewall;
- 3.1.6.2. Possuir base contendo no mínimo 20 milhões de sites internet web já registrados e classificados com atualização automática;
- 3.1.6.3. Implementar filtro de conteúdo transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes;
- 3.1.6.4. Permitir a criação de listas personalizadas de URLs permitidas e bloqueadas (lista branca e lista negra);
- 3.1.6.5. Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- 3.1.6.6. Possibilitar à criação de políticas por usuários, grupos de usuários, IPs, redes e grupos de redes;
- 3.1.6.7. O mecanismo de Controle de aplicação Web/URL deve apresentar contagem de utilização de regra de acordo com a utilização (hit count);
- 3.1.6.8. Permitir criar política de confirmação de acesso
- 3.1.6.9. Possibilitar a inspeção de tráfego HTTPS (Inbound/Outbound), sendo que para a opção de Outbound não será necessário efetuar o "man-in-the-middle", ou seja, a solução deverá prover mecanismo que irá analisar a conexão HTTPS para verificar se a URL solicitada está na lista de permissões de acesso, de acordo com a política configurada;
- 3.1.6.10. Permitir ao administrador adicionar filtros por palavra-chave de modo específico;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE - SEA
INSTITUTO ESTADUAL DO AMBIENTE - INEA

- 3.1.6.11. Permitir o bloqueio Web através de senha pré configura pelo administrador;
- 3.1.6.12. 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);
- 3.1.6.13. Fornecer mecanismo para solicitação de categorização de URL caso esta não esteja categorizada ou categorizada incorretamente;
- 3.1.6.14. Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD; o perfil de cada usuário deverá ser obtido automaticamente, para o controle das políticas de Filtro de Conteúdo sem a necessidade de uma nova autenticação.
- 3.1.6.15. Suportar a criação de políticas baseadas no controle por URL e categoria de URL;
- 3.1.6.16. Suportar base ou cache de URLs local no appliance ou possibilitar a replicação da base de conhecimento de URLs do fabricante via instalação de máquina virtual, a infraestrutura da máquina virtual (VM) para uso desse recurso será fornecida pelo CONTRATANTE, evitando delay de comunicação/validação das URLs;
- 3.1.6.17. Possuir pelo menos 50 categorias de URLs;
- 3.1.6.18. Suportar a criação de categorias de URLs customizadas;
- 3.1.6.19. Suportar a exclusão de URLs do bloqueio, por categoria;
- 3.1.6.20. Possibilitar a categorização ou recategorização de URL caso não esteja categorizada ou categorizada incorretamente;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

3.1.6.21. Permitir um mecanismo que permita sobrescrever as categorias de URL;

3.1.6.22. Permitir a customização de página de bloqueio.

3.1.7. Funcionalidades de Controle de Aplicações

Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidade abaixo:

3.1.7.1. Possibilitar a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;

3.1.7.2. Realizar filtragens/inspeções dentro de portas TCP conhecidas por exemplo porta 80 http, buscando por aplicações que potencialmente expõe o ambiente como: P2P, Kazaa, Morpheus, BitTorrent ou messengers;

3.1.7.3. Controlar o uso dos serviços de Instant Messengers como MSN, YAHOO, Google Talk, ICQ, de acordo com o perfil de cada usuário ou grupo de usuários, de modo a definir, para cada perfil, se ele pode ou não realizar download e/ou upload de arquivos, limitar as extensões dos arquivos que podem ser enviados/recebidos e permissões e bloqueio de sua utilização baseados em horários pré-determinados pelo administrador será obrigatório para este item;

3.1.7.4. Controlar software FreeProxy tais como ToR, Ultrasurf, Freegate etc.;

3.1.7.5. Permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

3.1.7.6. Permitir a criação de regras para acesso/bloqueio por subrede de origem e destino;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- 3.1.7.7. Atualizar a base de assinaturas de aplicações automaticamente;
- 3.1.7.8. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD;
- 3.1.7.9. Criar regras granulares possibilitando adicionar tipos de aplicação WEB e categorias por regra, sendo assim criando controle granular de qualquer tipo de acesso não permitido pela empresa;
- 3.1.7.10. Implementar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e protocolos;
- 3.1.7.11. Caso a solução não tenha assinaturas pré-definida, a mesma deverá possibilitar a criação ou importação de assinaturas personalizadas para os seguintes tipos ou protocolos: HTTP, FTP, Email e extensão de arquivos.
- 3.1.7.12. O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados a partir de comandos FTP pré-definidos;
- 3.1.7.13. Possibilitar que o controle de portas seja aplicado para todas as aplicações;
- 3.1.7.14. Possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, uTorrent, etc.) possuindo granularidade de controle/políticas para os mesmos;
- 3.1.7.15. Possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Facebook e bloquear chat;
- 3.1.7.16. Possibilitar a diferenciação de aplicações Proxies possuindo granularidade de controle/políticas para os mesmos;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

3.1.7.17. Possibilitar a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:

- ✓ Nível de risco da aplicação.
- ✓ Categoria de aplicações.

3.1.8. Proteção Contra Vírus e Bot-nets

A solução deverá ter as seguintes funcionalidades:

- 3.1.8.1. Possuir módulo de antivírus e anti-bot integrado no próprio appliance de segurança;
- 3.1.8.2. Possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliances através de assinaturas;
- 3.1.8.3. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;
- 3.1.8.4. Implementar funcionalidade de detecção e bloqueio de callbacks;
- 3.1.8.5. Ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE - SEA
INSTITUTO ESTADUAL DO AMBIENTE - INEA

- 3.1.8.6. Possuir mecanismo de detecção que inclui, reputação de endereço IP;
- 3.1.8.7. Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS.
- 3.1.8.8. Implementar interface CLI segura através do protocolo SSH;
- 3.1.8.9. Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, FTP, CIFS e TCP Stream;
- 3.1.8.10. Permitir criar regras de exceção de acordo com a proteção;
- 3.1.8.11. Possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts ou incidentes referentes a incidentes de vírus e Bots;
- 3.1.8.12. Permitir o bloqueio de malwares (vírus, worms, spyware e etc);
- 3.1.8.13. Ser capaz de proteger contra ataques para DNS;
- 3.1.8.14. A solução deverá ser gerenciada a partir de uma console centralizada com políticas granulares;
- 3.1.8.15. Ser capaz de prevenir acesso a websites maliciosos;
- 3.1.8.16. Ser capaz de realizar inspeção de tráfego SSL e SSH;
- 3.1.8.17. Receber atualizações de um serviço baseado em cloud;
- 3.1.8.18. Ser capaz de bloquear a entrada de arquivos maliciosos;
- 3.1.8.19. Suportar análise de arquivos que trafegam dentro do protocolo CIFS;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

3.1.8.20. A solução deve suportar funcionalidade de GeolP, ou seja, a capacidade de identificar, isolar e controlar tráfego baseado na localização (origem e/ou destino), incluindo a capacidade de configuração de listas customizadas para esta mesma finalidade.

3.1.9. Funcionalidades de Autenticação

A solução deverá ter as seguintes funcionalidades:

- 3.1.9.1. Permitir a utilização de LDAP, AD (Active Directory) e RADIUS;
- 3.1.9.2. Permitir o cadastro manual dos usuários e grupos diretamente na interface de gerencia remota do Firewall, caso onde se dispensa um autenticador remoto para o mesmo;
- 3.1.9.3. Suporte a uma rede com multiplus dominios, possibilitando a integração em um ambiente onde existas dominios diferentes e totalmente segregados.
- 3.1.9.4. Permitir a integração com qualquer autoridade certificadora emissora de certificados X509 que seguir o padrão de PKI descrito na RFC 2459, inclusive verificando as CRLs emitidas periodicamente pelas autoridades, que devem ser obtidas automaticamente pelo firewall via protocolos HTTP e LDAP;
- 3.1.9.5. Permitir o controle de acesso por usuário, para plataformas Windows Me, NT, 2000, 2000, XP, Windows 7, Windows 8 e Windows 10 de forma transparente, para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado;
- 3.1.9.6. Permitir a restrição de atribuição de perfil de acesso à usuário ou grupo independente ao endereço IP da máquina que o usuário esteja utilizando;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

3.1.9.7. Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD (Active Directory); o perfil de cada usuário deverá ser obtido automaticamente através de regras no Firewall DPI (Deep Packet Inspection) sem a necessidade de uma nova autenticação como por exemplo, para os serviços de navegação a Internet atuando assim de forma toda transparente ao usuário. Serviços como HTTP, HTTPS devem apenas consultar uma base de dados de usuários e grupos de servidores 2008/2012 com AD (Active Directory);

3.1.9.8. O INEA irá fornecer a infraestrutura de hardware e software (servidor e sistema operacional Windows Server) para instalação de componente de software ou agente necessário para a solução de autenticação integrada (single-sign-on) no Active Directory, de acordo com os requisitos do fabricante.

3.1.10. Funcionalidades Contra Ataques Avançados (Sandbox)

A solução deverá ter as seguintes funcionalidades:

3.1.10.1. Prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de callbacks;

3.1.10.2. Suportar os protocolos HTTP assim como inspeção de tráfego criptografado através de HTTPS e TLS;

3.1.10.3. Ser capaz de inspecionar o tráfego criptografado SSL e SSH;

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



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- 3.1.10.5. Implementar mecanismo de bloqueio de vazamento não intencional de dados oriundos de máquinas existentes no ambiente LAN em tempo real;
- 3.1.10.6. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF com até 10Mb;
- 3.1.10.7. Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows XP, Windows 7, Windows 10, MacOS, Android, Linux;
- 3.1.10.8. Conter ameaças de dia zero permitindo ao usuário final o recebimento dos arquivos livres de malware;
- 3.1.10.9. A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas;
- 3.1.10.10. Possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliance através de assinaturas;
- 3.1.10.11. Implementar a visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados;
- 3.1.10.12. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;
- 3.1.10.13. Conter ameaças avançadas de dia zero;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- 3.1.10.14. Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador;
- 3.1.10.15. Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos;
- 3.1.10.16. Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos;
- 3.1.10.17. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx) e Android APKs no ambiente controlado;
- 3.1.10.18. Implementar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;
- 3.1.10.19. Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, FTP, IMAP e CIFS;
- 3.1.10.20. Conter ameaças de dia zero de forma transparente para o usuário final;
- 3.1.10.21. Conter ameaças de dia zero através de tecnologias em nível de emulação e código de registro;
- 3.1.10.22. Implementar mecanismo de pesquisa por diferentes intervalos de tempo;
- 3.1.10.23. Conter ameaças de dia zero via tráfego de internet;
- 3.1.10.24. Permitir a contenção de ameaças de dia zero sem a alteração da infraestrutura de segurança;
- 3.1.10.25. Conter ameaças de dia zero que possam burlar o sistema operacional emulado;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- 3.1.10.26. Permitir a criação de White list baseado no MD5 do arquivo;
- 3.1.10.27. Conter ameaças de dia zero antes da execução e evasão de qualquer código malicioso;
- 3.1.10.28. Conter exploits avançados;
- 3.1.10.29. A 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 Antispyware automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover Informações sobre o usuário infectado (seu endereço IP e seu login de rede);
- 3.1.10.30. Suporte a submissão manual de arquivos para análise através do serviço de Sandbox.

3.1.11. Funcionalidades de Administração

A solução deverá ter as seguintes funcionalidades:

- 3.1.11.1. Suportar no mínimo 20.000 usuários autenticados com serviços ativos e identificados passando por este dispositivo de segurança em um único dispositivo de segurança. Políticas baseadas por grupos de usuários deverão ser suportadas por este dispositivo. Esta comprovação poderá ser exigida em testes sobre o ambiente de produção com o fornecimento do produto para comprovação deste e demais itens;
- 3.1.11.2. Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o firewall, cada um responsável por determinadas tarefas da administração;
- 3.1.11.3. Fornecer gerência remota, com interface gráfica nativa;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- 3.1.11.4. A interface gráfica deverá possuir assistentes para facilitar a configuração inicial e a realização das tarefas mais comuns na administração do firewall, incluindo a configuração de VPN IPSECs, NAT, perfis de acesso e regras de filtragem;
- 3.1.11.5. Possuir mecanismo que permita a realização de cópias de segurança (backups) e sua posterior restauração remotamente, através da interface gráfica, sem necessidade de se reinicializar o sistema;
- 3.1.11.6. Possuir mecanismo para possibilitar a aplicação de correções e atualizações para o firewall remotamente através da interface gráfica;
- 3.1.11.7. Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall e a remoção de qualquer uma destas sessões ou conexões;
- 3.1.11.8. Permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e as máquinas mais acessadas em um dado momento;
- 3.1.11.9. Permitir a visualização de estatísticas do uso de CPU, memória da máquina onde o firewall está rodando e tráfego de rede em todas as interfaces do Firewall através da interface gráfica remota, em tempo real e em forma tabular e gráfica;
- 3.1.11.10. Permitir a conexão simultânea de vários administradores, sendo um deles com poderes de alteração de configurações e os demais apenas de visualização das mesmas. Permitir que o segundo ao se conectar possa enviar uma mensagem ao primeiro através da interface de administração;
- 3.1.11.11. Possibilitar o registro de toda a comunicação realizada através do firewall, e de todas as tentativas de abertura de sessões ou conexões que forem recusadas pelo mesmo;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- 3.1.11.12. Possuir interface orientada a linha de comando para a administração do firewall a partir do console ou conexão SSH sendo está múltiplas sessões simultâneas;
- 3.1.11.13. Possuir mecanismo que permita inspecionar o tráfego de rede em tempo real (sniffer) via interface gráfica, podendo opcionalmente exportar os dados visualizados para arquivo formato PCAP e permitindo a filtragem dos pacotes por protocolo, endereço IP origem e/ou destino e porta IP origem e/ou destino, usando uma linguagem textual;
- 3.1.11.14. Permitir a visualização do tráfego de rede em tempo real tanto nas interfaces de rede do Firewall quando nos pontos internos do mesmo: anterior e posterior à filtragem de pacotes, onde o efeito do NAT (tradução de endereços) é eliminado;
- 3.1.11.15. Possuir sistema de respostas automáticas que possibilite alertar imediatamente o administrador através de e-mails, janelas de alerta na interface gráfica, execução de programas e envio de Traps SNMP.

3.1.12. Funcionalidades de Relatórios

A solução deverá ter as seguintes funcionalidades:

- 3.1.12.1. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps, URLs acessadas e ameaças identificadas;
- 3.1.12.2. Possibilitar a geração de pelo menos os seguintes tipos de relatório com cruzamento de informações, mostrados em formato HTML: máquinas acessadas X serviços bloqueados, usuários X URLs acessadas, usuários X categorias Web bloqueadas (em caso de utilização de um filtro de conteúdo Web);



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- 3.1.12.3. Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (em caso de existência de um filtro de conteúdo Web), maiores emissores e receptores de e-mail;
- 3.1.12.4. Permitir o envio dos relatórios, através de email para usuários pré-definidos;
- 3.1.12.5. Possuir relatórios pré-definidos na solução e permitir a criação de relatórios customizados;
- 3.1.12.6. Possibilitar a geração dos relatórios sob demanda e através de agendamento diário, semanal e mensal. No caso de agendamento, os relatórios deverão ser publicados de forma automática;
- 3.1.12.7. Disponibilizar download dos relatórios gerados.

3.1.13. Garantia, suporte e licenciamento

- 3.1.13.1. O licenciamento para todos os produtos de Next Generation Firewall deverá ser de 24 (vinte e quatro) meses;
- 3.1.13.2. A garantia deverá ser de 24 (vinte e quatro) meses;
- 3.1.13.3. Deve contemplar suporte do Fabricante pelo período vigente e com, no mínimo, as seguintes características:
 - ✓ O suporte do fabricante deve ter um sistema de abertura de chamados para acompanhamento – funcionando 24 horas por dia e 7 dias por semana. Para atendimento telefônico, deve operar em língua Portuguesa pelo menos em regime 8x5;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- ✓ Deve assegurar a utilização de novas versões de software da solução sem ônus a Licitante, sempre que esta estiver disponível a qualquer cliente;
- ✓ Deve permitir o acesso à base de conhecimento da solução.

3.1.14. Conformidade

- 3.1.14.1. O Fabricante deve comprovar participação no MAPP da Microsoft;
- 3.1.14.2. A tecnologia deve possuir pelo menos uma certificação da ICSA Labs, ICSA Firewall ou Antivírus;
- 3.1.14.3. O fabricante da solução deverá ser avaliado pela NSS Labs (Network Security Services) no desempenho do Next Generation Firewall Comparative Analysis do ano anterior, estando no “Security Value Map” acima de 90% (noventa por cento) da avaliação de segurança efetiva;
- 3.1.14.4. No momento da entrega dos equipamentos a proponente vencedora deverá fornecer declaração do(s) fabricante(s), em papel timbrado com firma reconhecida, dos produtos ofertados, declarando que a proponente possui credenciamento do mesmo para a implantação e suporte técnico de seus produtos;
- 3.1.14.5. O equipamento deve ser homologado pela ANATEL.



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

3.2. Solução de Segurança para Proteção de Servidores Virtuais e Físicos

3.2.1. Características Gerais

- 3.2.1.1. A solução deverá ser licenciada para 60 (sessenta) servidores, no modelo de subscrição anual, garantindo o uso do produto durante do período contratual (24 meses);
- 3.2.1.2. A solução deverá ter o console de gerenciamento na nuvem, não sendo necessário a instalação de servidores nas dependências do INEA;
- 3.2.1.3. As licenças devem ser fornecidas com os módulos de Firewall, Inspeção de Pacotes, Controle de Acesso a Sites Maliciosos, Anti-malware, Monitoramento de Integridade, Controle de Aplicações, HIPS e Inspeção Avançada de Tráfego, sem a necessidade de instalação de agente para ambiente VMWare v6 ou ambiente com NSX;
- 3.2.1.4. Deverá suportar, no mínimo, as seguintes Distribuições: Suse Linux enterprise 11; Red Hat enterprise Linux 6.0 e 7.0; CentOS 6.0 e 7.0;
- 3.2.1.5. Todos componentes que fazem parte da solução devem ser do mesmo fabricante;
- 3.2.1.6. Precisa ter a capacidade de controlar e gerenciar a segurança de múltiplas plataformas e sistemas operacionais a partir de uma console única e centralizada do próprio fabricante;
- 3.2.1.7. A solução deverá ser gerenciada por console Web. Deve suportar certificado digital para gerenciamento;
- 3.2.1.8. A console de administração deverá permitir o envio de notificações via SMTP;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- 3.2.1.9. A solução deve poder enviar os logs para um dispositivo SIEM (Security Information and Event Management);
- 3.2.1.10. Todos os eventos e ações realizadas na console de gerenciamento precisam ser gravados para fins de auditoria;
- 3.2.1.11. A solução deverá permitir que a distribuição de patterns e novos componentes possa ser efetuada automaticamente em diversos pontos do ambiente;
- 3.2.1.12. A solução deverá permitir a criação de múltiplos perfis de segurança, que serão vinculados aos diferentes tipos de servidores do ambiente;
- 3.2.1.13. A solução precisa permitir a criação de relatórios. A criação e envio destes relatórios deverá ocorrer sob demanda, ou agendado com o envio automático do relatório via e-mail;
- 3.2.1.14. A solução deverá a criação de relatórios no formato PDF;
- 3.2.1.15. O console de gerenciamento deve apresentar alta disponibilidade em nível de aplicação, através da criação de várias gerências, de modo que na ausência da principal, os clientes automaticamente se comuniquem com a secundária e com todas as configurações preservadas;
- 3.2.1.16. O console de gerenciamento deve armazenar políticas e logs em base de dados. A escolha da base de dados pode ser facultativa entre Oracle ou MSSQL;
- 3.2.1.17. Quando operadas em modo alta disponibilidade, as consoles devem compartilhar o mesmo database;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- 3.2.1.18. O console deve se integrar com o Active Directory para que os usuários do Active Directory possam administrar a solução, com permissões customizadas pela própria solução;
- 3.2.1.19. Os usuários devem ter a capacidade de receber determinados papéis para administração como "acesso total" e "acesso parcial", podendo ser customizado o que compõe o "acesso parcial";
- 3.2.1.20. Quando configurado o acesso parcial, este deve permitir que um usuário possa gerenciar a segurança de um único computador, podendo ainda definir em quais módulos de proteção será possível editar ou criar novas políticas de segurança;
- 3.2.1.21. A console deve se integrar com o Active Directory para que possa ser efetuado o controle das máquinas no Active Directory;
- 3.2.1.22. A comunicação entre a console de gerenciamento e componentes de proteção deverá ser criptografada;
- 3.2.1.23. A console de gerenciamento deverá ter dashboards para facilidade de monitoração, as quais deverão ser customizadas pelo administrador em quantidade e período de monitoração;
- 3.2.1.24. Os componentes de atualização deverão buscar os updates das assinaturas e distribuí-las;
- 3.2.1.25. O console de gerenciamento deverá ser gerenciado por Internet Explorer, Chrome e Firefox;
- 3.2.1.26. A solução deve possuir a capacidade de criar políticas de forma global para todas as máquinas, por perfis e individualmente para cada host;
- 3.2.1.27. Cada perfil poderá ser atribuído para um host ou um conjunto de hosts;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- 3.2.1.28. A solução deverá vir com perfis padrão pré-definidos;
- 3.2.1.29. A solução deve possuir a capacidade de isolamento de placa de rede, de forma que impeça a comunicação entre placas de rede do mesmo host, de acordo com definição do administrador;
- 3.2.1.30. A solução deverá ser capaz de aplicar políticas de firewall diferentes para placas de redes diferentes em um mesmo host;
- 3.2.1.31. A solução deverá ser capaz de executar by-pass completo de rastreamento de tráfego de forma que os módulos não atuem em determinado tipo de conexão ou pacote;
- 3.2.1.32. A solução deverá ser capaz de reconhecer e bloquear endereços IP que estejam realizando Network Scan, Port Scan, TCP Null Scan, TCP SYNFIN Scan, TCP Xmas Scan e Computer OS Fingerprint;
- 3.2.1.33. A solução deverá ter a possibilidade de enviar logs para SYSLOGS;
- 3.2.1.34. A solução deverá ter a possibilidade de enviar eventos da console via SNMP;
- 3.2.1.35. Solução deverá apresentar relatórios customizados de todas as suas funcionalidades;
- 3.2.1.36. Os relatórios deverão poder ser exportados nos formatos PDF;
- 3.2.1.37. Deve permitir enviar os relatórios para uma lista de contatos independente de login na console de administração;
- 3.2.1.38. As atualizações de assinaturas deverão ocorrer de forma agendada e automática;
- 3.2.1.39. Deve ser possível baixar as assinaturas na console de gerenciamento, mas não as distribuídas aos componentes de proteção;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- 3.2.1.40. A solução deverá ter capacidade de gerar pacote de auto diagnóstico de modo a coletar arquivos relevantes para envio ao suporte do produto;
- 3.2.1.41. No gerenciamento das licenças, deve ser informada a quantidade contratada, assim como, a quantidade em utilização de componentes de proteção;
- 3.2.1.42. Solução deverá ter mecanismo de procura em sua console de gerenciamento de modo que seja facilitada a busca de regras;
- 3.2.1.43. Possibilidade de identificação dos IPs que estejam realizando ataques;
- 3.2.1.44. O fabricante deverá participar do programa “Microsoft Active Protection Program” para obtenção de informações de modo a permitir a criação de regras de proteção antes mesmo dos patches serem publicados pelo fabricante;
- 3.2.1.45. O console de gerenciamento deve se integrar com o VMware vCenter 5.1 ou Superior, de modo a importar e sincronizar os objetos (hosts VMware e guests vm) para o console de gerenciamento da solução;
- 3.2.1.46. A partir desta integração, deverá ser possível gerir a segurança dos guests vm, podendo ser atribuídos perfis de segurança, regras únicas para cada host, além de possibilitar a coleta dos logs gerados para cada módulo habilitado;
- 3.2.1.47. Esta integração deve possibilitar que, a partir da instalação e integração de um virtual appliance do fabricante da solução de segurança com o ambiente VMware e suas APIs, seja possível proteger as guests vms sem a necessidade de instalação de agentes de segurança do fabricante da solução nas guests vms;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

3.2.1.48. Este virtual appliance deverá integrar-se com o VMware NSX, possibilitando que no mínimo 3 funcionalidades possam ser efetuadas diretamente via hypervisor e virtual appliance em conjunto, não necessitando a instalação de agentes adicionais de segurança do fabricante nos guests VMs protegidos. Dentre as funcionalidades, estão incluídas apenas:

- ✓ Firewall
- ✓ Anti-malware
- ✓ Controle de Acesso a Sites Maliciosos
- ✓ Controle de Aplicações
- ✓ Monitoramento de Integridade
- ✓ IDS/IPS

3.2.1.49. Precisa ter a capacidade de detectar e aplicar as regras necessárias do módulo de IDS/IPS, para cada servidor através da console de administração;

3.2.1.50. A console de gerenciamento deve permitir a utilização do mesmo perfil de segurança para servidores virtuais, físicos e desktops virtuais;

3.2.1.51. A solução deverá ter a capacidade de proteger automaticamente os servidores que são adicionados ao ambiente com perfil de segurança pré-definido pelo administrador;

3.2.1.52. Para virtualização em ambiente Hyper-V (Microsoft Windows Server 2008 R2 com Hyper-V e/ou Microsoft Windows Server 2012 com Hyper-V), a solução deverá integrar-se com a utilização de agente, possibilitando a execução das funcionalidades de Anti-malware, Web



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

Reputation, Firewall, IDS/IPS, Monitoramento de Integridade e Controle de Aplicações;

3.2.2. Características para Firewall de Host

- 3.2.2.1. Operar como firewall de host para proteção dos servidores virtualizados;
- 3.2.2.2. Precisa ter a capacidade de controlar o tráfego baseado no Endereço IP, Tipos de Protocolos e intervalo de portas;
- 3.2.2.3. Precisa ter a capacidade de definir regras distintas para interfaces de rede distintas;
- 3.2.2.4. A solução deverá ser capaz de reconhecer e possibilitar o bloqueio endereços IP que estejam realizando Network Scan, Port Scan, TCP Null Scan, TCP SYNFIN Scan, TCP Xmas Scan e Computer OS Fingerprint;
- 3.2.2.5. Precisa ter a capacidade de implementação de regras em determinados horários que podem ser customizados pelo administrador;
- 3.2.2.6. Precisa ter a capacidade de definição de regras para contextos específicos;
- 3.2.2.7. Para facilitar a criação e administração de regras de firewall, as mesmas poderão ser baseadas em objetos que podem ser lista de IPs e lista de portas;
- 3.2.2.8. Regras de firewall poderão ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo se está no domínio ou não);
- 3.2.2.9. Regras de firewall poderão ser válidas de acordo com agendamento por horário ou dia da semana;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- 3.2.2.10. O firewall deverá ser stateful bidirecional;
- 3.2.2.11. As regras de Firewall deverão permitir, minimamente as ações de bloqueio, permissão e registro do tráfego;
- 3.2.2.12. O firewall deverá permitir a criação de regras através do protocolo, origem do tráfego, destino e direção;
- 3.2.2.13. As regras de Firewall deverão permitir, minimamente as ações de bloqueio, permissão e registro do tráfego;
- 3.2.2.14. A solução deverá utilizar o conceito de regras implícitas para a regra ALLOW, negando o tráfego para todo o restante que não estiver liberado;
- 3.2.2.15. A solução deve permitir a utilização de atribuição de prioridades diferentes as regras de firewall;
- 3.2.2.16. Deverá logar a atividade stateful;
- 3.2.2.17. Deverá prevenir ack storm;
- 3.2.2.18. Deverão existir regras padrão que facilitem a criação e adição de novas regras;

3.2.3. Características para Inspeção de Pacotes

- 3.2.3.1. Precisa ter a capacidade de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do S.O. e demais aplicações;
- 3.2.3.2. Precisa ter a capacidade de varrer o servidor protegido detectando o tipo e versão do S.O., detectando também as demais aplicações, recomendando e aplicando automaticamente regras IDS/IPS que



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

blindem vulnerabilidades existentes no S.O. e aplicações. Esta varredura deverá poder ser executada sob demanda ou agendada;

- 3.2.3.3. Precisa ter a capacidade de detectar uma conexão maliciosa, com a possibilidade de bloquear esta conexão. A opção de detecção e bloqueio deverá possibilitar a implementação de forma global (todas as regras) e apenas para uma regra ou grupos de regras;
- 3.2.3.4. Precisa conter ou permitir a customização de regras de defesa para blindagem de vulnerabilidades e ataques que explorem Windows 2003, 2008, 2012 e mais de 100 tipos de aplicações padrão de mercado, incluindo Microsoft IIS, SQL Server, Microsoft Exchange, Oracle Database, Adobe Acrobat, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome e Web Server Apache;
- 3.2.3.5. Precisa ter a capacidade de armazenamento do pacote capturado quando detectado um ataque;
- 3.2.3.6. Deverá possibilitar a criação de regras de IPS customizadas, para proteger aplicações desenvolvidas pelo cliente;
- 3.2.3.7. Precisa possuir a capacidade de detectar e controlar conexões de aplicações específicas incluindo Team Viewer, programas P2P e instant messaging;
- 3.2.3.8. Precisa ter a capacidade de detectar e bloquear ataques em aplicações Web tais como SQL Injections e Cross Site Scriptings. Deverá ainda existir a possibilidade de captura do pacote relacionado ao ataque para fins de investigação do incidente;
- 3.2.3.9. Deverá bloquear tráfego por aplicação independente da porta que a aplicação utilize, de modo que a aplicação não consiga comunicar na rede, como por exemplo: bloqueio de tráfego de um determinado web browser ou aplicação de backup;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- 3.2.3.10. Solução deve ser capaz de habilitar modo debug na coleta dos pacotes de forma a capturar o tráfego anterior e posterior ao que foi bloqueado para facilidade de análise;
- 3.2.3.11. As regras de IPS deverão obrigatoriamente ter descrições de seu propósito;
- 3.2.3.12. As regras de IPS poderão atuar detectando ou bloqueando os eventos que as violem de modo que o administrador possa optar por qual ação tomar;
- 3.2.3.13. As regras de IPS de vulnerabilidade deverão apresentar severidade baseada em CVSS;
- 3.2.3.14. As regras de IPS quando disparadas poderão ter a possibilidade de emitir um alerta;
- 3.2.3.15. As regras devem ser atualizadas automaticamente pelo fabricante;
- 3.2.3.16. Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas.

3.2.4. Características para Controle de Acesso a Sites Maliciosos

- 3.2.4.1. Permitir a proteção contra acesso a websites ou URLs consideradas maliciosas ou reputação ruim;
- 3.2.4.2. A lista de URLs deve ser fornecida e atualizada automaticamente pelo fabricante, permitindo a consulta em uma base local ou na nuvem da reputação das URLs acessadas;
- 3.2.4.3. Deve permitir a criação de listas de exclusão, permitindo que usuários acessem determinadas URLs especificadas pelo administrador do sistema;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

3.2.4.4. A solução de permitir o bloqueio de URLs com incidência de palavras chave definidas pelo administrador.

3.2.5. Características para Anti-malware

3.2.5.1. A solução deve permitir a proteção contra códigos maliciosos sem a necessidade da instalação de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e conforme agendamento, possibilitando a tomada de ações distintas para cada tipo de ameaça;

3.2.5.2. A solução deve possibilitar a criação de listas de exclusão, para que o processo do antivírus não execute a varredura de determinados diretórios ou arquivos do S.O.;

3.2.5.3. A solução deve possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção;

3.2.5.4. A solução deve possuir uma cache dos arquivos verificados de modo a evitar a redundância da varredura;

3.2.5.5. A cache de arquivos verificados deverá estar disponível para varredura sob demanda e varredura em tempo real;

3.2.5.6. Em ambientes Windows, deve ter capacidade de realizar inspeção e detecção sem vacina, especialmente para Ransomware e ataques de dia zero;

3.2.5.7. A solução deve ter capacidade de monitorar arquivos do sistema e softwares instalados contra mudanças não autorizadas, a fim de detectar e bloquear ameaças;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- 3.2.5.8. A solução deve ter capacidade de monitorar processos legítimos contra realizações de ações que não são tipicamente realizada pelos mesmos, a fim de detectar e bloquear ameaças;
- 3.2.5.9. A solução deve ter capacidade de monitorar documentos contra a criptografia;
- 3.2.5.10. A solução deve proteger Docker hosts.

3.2.6. Características para Monitoramento de Integridade

- 3.2.6.1. A solução deve permitir o monitoramento de integridade de arquivos na máquina virtual (VMWARE) a ser monitorada;
- 3.2.6.2. Precisa ter a capacidade de detectar mudanças de integridade em arquivos e diretórios do S.O. e aplicações terceiras;
- 3.2.6.3. Precisa ter a capacidade de monitorar o status de serviços e processos do sistema operacional;
- 3.2.6.4. Precisa ter a capacidade de monitorar mudanças efetuadas no registro do Windows;
- 3.2.6.5. Precisa ter a capacidade de criação de regras de monitoramento em chaves de registro, diretórios e subdiretórios e para criação de regras avançadas;
- 3.2.6.6. Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de monitoramento de acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada;
- 3.2.6.7. O monitoramento poderá ser realizado em Real-time ou utilizando de scans periódicos para detectar mudanças de integridade;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- 3.2.6.8. A solução deverá monitorar modificações em arquivos, pastas, registros, processos, serviços e portas;
- 3.2.6.9. Referente à integridade dos arquivos deverá rastrear por criação, última modificação, último acesso, permissões, owner, grupo, tamanho, Sha1, Sha256 e Flags;
- 3.2.6.10. Deverá alertar toda vez que uma modificação ocorrer;
- 3.2.6.11. Deverá logar e colocar em relatório todas as modificações que ocorreram;
- 3.2.6.12. As regras de monitoramento de integridade deverão ser atualizadas pelo fabricante ou melhoradas de forma automática;
- 3.2.6.13. O monitoramento deverá ocorrer em real time;
- 3.2.6.14. Deverá poder classificar as regras de acordo com severidade para melhor verificação nos logs e recebimento de alertas;
- 3.2.6.15. Deverá possibilitar escolher o diretório onde o arquivo será monitorado e incluir ou não incluir determinados tipos de arquivos dentro desse mesmo diretório;
- 3.2.6.16. Algumas regras podem ser modificadas pelo administrador para adequação ao seu ambiente.

3.2.7. Características para Controle de Aplicação

- 3.2.7.1. A solução deve permitir o controle de aplicações ao menos para Sistemas Operacionais Red Hat 6 e 7;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

3.2.7.2. Um scan deve ser rodado na máquina e todas as aplicações inicialmente instaladas devem ser consideradas seguras para uso, o chamado baseline.

3.2.8. Funcionalidade de HIPS – Host IPS e Host Firewall

3.2.8.1. Deve ser capaz de realizar a proteção contra-ataques nos seguintes sistemas operacionais:

3.2.8.1.1. Windows Server 2008 R2 e 2012 (32/64-bit);

3.2.8.2. Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host IPs e host firewall;

3.2.8.3. Todas as regras das funcionalidades de firewall e IPs de host devem permitir apenas detecção (log) ou prevenção (bloqueio);

3.2.8.4. Deve permitir ativar e desativar o produto sem a necessidade de remoção;

3.2.8.5. A funcionalidade de host IPs deve possuir regras para controle do tráfego de pacotes de determinadas aplicações;

3.2.8.6. Precisa conter ou permitir a customização de regras de defesa para blindagem de vulnerabilidades e ataques que explorem Windows 2003, 2008, 2012 e mais de 100 tipos de aplicações padrão de mercado, incluindo Microsoft IIS, SQL Server, Microsoft Exchange, Oracle Database, Adobe Acrobat, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome e Web Server Apache;

3.2.8.7. Deve permitir a criação de políticas de firewall diferenciadas em múltiplas placas de rede no mesmo sistema operacional;

3.2.8.8. Deve permitir a criação de políticas de segurança personalizadas;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- 3.2.8.9. Deve permitir a emissão de alertas via SMTP ou SNMP;
- 3.2.8.10. Deve permitir configuração e manipulação de políticas de firewall através de prioridades;
- 3.2.8.11. Deve permitir criação de regras de firewall utilizando os seguintes protocolos: icmp, icmpv6, tcp, udp, tcp+udp.
- 3.2.8.12. Deve permitir criação de regras de firewall por origem de ip ou mac ou porta e destino de ip ou mac ou porta;
- 3.2.8.13. Deve permitir a criação de regras de firewall pelos seguintes frames types: Ip, ipv4 e ipv6,
- 3.2.8.14. Deve permitir a criação de contextos para a aplicação para criação de regras de firewall;
- 3.2.8.15. Deve permitir o isolamento de interfaces de rede, possibilitando o funcionamento de uma interface por vez;
- 3.2.8.16. Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;
- 3.2.8.17. Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar a visualização e gerenciamentos;
- 3.2.8.18. A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação.



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

4. DESCRIÇÃO DOS SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DAS SOLUÇÕES DE SEGURANÇA

4.1. Serviço De Instalação, Configuração E Suporte Por 12 Meses - Solução De Segurança De Perímetro - Firewall/UTM

4.1.1. Descrição das atividades técnicas:

A CONTRATADA será responsável pelas atividades instalação, configuração, gerenciamento, administração e suporte de todos os equipamentos envolvidos na solução de segurança de perímetro - Firewall/UTM, a ser fornecida e instalada no INEA, de acordo com este termo de referência.

A CONTRATADA deverá garantir a continuidade dos serviços providos pela solução de Firewall/UTM, através de atividades de monitoração, administração, gerenciamento e suporte por 12 meses após a data de instalação da solução em ambiente de produção do INEA.

O projeto de instalação e configuração da solução deverá iniciar em até 5 (cinco) dias úteis após a entrega de todos dos equipamentos e softwares envolvidos na solução. Neste prazo deverá ser apresentado à gerência de TI do INEA o plano de projeto com os requisitos técnicos, cronograma, riscos e estratégia de migração para a nova solução de Firewall/UTM. O INEA deverá aprovar o plano de projeto em até dois (02) dias uteis, a partir da entrega da documentação.

O prazo para a instalação da solução de segurança de perímetro em pleno funcionamento no ambiente de produção do INEA é de 30 dias, após a aprovação do plano de projeto pela gerência de TI do INEA.

A equipe responsável pelo instalação, gerenciamento, administração e suporte da solução de firewall/ UTM deverá ser especializada e certificado pelo fabricante no produto fornecido para este termo de referência.



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

As atividades de instalação física e configuração lógica executadas pela CONTRATADA que tenham impacto direto no ambiente de produção do INEA deverão ser realizados de forma presencial nas dependências do INEA e preferencialmente fora do horário comercial. Atividades sem impacto no ambiente de produção poderão ser executadas remotamente, mediante acesso seguro e com a aprovação da gerência de TI do INEA.

São atividades do serviço de instalação e configuração da solução de firewall/UTM:

- Realizar mapeamento e documentação das regras, políticas e configurações, do ambiente de firewall/UTM atual para avaliação da Gerência de Tecnologia do INEA com o objetivo de eliminar regras redundantes, duplicadas, muito permissivas ou não utilizadas no novo ambiente. A documentação deverá ser entregue a área de segurança da informação do INEA para a sua revisão e aprovação.
- Definir em conjunto com a Gerência de Tecnologia do INEA, as regras de navegação e perfis de acesso com o objetivo de garantir que os funcionários tenham os acessos pertinentes às suas funções, permitindo o ambiente mais seguro.
- Implantar as regras, políticas e configurações no novo ambiente de firewall/UTM baseado do que foi revisado e aprovado pela área de segurança da informação do INEA.
- Implementar regras de filtragem com o objetivo de controlar o tráfego de entrada e saída baseados nos endereços IPs e portas definidas e aprovadas na fase de levantamento.
- Implementar regras de NAT (Network Address Translations) para publicação de serviços de TI hospedados na rede interna, para se comunicarem com o mundo externo, através de endereços IPs públicos.
- Implementar redes virtuais (VPN – Virtual Private Networks) para permitir acesso externo seguro à rede interna do INEA, através de um software



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

cliente instalado na estação do usuário (conexão cliente-to-site) e acesso permanente de uma rede privadas de fornecedores ou unidades remotas do INEA através de uma conexão VPN permanente (site-to-site).

- Implementar regras de QoS, controle de banda, análise e priorização de tráfego para as aplicações e serviços relevantes para a rede de dados de longa distância e internet.
- Implantar de forma proativa as práticas de segurança na infraestrutura de segurança de perímetro como backup das configurações, atualizações de firmwares e patches atualizações críticos, disponibilizados pelo fabricante da solução.
- Configurar a integração da solução de segurança de perímetro com o serviço de diretório Microsoft Active Directory do INEA para possibilitar a configuração e emissão de relatórios baseados no nome do usuário da rede local.
- Apontar vulnerabilidades, brechas de segurança ou qualquer inconformidade nas configurações da solução de Firewall/UTM atual, de acordo com as boas práticas de segurança, para a Gerência de TI do INEA, para sua avaliação e tomada de decisão.
- Gerar documentação do ambiente de solução de segurança de perímetro - Firewall/UTM, contemplando topologia e configurações implantadas.
- As mudanças serão submetidas para aprovação do gestor técnico do INEA, mediante a um formulário de requisição de mudanças (GMUD), que constará todas as informações.

O atendimento de suporte especializado deverá ser executado pela CONTRATADA preferencialmente de forma remota, mas em caso de necessidade de acesso físico ao ambiente para resolução do problema ou da atividade a ser executada, poderá ser realizado atendimento presencial nas dependências do INEA. Da mesma forma que a equipe de TI do INEA, poderá a qualquer momento, solicitar à CONTRATADA o atendimento presencial dependendo do impacto e urgência do incidente.

São atividades do atendimento de suporte especializado (2º nível) da solução de firewall/UTM:



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- Elaborar relatórios técnicos que subsidiem a análise de soluções, projetos, novas implantações, homologação de equipamentos e softwares, solicitações de auditoria, relacionados a Firewall/UTM.
- Manter documentação completa da instalação e funcionamento dos ativos, serviços de rede, inclusive topologias de rede, alta disponibilidade, redundância e sistemas de balanceamento de carga da Firewall/UTM.
- Analisar a viabilidade e impacto da instalação de novas soluções, equipamentos e serviços a serem implantados no INEA que tenham relacionamento com infraestrutura de segurança de perímetro, mediante a solicitação forma da equipe de TI do INEA.
- Prover relatórios relacionados ao desempenho de recursos de hardware, tráfego de rede de links de longa de longa distância e internet.
- Configurar perfis de acesso remoto, através do serviço VPN para usuários, usuários corporativos e parceiros/fornecedores solicitados pelo INEA.
- Fornecer suporte à instalação, configuração, substituição e remanejamento de hardware (firewalls, switches, servidores de SSO) e software relacionados à Firewall/UTM.
- Realizar suporte, mudanças ou atividades de troubleshooting em problemas relacionados à links de dados, redes de longa distância, Internet e roteamento da rede em conjunto com as operadoras de telecomunicações.
- Realizar suporte, mudanças ou atividades de troubleshooting em problemas relacionados conexões de vídeo/voz sobre IP da rede de dados local do INEA, em conjunto com as operadoras de telecomunicações ou fornecedores das soluções.
- Analisar relatórios de segurança providos pela solução de Firewall/UTM com o objetivo de recomendar ao INEA ações para correção de vulnerabilidades ou inconformidades identificadas.
- Analisar eventos de disponibilidade do firewall, com o objetivo de minimizar ou evitar impactos na infraestrutura do INEA atuando de maneira proativa em caso de falhas de hardware.
- Analisar eventos de capacidade, ou seja, utilização física da banda (bandwidth) dos links de comunicação de dados (Internet/MPLS/VPNs), prevenido gargalhos de rede que possam impactar o dia a dia das operações.



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- Analisar o registro (logs) do(s) firewall, que foram correlacionados e priorizados pela ferramenta, onde os eventos de segurança relevantes deverão ser categorizados com base no nível de gravidade e propostas ações de mitigação de riscos.
- Redirecionar os incidentes para outros grupos solucionadores, caso a falha não seja um erro conhecido, ou seja, escopo do atendimento de suporte 2º nível. Como por exemplo, o acionamento do suporte 3º nível do fabricante da Firewall/UTM.
- Realizar atividades de controle e gerenciamento técnico, relacionados a aderência da infraestrutura de segurança de perímetro – Firewall/UTM às normas e políticas de segurança da informação do INEA.
- Realizar o backup de todas as informações de configuração da Firewall/UTM, como: regras, políticas e outras definições, em um repositório seguro de armazenamento.
- Executar de atividades críticas relacionadas a alterações/adições de funcionalidades ou configurações na infraestrutura de segurança que irão ou poderão causar impacto nos serviços da organização, através de um processo de gerenciamento de mudanças.
- Executar atividades de mudanças relacionadas de resolução de incidentes que necessitam uma paralização total ou parcial do dispositivo de segurança e seus componentes relacionados.
- Avaliar a aplicabilidade de versão de firmware dos equipamentos da Firewall/UTM, atuando em conjunto com o INEA para agendar as atualizações remotas, se necessário. As atualizações periódicas do firmware, devem ser realizadas para que todos requisitos mínimos exigidos pelo fabricante estejam de acordo, garantindo a estabilidade e operação normal da solução.
- As mudanças serão submetidas para aprovação do gestor técnico do INEA, mediante a um formulário de requisição de mudanças (GMUD), que constará todas as informações.
- Gerar relatórios mensais de nível de serviço - Disponibilidade, Gestão de Incidentes, Gestão de Requisições de serviço, Gerenciamento de Conformidade e Gerenciamento de Mudanças.
- Gerar relatórios mensal de segurança de informação, providos pela solução de segurança de perímetro incluindo dados sobre utilização de dados,



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

aplicações, atividade dos usuários, atividades web, uso de VPN, tentativas de intrusão, Vírus, tentativas de ataques e up/down dos equipamentos.

- Manter documentação completa da instalação e funcionamento dos serviços de segurança de perímetro incluindo firewall/UTM e servidores de SSO.

4.2. Serviço De Instalação, Configuração E Suporte Por 12 Meses - Solução De Segurança De Servidores Virtuais E Físicos

4.2.1. Descrição das atividades técnicas

A CONTRATADA será responsável pelas atividades de gerenciamento, administração e suporte de todos os módulos envolvidos na solução de segurança de servidores, a ser fornecida e instalada no INEA, de acordo com este termo de referência.

A CONTRATADA deverá garantir a continuidade dos serviços providos pela solução de segurança de servidores, através de atividades de administração, gerenciamento e suporte por 12 (doze) meses após a data de instalação da solução em ambiente de produção do INEA.

O projeto de instalação e configuração da solução deverá iniciar em até 5 (cinco) dias úteis após a entrega de todos os softwares e licenças envolvidos na solução. Neste prazo deverá ser apresentado a gerência de TI do INEA o plano de projeto com os requisitos técnicos, cronograma, riscos e estratégia de migração para a nova solução de segurança de servidores. O INEA deverá aprovar o plano de projeto em até dois (02) dias úteis, a partir da entrega da documentação.

O prazo para a instalação da solução de segurança de servidores em pleno funcionamento no ambiente de produção do INEA é de 30 dias, após a aprovação do plano de projeto pela gerência de TI do INEA.





GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

A equipe responsável pela instalação, gerenciamento, administração e suporte da solução de segurança de servidores deverá ser especializada e certificado pelo fabricante no produto fornecido para este termo de referência.

As atividades de instalação e configuração lógica executadas pela CONTRATADA que tenham impacto direto no ambiente de produção do INEA deverão ser realizados de forma presencial nas dependências do INEA e preferencialmente fora do horário comercial. Atividades sem impacto no ambiente de produção poderão ser executadas remotamente, mediante acesso seguro e com a aprovação da gerência de TI do INEA.

São atividades do serviço de instalação e configuração da solução de segurança de servidores:

- Apresentar as o método de funcionamento das principais funcionalidades da solução proteção servidores para a Gerência de Tecnologia do INEA, com o objetivo de identificar possíveis impactos nos serviços de negócio do instituto, e a partir desse entendimento definir a melhor estratégia de implantação.
- Definir em conjunto com a Gerência de Tecnologia a estratégia de implantação da solução objetivando o menor impacto no ambiente de produção.
- Realizar a instalação dos agentes de software de acordo com as políticas de segurança e estratégias definidas em conjunto com a Gerência de Tecnologia do INEA, na etapa de planejamento.
- Instalar os agentes de software da solução de proteção em todos os servidores relacionados no ANEXO I.
- Implantar de forma proativa as práticas de segurança na infraestrutura de segurança de servidores, como backup das configurações, atualizações de software e patches atualizações críticos, disponibilizados pelo fabricante da solução.
- Apontar vulnerabilidades, brechas de segurança ou qualquer inconformidade nas configurações da solução identificados após a implantação da solução de segurança de servidores, de acordo com as boas



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

práticas, para a Gerência de TI do INEA, para sua avaliação e tomada de decisão.

- Configurar a integração da solução de segurança de servidores com o serviço de diretório Microsoft Active Directory do INEA para possibilitar a configuração e emissão de relatórios baseados no nome do usuário da rede local.
- Apresentar para a Gerência de Tecnologia do INEA o método de acesso ao portal de gerenciamento, as funcionalidades e políticas implantadas, painéis de aletas, relatórios de ameaças e bem como qualquer informação relevante para o gerenciamento e acompanhamento da solução.
- Gerar documentação do ambiente de solução de segurança de servidores do ambiente do INEA, contemplando topologia e configurações implantadas.
- As mudanças serão submetidas para aprovação do gestor técnico do INEA, mediante a um formulário de requisição de mudanças (GMUD), que constará todas as informações.

O atendimento de suporte especializado (2º nível) deverá ser executado pela CONTRATADA preferencialmente de forma remota, mas em caso de necessidade de acesso físico ao ambiente para resolução do problema ou da atividade a ser executada, poderá ser realizado atendimento presencial nas dependências do INEA. Da mesma forma que a equipe de TI do INEA, poderá a qualquer momento, solicitar à CONTRATADA o atendimento presencial dependendo do impacto e urgência do incidente.

A equipe responsável pelo atendimento à solução de segurança de servidores deverá ser especializada e certificado pelo fabricante no produto fornecido para este termo de referência.

São atividades do entendimento de suporte da solução de segurança de servidores:



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- Realizar suporte, administração, mudanças ou atividades de troubleshooting em problemas relacionados à bloqueio de aplicações, bloqueio de portas TCP/IP, falha de acesso a endereços internos e externos, lentidão do sistema operacional, lentidão de aplicações, qualquer outro problema que seja impactado pela instalação da solução de segurança de servidores.
- Apoio no suporte, mudanças ou atividades de troubleshooting para incidentes relacionados as aplicações do INEA, que estejam sendo impactados pela solução de segurança de servidores, em conjunto com as áreas internas ou fornecedores do INEA.
- Manter documentação completa da instalação e funcionamento dos serviços de segurança de servidores.
- Analisar relatórios de segurança providos pela solução de segurança de servidores com o objetivo de recomendar ao INEA ações para correção de vulnerabilidades ou inconformidades identificadas, que serão direcionadas ao suporte 2º nível.
- Analisar o registro (logs) do(s) da solução de segurança de servidores, que foram correlacionados e priorizados pela console do produto, onde os eventos de segurança relevantes deverão ser categorizados com base no nível de gravidade e propostas ações de mitigação de riscos.
- Redirecionar os incidentes relacionados ao sistema operacional e aplicações para outros grupos solucionadores, caso a falha não seja um erro conhecido, ou seja, escopo do atendimento de suporte 2º nível.
- Redirecionar os incidentes relacionados a erros não conhecidos para o suporte o suporte 3º nível do fabricante da solução de segurança de servidores.
- Realizar atividades de controle e gerenciamento técnico, relacionados a aderência da solução de segurança de servidores às normas e políticas de segurança da informação do INEA, como gestão de políticas de segurança, regras, configurações, rotinas, alertas, entre outras atividades inerentes a administração do produto.
- Avaliar a aplicabilidade de versão de software dos agentes da solução instalados nos servidores, atuando em conjunto com o INEA para agendar as atualizações remotas, se necessário. As atualizações periódicas da solução implementada, devem ser realizadas para que todos requisitos



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

mínimos exigidos pelo fabricante estejam de acordo, garantindo a estabilidade e operação normal da solução.

- Realizar o backup de todas as informações de configuração solução de segurança de servidores, como: regras, políticas e outras definições, em um repositório seguro de armazenamento.
- Executar de atividades críticas relacionadas a alterações/adições de funcionalidades ou configurações na solução de segurança de servidores que irão ou poderão causar impacto nos serviços da organização, através de um processo de gerenciamento de mudanças.
- Executar atividades de mudanças relacionadas de resolução de incidentes que necessitam uma paralização total ou parcial do dispositivo de segurança e seus componentes relacionados.
- Analisar a viabilidade e impacto da instalação de novas soluções, equipamentos e serviços a serem implantados no INEA que tenham relacionamento com a solução de segurança de servidores, mediante a solicitação forma da equipe de TI do INEA.
- As mudanças serão submetidas para aprovação do gestor técnico do INEA, mediante a um formulário de requisição de mudanças (GMUD), que constará todas as informações.
- Gerar relatórios mensais de nível de serviço - Disponibilidade, Gestão de Incidentes, Gestão de Requisições de serviço, Gerenciamento de Conformidade e Gerenciamento de Mudanças.
- Gerar relatórios mensal de segurança de informação, providos pela solução de segurança de servidores incluindo dados sobre versão dos agentes, bloqueios, ataques identificados, quarentena, usuários mais afetados, vírus identificados e vulnerabilidades encontradas.
- Gerar documentação do ambiente de solução de segurança de servidores do ambiente INEA, contemplando topologia e configurações implantadas.



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

5. SERVIÇO DE MONITORAMENTO DO AMBIENTE

5.1. Características gerais

- 5.1.1. Compreende o no processo de monitoramento do ambiente de Tecnologia da Informação do INEA, através de um conjunto de ferramentas, processos e mão de obra especializada, com a finalidade de atuar de forma proativa e com agilidade no processo de detecção e resolução de incidentes da Solução de segurança de perímetro - Firewall/UTM, soluções de segurança para servidores físicos e virtuais e infraestrutura de TI, assim como realizar o envio de comunicados de todos os eventos que causem impacto no usuário final.
- 5.1.2. A Central de Monitoramento de Redes e Serviços (NOC), deverá operar em regime de 24x7x365, a disponibilidade mensal do serviço deverá ser de no mínimo 98%, comprovado através de envio de relatório mensal de disponibilidade do serviço, gerado pela solução de monitoramento. Este relatório deverá conter o percentual de disponibilidade no período mensal dos itens da infraestrutura que compõem o serviço de monitoramento da CONTRATADA, como: Serviços, servidores, firewalls, links, telefonia, etc. O cálculo da disponibilidade total será a média aritmética dos percentuais de disponibilidade de cada item que compõem o serviço.
- 5.1.3. A CONTRATADA deverá manter, em suas dependências, uma infraestrutura do tipo NOC (Central de Monitoramento de Redes e Serviços), com a visualização do ambiente de TI através de um painel de alarmes e uma ferramenta de gerenciamento de tickets, necessário para o gerenciamento dos eventos e controle do ciclo de vida dos incidentes na infraestrutura do INEA.



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- 5.1.4. Os eventos de falha identificados pela solução de monitoramento deverão ser tratados pela equipe de operadores do NOC através dos chamados abertos a partir do evento original, ou seja, a solução de monitoramento deverá ter uma integração sistêmica com a ferramenta de gestão de tickets, onde todas as informações do evento como: número identificador do alerta, hora do alerta, item de configuração afetado, mensagem de falha do evento, subsistema afetado, entre outras informações relevantes, deverão estar contidas no chamado aberto automaticamente na ferramenta de gerenciamento de tickets.
- 5.1.5. A CONTRATADA, deverá possuir estrutura de comunicação de dados redundante, ou seja, possuir links internet redundantes com diferentes operadoras, de modo que a comunicação entre a solução de monitoramento e a instancia local no INEA, seja mantida mesmo com a indisponibilidade de um dos links de dados da CONTRATADA.
- 5.1.6. A CONTRATADA deverá disponibilizar uma conexão VPN (virtual private network) entre a Central de Monitoramento de Servidores e Rede (NOC) e o Datacenter do INEA para permitir o acesso remoto dos operadores do NOC aos servidores e ativos de rede. Este acesso será responsável para a execução das atividades de suporte 1º nível, necessários no processo de atendimento. Todo o hardware e software necessário para esta conexão deverá ser fornecido pela CONTRATADA, sem custos para o INEA.
- 5.1.7. A CONTRATADA deverá prover painéis de visualização dos alarmes, relatórios de performance, capacidade e SLA, através de um site web. A solução de monitoramento deverá permitir o acesso aos alarmes através de um APP para dispositivos móveis iOS e Android.



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

5.1.8. A solução de monitoramento, seus painéis, relatórios, bem como o sistema de gerenciamento de tickets, serviço de envio de e-mails e telefonia, ou seja, toda a infraestrutura necessária para a prestação do serviço ao INEA, devem estar disponíveis 24 horas por dia, 7 dias por semana e 365 dias no ano. Caso seja necessário realizar ações de manutenção programadas na infraestrutura do serviço da CONTRATADA, a mesma deverá comunicar ao INEA com até 48 horas antecedência. Estas ações não poderão ser realizadas durante do horário comercial.

5.2. Serviço de monitoramento (Firewall-UTM e Infraestrutura de TI)

5.2.1. Requisitos técnicos

5.2.2. A CONTRATADA deverá, em um prazo máximo em 05 (cinco) dias corridos contados a partir da data de início do contrato, prover todos os recursos necessários na sua Central de Monitoramento de Redes e Serviços, para a ativação do serviço de monitoramento. O monitoramento básico dos servidores e ativos de TI constantes no ANEXO I devem estar disponíveis, de forma a permitir sua efetiva entrada em operação em até 30 (trinta) dias após o início do contrato.

5.2.3. O INEA considera monitoramento básico, realizar o monitoramento das métricas básicas de disponibilidade e capacidade do ambiente, compreendendo o status de up/down dos servidores e ativos de rede, medição da utilização da CPU, disco e memória dos servidores e medição do tráfego das interfaces físicas do firewall/UTM que estão conectadas diretamente os links de comunicação de dados.

5.2.4. Nesta etapa a CONTRATADA deverá definir em conjunto com o INEA os thresholds (limites) a serem parametrizados para geração de alarmes e estratégia de notificação dos eventos.



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

5.2.5. Em até 30 (trinta) dias corridos após a assinatura do contrato, deverá estar disponível na sede da CONTRATANTE um dashboard operacional, em tempo real, com as principais métricas do ambiente do INEA coletadas nesse período, para visualização das equipes responsáveis da CONTRATANTE em uma TV de LED de 49”. Este painel poderá ser alterado a qualquer momento mediante a solicitação formal a CONTRATADA.

5.2.6. O dashboard operacional deverá conter:

- Visão topológica das redes, representando graficamente todos os relacionamentos de parentesco entre os dispositivos monitorados e o estado atual do monitoramento em tempo real;
- Visão por localidade de cada localidade do INEA;
- O mapa de rede do ambiente de TI do INEA distribuído geograficamente no Estado do Rio de Janeiro;
- Deverão ser representados neste mapa, com clareza, através do uso das cores verde, amarelo e vermelho, os dispositivos gerenciados que apresentem qualquer problema de configuração ou disponibilidade, refletindo uma rápida visualização de pontos de problemas na infraestrutura;
- Apresentar na mesma interface os eventos e alarmes de todo o ambiente, permitindo que ao INEA possa expandir para níveis detalhados de informação para um evento ou alarme selecionado (recurso de "drill down");



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

5.2.7. O monitoramento completo, de toda a infraestrutura do INEA, incluindo a medição das métricas das aplicações e serviços de negócios deverá estar disponível em até 30 (trinta dias) após o início do contrato.

5.3. Gerenciamento de eventos

5.3.1. O Gerenciamento de Eventos é responsável pelo monitoramento de todos os eventos que ocorrem na infraestrutura de TI, para atestar a normalidade da operação. Caso sejam detectadas condições de exceção, este processo deve escalar para resolução pelas equipes técnicas ou para atuação hierárquica.

5.3.2. Por meio do gerenciamento de eventos, a equipe de TI do INEA poderá analisar e determinar as ocorrências rapidamente para tomar ações proativas, garantindo o funcionamento normal dos serviços com o mínimo de interrupção e intervenção ao usuário. Além disso, será possível atender os prazos de Acordo de Nível de Serviço estabelecidos e desafogar a Central de Serviços (ou equipe de Suporte), tratando os eventos antes que se tornem incidentes.

5.3.3. São atividades do gerenciamento de eventos:

- Monitorar, em tempo real, a disponibilidade, performance de rede e outros parâmetros relativos ao ambiente de TI, por SNMP, WMI, Agentes ou Consultas em bases de dados;
- Possuir procedimento de escalonamento de incidentes, de modo a encaminhar os alarmes e incidentes a níveis superiores de suporte, representados por equipes, pessoas e/ou de terceiros, quando os mesmos não forem resolvidos ou não forem tratados nos prazos pré-determinados;
- Oferecer a visualização dos dados de monitoração de performance, históricos e tempo real, permitindo a seleção de um determinado ponto na linha de



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

tempo, possibilitando a identificação do momento exato no qual um determinado problema ou comportamento anormal se iniciou;

- O INEA indicará a CONTRATADA a criticidade dos ativos a fim de priorizar o tratamento das ocorrências que mais impactam os serviços monitorados;
- Reportar mensalmente a lista dos 10 (dez) eventos que causaram maior impacto na infraestrutura do INEA e descrevendo a causa raiz e propor ações para melhoria do ambiente de forma a fim de evitar a ocorrência destes tipos de eventos novamente;
- Analisar os eventos gerados e propor alterações, casos sejam necessárias, na configuração do sistema de monitoramento para gerar apenas alertas relevantes, que reflitam um comportamento anormal do ambiente de TI do INEA e que requeiram alguma ação;
- Configurar o envio dos eventos, alarmes e notificações para os profissionais da equipe de suporte do INEA e para a sua própria equipe, através de e-mail e SMS de forma automatizada.

5.3.4. A CONTRATADA deverá prover mensalmente ou quando solicitada os relatórios de disponibilidade e capacidade informados abaixo, não se limitando somente a esses:

- Relatório com a Disponibilidade dos Hosts (Servidores, Switches, Routers etc.) que não atingiram os objetivos de disponibilidade para a Infraestrutura de Datacenter;
- Relatório de Disponibilidade dos Serviços (Correio etc.) que não atingiram os objetivos de disponibilidade para a Infraestrutura de Datacenter;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- Relatório com o Tempo Médio Entre Falhas (MTBF) e Tempo Médio de Reparo (MTTR) dos Hosts (Servidores, Switches, Routers);
- Relatório com o Tempo Médio Entre Falhas (MTBF) e Tempo Médio de Reparo (MTTR) dos serviços (Correio etc.);
- Relatório com os Hosts e Serviços que mais geraram alerta de indisponibilidade;
- Relatório com os SLA's de disponibilidade dos Serviços de TI ou outros que venham a ser criados;
- Relatório de Disponibilidade de links WAN com percentual e seus respectivos tempos de indisponibilidade, para confrontar os SLAs contratados junto às operadoras;
- Relatório de Disponibilidade dos Elementos de acordo com o Serviço de TI;
- Relatório ou Dashboard com os Itens de configuração em alarme com os seus respectivos status de tratamento;
- Relatório com os 5 (cinco) links WAN que apresentaram maior indisponibilidade no mês;
- Relatórios de Capacidade média de consumo dos links WAN.



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

5.4. Gerenciamento de incidentes

- 5.4.1. O INEA será responsável pelo atendimento de suporte de 1º e 2º níveis, bem como o gerenciamento do ciclo de vida de todos os incidentes abertos pela Central de Monitoramento de Redes e Serviços (NOC), relacionados a sua infraestrutura de TI, até a sua conclusão. Onde se necessário, deverá realizar o escalonamento do incidente para grupos de atendimento internos no INEA, ou seus parceiros e fornecedores.
- 5.4.2. A CONTRATADA será responsável pelo atendimento de suporte de 1º e 2º níveis, bem como o gerenciamento do ciclo de vida de todos os incidentes abertos pela Central de Monitoramento de Redes e Serviços (NOC), relacionados somente aos equipamentos, software e serviços da solução de segurança de perímetro - Firewall/UTM, fornecido neste termo de referência, até a sua conclusão. Onde se necessário, deverá realizar o escalonamento do incidente para outros grupos de atendimento como por exemplo: Operadoras de telecomunicações, fabricante do produto, área de infraestrutura do INEA, entre outros.
- 5.4.3. A CONTRATADA deverá realizar o tratamento dos incidentes através da ferramenta de gerenciamento de chamados disponibilizada pela mesma e todas as informações pertinentes ao atendimento deverão ser registradas no chamado, incluindo o item de configuração afetado, serviço afetado, criticidade, impacto, grupo resolvidor responsável, analista responsável, código de resolução, método de resolução, procedimento utilizado e descrição atividade técnica para a resolução do incidente.
- 5.4.4. A ferramenta de monitoramento da CONTRATADA deverá realizar a abertura de chamados de forma automática dos eventos de infraestrutura de TI do INEA na ferramenta de gerenciamento de chamados da mesma, através Webservices ou enviar todas as informações pertinentes ao alerta por e-mail às equipes responsáveis.



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

5.4.5. Os chamados escalonados para as equipes técnicas externas e internas, terão o ANS (Acordo de nível de serviço) pausado, não ferindo o acordo de nível de serviço do atendimento do suporte 1º nível. Mas, a ferramenta de gerenciamento de chamado da CONTRATADA deverá ser capaz de medir o TMA (tempo médio de atendimento) das equipes externas e equipes internas do INEA.

5.4.6. São atividades de suporte de responsabilidade da CONTRATADA:

- Executar procedimentos técnicos iniciais (1º nível) na Solução de segurança de perímetro - Firewall/UTM, conforme definidos previamente de acordo com procedimentos de escalação estabelecidos, registrando a análise inicial e direcionando quando necessário à equipe de suporte 2º nível – Suporte Especializado especificados no item **Erro! Fonte de referência não encontrada..**, a serem fornecidos pela CONTRATADA ou operadoras de telecomunicações, fabricantes, entre outros para a resolução do problema;
- Registrar os eventos de monitoramento de forma automatizada na ferramenta de gerenciamento de chamados da CONTRATADA;
- Realizar o gerenciamento do ciclo de vida dos incidentes relacionados a solução de segurança de perímetro - Firewall/UTM abertos pela Central de monitoramento de redes e serviços (NOC), desde a sua abertura até a resolução;
- Escalar para outros níveis de suporte em caso de insucesso na resolução do incidente de cumprimento do acordo de nível de serviços (ANS);
- Encerrar os incidentes após notificação e aprovação do cliente;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE - SEA
INSTITUTO ESTADUAL DO AMBIENTE - INEA

- Realizar o agendamento de interrupções periódicas e ou interrupções ocasionais de Itens de configuração quando solicitada, com o objetivo de planejamento e execução de manutenções sem a geração de alarmes;
- Realizar análise inicial do problema e fará a indicação da solução do evento de indisponibilidade ou capacidade durante o processo de abertura de tickets, porém as possíveis soluções finais para cada evento é uma atribuição do INEA fazendo parte das atividades de resolução de incidentes;
- Realizar o escalonamento de chamados para outros níveis de suporte do INEA, como por exemplo equipe técnica de infraestrutura, através de fluxo automatizado, provido pela integração entre as ferramentas de gerenciamento da CONTRATADA e do INEA. Onde os campos relevantes, como: número do evento, item monitorado, descrição, prioridade, impacto, urgência, entre outros, devem ser sincronizados de forma bidirecional entre as ferramentas, para ser possível realizar o rastreamento do atendimento;
- Para realizar o escalonamento de chamados para equipe de suporte externas ao INEA, como por exemplo operadores de telecomunicações, fabricantes da Solução de segurança de perímetro - Firewall/UTM etc., o status do chamado deverá ser alterado, indicando que o mesmo está sendo atendido por fornecedor externo.

5.4.7. São atividades de suporte de responsabilidade do INEA:

- Realizar procedimentos técnicos de análise, investigação (troubleshooting) e resolução dos incidentes de infraestrutura de TI, incluindo servidores Windows/Linux, redes LAN/WAN, banco de



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE - SEA
INSTITUTO ESTADUAL DO AMBIENTE - INEA

dados, aplicações de negócio, backup, ou seja, todos o parque tecnológico do INEA.

- Escalar para outros níveis de suporte em caso de insucesso na resolução do incidente de cumprimento do acordo de nível de serviços (ANS).
- Encerrar os incidentes após notificação e aprovação do usuário final.
- Realizar o agendamento na Central de Monitoramento de Redes e Serviços (NOC) de interrupções periódicas e ou interrupções ocasionais de Itens de configuração sobre a responsabilidade do INEA, com o objetivo de planejamento e execução de manutenções sem a geração de alarmes.
- Realizar análise inicial do problema e fará a indicação da solução do evento de indisponibilidade ou capacidade durante o processo de abertura de tickets, porém as possíveis soluções finais para cada evento é uma atribuição do INEA fazendo parte das atividades de resolução de incidentes.



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

5.5. Solução de Monitoramento

5.5.1. Implantação do serviço de monitoramento

5.5.1.1. O INEA, através da sua equipe de infraestrutura irá realizar a passagem do conhecimento do ambiente, incluindo: rotinas manuais que são executadas, eventos recorrentes que causam impactos, sazonalidades de performance do ambiente ou qualquer evento relevante que ocorra no dia a dia da operação, para que a CONTRATADA leve em consideração na fase de parametrização do monitoramento do ambiente.

5.5.1.2. A CONTRATADA deverá realizar, baseado na relação de itens de configuração descritos no ANEXO I e o conhecimento passado pela equipe de TI do INEA, um documento contendo a especificação técnica da metodologia de monitoramento que será implantada no ambiente de TI do INEA.

5.5.1.3. O documento deverá conter todos os itens de configuração que serão monitorados e seus relacionamentos com os serviços de TI, informar o tipo de monitoramento a ser realizado, sondas que serão implantadas para cada tecnologia, métricas que serão coletadas, tempos de coleta das métricas e limites (thresholds) configurados para geração de alertas e método de notificação. Este documento deverá ser submetido para aprovação a equipe de TI do INEA, que deverá ocorrer em até 3 (três) dias úteis. O INEA, poderá solicitar alterações neste documento e a CONTRATADA deverá realizar as alterações solicitadas.

5.5.1.4. Mediante o documento da estratégia de monitoramento finalizado e aprovado pelo INEA, a CONTRATADA irá realizar configuração e parametrização da solução de monitoramento no ambiente baseado nas melhores práticas de mercado, utilizando profissionais certificados na solução proposta e com experiência técnica equivalente nas tecnologias existentes na infraestrutura de TI do INEA.



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE - SEA
INSTITUTO ESTADUAL DO AMBIENTE - INEA

5.5.1.5. A CONTRATADA nesta etapa deverá realizar, além do levantamento técnico, o levantamento do processo de suporte primeiro nível, incluindo a criação do catálogo de serviço das atividades que serão realizadas pela equipe do NOC. Este levantamento deverá ser realizado em conjunto com a equipe de TI do INEA, no qual será identificado quais atividades poderão ser executadas pelos operadores, de acordo com os serviços especificados neste termo de referência. Neste documento, deverá ser entregue ao INEA para sua aprovação e deverá conter as seguintes informações:

- ✓ Catálogo de serviços do atendimento de 1º nível dos serviços providos neste termo de referência.
- ✓ Diagrama de blocos do processo de atendimento de suporte primeiro nível e sua interação com o gerenciamento de eventos.
- ✓ Mapeamento das equipes internas ou externas responsáveis pela resolução dos incidentes. As informações básicas como contato (nome, telefone e e-mail), descrição do serviço prestado, janela de atendimento e SLA devem ser mapeadas.
- ✓ Matriz de escalonamento, forma de acionamento e contatos.



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

5.6. Arquitetura da solução

- 5.6.1. A solução de monitoramento disponibilizada na nuvem pela CONTRATADA deverá se comunicar com um servidor local nas dependências do INEA, a ser fornecido, instalado, configurado e mantido pela CONTRATADA, durante o prazo de prestação dos serviços. Este servidor local será responsável pela monitoração via protocolos SNMP ou através de agentes, dos elementos que compõem o ambiente de TI. O monitoramento propriamente dito, será executado a partir desta instância, para em caso de falhas de comunicação com a solução de monitoramento da CONTRATADA, a monitoração local permaneça ativa. Esta funcionalidade irá garantir que após o retorno da comunicação, todos os dados de métricas coletados no período de indisponibilidade sejam enviados ao servidor de monitoramento da CONTRATADA.
- 5.6.2. A solução deve ser escalável, permitindo instalação de instâncias locais em diferentes "Data Centers", permitindo assim com que o administrador possa distribuir a camada de coleta, porém, todas as mensagens coletadas, sejam centralizadas no gerenciador principal. Os equipamentos a serem instalados localmente, para cada uma das 02 (duas) localidades do INEA, deverão ser fornecidos pela CONTRATADA.
- 5.6.3. A comunicação da solução de monitoramento da CONTRATADA, disponibilizada através da internet, deverá se comunicar com a instância local utilizando de protocolos seguros (SSL), nativos na solução, para garantir a privacidade das informações à instância central da CONTRATADA. Não será permitido a comunicação direta, sem criptografia, ou acessos através de NAT (Network address translation) da solução de monitoramento na nuvem da CONTRATADA com os itens de configurações internos, na rede do INEA.
- 5.6.4. Em caso de perda de comunicação entre a instância local e a instância central, a solução deverá ter a capacidade de armazenar todas as mensagens coletadas em disco e entregá-las à instância central assim que reestabelecer a comunicação de uma forma síncrona, garantindo assim que mesmo o "link" de comunicação inoperante.



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- 5.6.5. Com o objetivo de ter um monitoramento unificado, toda a solução deve ter um único banco de dados e por sua vez uma única base de eventos.
- 5.6.6. A solução de monitoramento poderá ter a capacidade de monitorar sistemas usando agentes instalados nos servidores para uma melhor performance e coleta de métricas, porem também a solução deve oferecer opção de não utilizar agentes para casos específicos. (Ex: banco de dados, Apache, VMWare etc.).
- 5.6.7. Caso a CONTRATADA utilize agentes de monitoramento, esses não devem causar impacto no uso de recursos de forma que comprometa o desempenho, capacidade e disponibilidade do equipamento em que esteja hospedado ou dos demais sistemas que estejam em funcionamento neste equipamento;
- 5.6.8. Quanto aos agentes de software a serem instalados nos servidores, os mesmos deverão ter o seguinte requerimento:
- Devem utilizar menos de 1% de CPU dos servidores, para não impactar a performance dos mesmos;
 - Devem utilizar menos de 10MB de Memória RAM, para não impactar a performance dos mesmos.
- 5.6.9. A CONTRATADA deverá prover os recursos necessários para o armazenamento dos dados históricos dos eventos do ambiente de TI do CONTRATANTE pelo prazo mínimo de 06 (seis) meses;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

5.6.10. A infraestrutura da Central de monitoramento de redes e serviços (NOC) destinada à suportar os serviços de monitoramento previstos nesse termo de referência, poderão ser compartilhados com outros clientes da CONTRATADA, desde que sejam disponibilizadas consoles específicas para o monitoramento do ambiente de TI do INEA e que os níveis de serviço sejam cumpridos, garantindo que todos os dados gerados por qualquer ativo ou serviços monitorados do ambiente do INEA sejam considerados como confidenciais não permitindo a sua divulgação sob nenhuma circunstâncias sem a autorização prévia.

5.7. Tecnologias suportadas

5.7.1. Funcionalidades técnicas gerais:

- Prover suporte para a instalação da solução em ambientes Windows e Linux.
- Utilizar protocolo TCP como meio de comunicação entre os diversos componentes da solução.
- Prover suporte a protocolos de mercado incluindo ICMP, SNMP e syslog, HTTP, HTTPS, DNS, DHCP, LDAP.
- A instalação de agente não deve necessitar de reboot do sistema.
- Mudanças de configuração no agente não devem precisar de reboot do sistema.
- Quando o agente gerar um evento, ele deve ser responsável por entregar este evento na console, com garantia de entrega.
 - ✓ A solução deve permitir instalar os agentes de forma manual.
 - ✓ A solução deve ter mecanismo de distribuição do agente.
 - ✓ A solução deve permitir a distribuição de configuração aos agentes de forma automatizada.
 - ✓ A solução deve permitir a distribuição de configuração aos agentes com facilidade de arraste e solte ("drag and drop").
 - ✓ A solução deve ser escalável.
 - ✓ A solução deve ser multi tier.
 - ✓ A solução deve suportar usuários concorrentes.



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- Os agentes devem ser configurados via interface gráfica a partir do gerenciador da solução.
- Os agentes devem suportar configuração manual via edição de arquivos e via API.
- A solução deve permitir reutilizar configuração criada para a monitoração em vários agentes.
- A atualização de versão de agente não deve alterar a configuração de thresholds.
- O agente deve ter capacidade de filtrar e definir que informação é direcionada ao gerenciador.
- No caso de problema de conexão com o manager o agente deve armazenar as informações por período definido. Uma vez reestabelecida a conexão ele deve enviar as informações coletadas.
- Prover a capacidade de utilizar diferentes níveis de severidade ou urgência dos alarmes (ex. Crítico, Informação, etc.).
- A solução deve ter eventos com severidades previamente configurados para diversos tipos de monitoração.
- A solução deve permitir alterar a severidade e texto dos eventos já existentes na monitoração.
- A solução deve permitir criar novos eventos definindo o texto e severidade.
- A solução deve permitir que eventos e/ou alarmes sejam escalados, reiniciados, e/ou suprimidos baseado em critérios múltiplos como fonte, conteúdo, horário ou outros itens que sejam obtidos pela monitoração.
- O agente deve permitir executar ações de remediação no caso de uma situação identificada na monitoração. Por exemplo iniciar um processo ou serviço no caso de queda do mesmo.

5.8. Portal de gerenciamento WEB

- Para um excelente controle, administração e governança de monitoração, a solução deve possuir um único Portal de acesso para administradores, operadores, gerentes de nível de serviço e executivos de TI.



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- Por motivos de flexibilidade e facilidade de acesso, este portal deverá ser WEB e acessível pelos principais navegadores de mercado como: Google Chrome, Internet Explorer, Mozilla Firefox e outros.
- O Portal deve consolidar e apresentar toda e qualquer métrica coletada pela solução de monitoração.
- O Portal também deve ser capaz de trazer informações de fontes externas através de API, Arquivos de texto e URLs, mesmo que estes não estejam sendo monitorados pela própria solução de gerenciamento.
- Dentro do portal de monitoração mostrar dados de negócio, através de APIs ou simplesmente apresentar o WEB Site ou qualquer outra aplicação WEB.
- A console de gerenciamento deve permitir notificação por e-mail e SMS.
- A console de gerenciamento deve permitir executar ações por trigger de um alarme.
- A solução deve permitir que sobre os alarmes gerados os usuários possam aceita-los, assinalar, assumir responsabilidade e tomar ação apropriada.
- A solução deve permitir os operadores e administradores inserir uma "nota" (texto) no alarme para melhor acompanhamento do caso.
- A console de alarmes deve permitir os operadores executar ações via "URL" a partir de um alarme que já foram determinadas anteriormente pelo administrador do sistema. Exemplo: teste icmp em um device, Acesso RDP, Acesso SSH etc.
- A console de alarmes deve permitir os operadores a criar filtros rápidos a partir de "clicks" por diferentes categorias sendo no mínimo: Por Severidade, por hostname, por endereço IP, por servidor de coleta, por data e hora, por tipo de tecnologia monitorada (ex.: Oracle, Apache, Disco, CPU, JBoss, etc.), permitindo assim os operadores trabalharem de forma dinâmica, correlacionando eventos visualmente para uma rápida solução da falha.
- Capacidade de gerar os alertas quando uma dada métrica de desempenho se mantiver acima do limiar estabelecido por um dado período de tempo configurável, dentro de uma janela de tempo maior, também configurável.



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- Capacidade de gerar alertas baseado em desvio de comportamento para que possa monitorar métricas fora do seu desvio padrão evitando assim para alguns casos o falso/positivo alarmes.
- Capacidade de gerar alertas dias/semanas/mês antes que uma métrica atinge o limiar estabelecido no intuito de ter análise de tendência e ser proativo na monitoração
- Capacidade de receber traps dos dispositivos indicando o tipo de problema que está ocorrendo, além de apresentá-lo graficamente e em tabelas.
- A solução deve permitir consultar o histórico dos alarmes.
- A solução deve realizar a de-duplicação de alarmes por meio de supressão de eventos similares.
- A solução deve permitir o uso de variáveis no texto do alarme.
- A solução deve permitir ao usuário/operador filtrar e/ou ordenar os alarmes por meio de campos do alarme.
- A solução deve permitir que se defina que usuário/operador possa ver quais tipos de alarmes.
- A solução deve permitir ao usuário/operador adicionar comentários aos alarmes.
- A solução deve suportar baseline de métricas de desempenho coletadas, permitindo alertas inteligentes com os indicadores críticos de sistemas e aplicações.
- A solução deve permitir criar regra de correlação de eventos para a geração de alarmes.
- A solução deve ter portal web com informações gráficas contendo o status, alarmes e métricas dos sistemas monitorados.
- O portal da solução deve apresentar informações atualizadas e históricas de alarmes
- O portal da solução deve ter visões pré configuradas.
- A portal da solução deve ser acessado via web browsers de mercado tais como Microsoft Internet Explorer, Google Chrome e Mozilla Firefox.
- A solução deve suportar múltiplos métodos de notificação, incluindo e-mail, SMS, SNMP Traps ou abertura de incidentes em sistema de Trouble Ticket (Sistema de Service Desk).



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- A solução deve ter sistema de agendamento para a tomada de ação de escalação/notificação de alertas.
- A solução deve ter acesso por meio de sistemas moveis (Mobile Apps) com suporte a Android e IOS.

5.8.1. Painéis e Relatórios

- A solução deve ter sistema de geração de relatórios baseado nos dados contidos no banco de dados relacional da solução.
- O sistema de relatórios deve conter relatórios prontos para uso com temas sobre utilização, capacidade ou disponibilidade.
- Os relatórios devem conter gráficos, tabelas ou objetos gráficos contendo dados de desempenho.
- Os relatórios devem conter gráficos, tabelas ou objetos gráficos (como imagens, URL links) contendo dados de desempenho.
- Os usuários devem ter acesso apenas aos relatórios que são destinados a eles.
- Os usuários podem modificar em seus relatórios informações como, cabeçalho/título, gráficos, textos, URLs/links, imagens, cores, fundo do relatório entre outros.
- A solução deverá disponibilizar relatórios prontos para uso (sem necessidade de configurar ou contratar serviços profissionais) que inclua as seguintes características:
 - ✓ Gerar relatório por tecnologia (Exemplo: Servidores, Routers, LAN/WAN, etc.)
 - ✓ Que o relatório seja de um grupo de dispositivos e que permita identificar problemas de maneira imediata, por exemplo, os servidores por localidade, ou os links wan ou os routers do core, etc.
 - ✓ Poder gerar relatórios das exceções ou funcionamento anormal obtidos em cada uma das interfaces e diferentes dispositivos que compõem a rede.
 - ✓ Média de linhas de volume de dados do grupo de dispositivos.
 - ✓ Indicar as principais fontes de problemas do grupo de dispositivos.



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE - SEA
INSTITUTO ESTADUAL DO AMBIENTE - INEA

- ✓ Gerar relatórios para grupos de dispositivos (Server / Routers / switches). Com no mínimo as métricas:
- ✓ Para routers/switches indicar CPU, Line, Buffer Utilization, Discards, Errors.
- ✓ Para Servers indicar Memória, Partições, Paginação, etc.
- ✓ Para Lan/Wan indicar se o problema é Largura da Banda, Erros, Discards etc.
- ✓ Volume dos 10 principais elementos do grupo.
- ✓ 10 Líderes de volume, indicando se o volume é de entrada ou de saída.
- ✓ Máximos e Mínimos históricos, médias de linhas de volume de cada dispositivo.
- ✓ Indicar se os dispositivos estão abaixo o acima das médias de linhas de volume.
- ✓ Os relatórios devem ser acessíveis via HTML.
- ✓ Os relatórios devem permitir versão em formato PDF.
- ✓ Os relatórios podem ser enviados via e-mail (com formato PDF).
- ✓ O sistema deve permitir o agendamento de relatórios.
- ✓ O sistema deve permitir o envio de relatórios pelo sistema de agendamento a usuários internos cadastrados no sistema.
- ✓ Relatórios podem ser enviados a outros web servers (tal como IIS ou Apache) para serem mostrados em site web/portal ou intranet.
- ✓ A solução deve ter portal web com informações gráficas contendo o status, alarmes e métricas dos sistemas monitorados e a ferramenta de relatórios.
- ✓ O portal da solução deve permitir a criação de painéis (Dashboards) conforme o perfil do usuário.
- ✓ A solução deve conter um campo para criação de painéis (dashboards) customizados em uma interface moderna tipo HTML5 compatível com os principais navegadores do mercado e tablets.
- ✓ A interface para criação de painéis customizados, deve permitir a importação de imagens, inserção de texto e componentes próprios do tipo: Tabelas, gauge, status de alertas, texto, linha, listas, gráfico e pizza, etc....



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- ✓ Os painéis customizados devem ser facilmente exportados para um link URL externo onde poderá ser usado em outros sites ou em telas nos centros de gerencias.
- ✓ Os painéis customizados deve permitir apresentação de informações de métricas de negócios através de APIs no mesmo painel existente com métricas de TI, proporcionando assim uma visão única de TI e negocio no mesmo painel.
- ✓ O portal da solução deve ser acessado via web browsers de mercado tais como Microsoft Internet Explorer, Google Chrome e Mozilla Firefox.

5.9. Monitoramento dos Servidores

- A solução deve ter capacidade de medir níveis de serviço da infraestrutura monitorada que seja relacionada as aplicações de negócios.
- Os eventos e informações de monitoração de sistemas operacionais devem ser apresentadas no portal web e relatórios descritos na sessão “Painéis e Relatórios”.
- A monitoração de sistemas operacionais deve suportar nativamente, sem necessidade de customização, métricas padrão de mercado com o propósito de apresentá-las em forma de alarmes e relatórios.

5.10. Monitoramento de Banco de Dados

- Deve suportar a monitoração dos seguintes fabricantes de bancos de dados: Oracle, SQL Server, MySQL e outros.
- A monitoração deve coletar métricas de desempenho do uso de recursos dos bancos de dados, tais como espaço de tabelas, buffer cache hit ratios, usuários ativos, locks e mais.
- A solução deve conter dicas que auxiliem os usuários com informações sobre as métricas de banco de dados coletadas.
- A solução deve permitir a criação de queries customizadas para Oracle, MS SQL e MySQL. Sendo que estas queries são statements SQL



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

executados com o intuito de gerar alarmes, coletar métricas de desempenho, tempo de resposta ou valor que deva ser armazenado e reportado pela solução.

- A solução deve permitir a descoberta de instancias de banco de dados.
- A solução deve permitir a definição de coleta de métricas e thresholds para cada instancia ou de forma global.
- A solução deve ter templates de monitoração prontos.
- A solução deve permitir alterar os templates de monitoramento, adicionando coletas, thresholds ou adicionando novas monitorações (SQL Statement).
- A solução deve permitir o monitoramento baseada em calendário, determinando quando certa monitoração em banco de dados deve iniciar e terminar.
- A solução deve permitir o monitoramento de Banco de Dados Oracle, com métricas como: Global cache service utilization, fusion ratio, lock get time, lock conversation timeouts, average lock get time, corrupt blocks count e lost clocks count.
- Os eventos e informações de monitoração de bancos de dados devem ser apresentadas no portal web e relatórios descritos na sessão “Painéis e Relatórios”.
- A monitoração para bancos de dados Oracle deve suportar nativamente, sem necessidade de customização, métricas padrão de mercado com o propósito de apresentá-las em forma de alarmes e relatórios.

5.11. Monitoramento de Aplicações

- Deve ter capacidade de monitorar aplicações residentes nos sistemas operacionais gerenciados pela solução.
- Deve monitorar sistemas de e-mail.
- Na gerencia de e-mail deve monitorar serviços, processos e logs de eventos.
- Na gerencia de e-mail deve coletar informações sobre as caixas de e-mail e métricas.



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- Na gerencia de e-mail deve ter Dashboards e relatórios relacionados a aplicação.
- Na gerencia de e-mail deve executar testes de tempo de resposta no envio e recebimento de e-mails.
- A solução deve permitir monitoração por testes sintéticos baseados em SMTP, POP3 ou IMAP.
- Para a monitoração de e-mail deve suportar testes de conexão nos servidores, sendo realizadas sessões com logon e logoff, envio e recebimento de e-mails de teste refletindo a experiência do usuário nos servidores.
- A solução deve monitorar LDAP e/ou Active Directory (AD).
- A gerencia de LDAP e/ou AD deve executar queries LDAP medindo o tempo de resposta e numero de itens encontrado.
- Na gerencia de AD deve monitorar serviços, processos e logs de eventos.
- Deve monitorar desempenho e disponibilidade de servidores Apache.
- Para gerenciamento de Apache deve monitorar tempos de resposta e métricas de recursos individuais do Apache, bem como prover análise nos dados coletados e detectar problemas e degradações.
- Para gerenciamento de IIS deve monitorar checkpoints individuais como System, Web Services, IIS e ASP.
- Deve monitorar desempenho e disponibilidade de Tomcat.
- Deve executar testes sintéticos em URLs para coleta de tempo de resposta e disponibilidade.
- Os testes sintéticos de URL devem monitorar o tempo de download da página e comparar conteúdo da página com valores definidos.
- Os testes sintéticos de URL devem suportar proxies e autenticação de usuário.
- Os eventos e informações de monitoração de aplicações devem ser apresentadas no portal web e relatórios descritos na sessão “Painéis e Relatórios”.



5.12. Monitoramento da Rede de Dados

- Deve monitorar nos dispositivos de rede e servidores o tráfego das interfaces de rede do ponto de vista de desempenho.
- Deve monitorar para todas as interfaces todo o tráfego TCP/IP com contadores relacionados ao volume trafegado.
- Para o Tráfego nas interfaces de servidores deve analisar por protocolos tais como IP, ARP, RARP e IPX e comparar ao dado coletado.
- Deve permitir criar thresholds para monitorar a banda de rede via coleta da interface de rede.
- A solução deve monitorar o tempo de resposta para LDAP, DHCP e DNS por meio de testes sintéticos.
- Para DNS deve monitorar tempo de resposta de resolução, monitorar diretórios sem resposta para um ou mais servidores DNS. O DNS pode ser questionado por hostname, mail server ou name server.
- Para DHCP deve monitorar o tempo de resposta de assinalar um IP para um ou mais servidores DHCP.
- Para LDAP deve monitorar o tempo de resposta e número de itens encontrados nas queries LDAP.
- Ter capacidade de fazer testes de Ping e conexão em portas definidas pelo usuário, para identificar a disponibilidade do host e serviços.
- Ter capacidade de fazer queries SNMP em dispositivos que o suportem a fim de coletar métricas de disponibilidade e desempenho.
- Receber traps SNMP de outros dispositivos ou EMSs para tratamento e geração de alarmes.
- Suportar coletas via SNMP v1, v2 e v3.
- Deve permitir agendar manutenções programadas de roteadores e switches.
- Deve permitir configurar o timeout para coleta de estatísticas por elemento.
- Deve permitir configurar testes de tempo de resposta ICMP e TraceRoute entre dispositivos de rede.
- Deve permitir configurar testes de tempo de resposta FTP, DNS, HTTP e TCP entre um dispositivo de rede e um destes serviços de rede (servidor FTP, servidor DNS, servidor web e servidor que responda a uma conexão TCP).



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- Deve permitir configurar número de novas tentativas de pesquisa por elemento.
- A instalação e execução da solução de gerenciamento de desempenho deve ser suportada nativamente em ambientes IPv4 puro, IPv6 puro e ambientes híbridos IPv4/IPv6.
- Deve permitir a descoberta, coleta, apresentação e geração de relatórios de dispositivos com endereçamento IPv4 e IPv6.
- Deve prover mecanismo de descoberta de dispositivos de redes e servidores por:
 - ✓ Protocolo SNMP para devices de redes, appliances e servidores;
 - ✓ Protocolo WMI para servidores Windows;
 - ✓ Protocolo SSH para servidores Unix/Linux;
 - ✓ Faixa de endereço IP;
 - ✓ Importação de arquivos.
 - ✓ Entrada manual de uma relação de endereços IP.
- A solução deve prover ao INEA a possibilidade de agrupar dispositivos e interfaces dinamicamente para facilitar a organização das informações e um rápido diagnóstico de falhas, com visões por:
 - ✓ Localidade geográfica;
 - ✓ Estrutura organizacional;
 - ✓ Grupo de interface, onde o administrador pode agrupar diferentes tipos de interfaces automaticamente pela solução baseado em: Descrição da interface, Admin e Oper Status, IP, MAC, Velocidade, Index e Tipo de Interface;
 - ✓ Topológica (redes e sub-redes) representando graficamente os dispositivos, suas interfaces e os circuitos de comunicação que os interconecta.
- Apresentar os eventos de toda a topologia, bem como os eventos particulares a cada objeto representado na topologia (roteadores, switches, interfaces).
- Apresentar os alarmes de toda a topologia, bem como os eventos particulares a cada objeto representado na topologia (roteadores, switches, interfaces).
- Possuir visões de desempenho dos dispositivos, tanto geral (todo o equipamento), como por porta específica.



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- Permitir configuração de tempo diferente de "pulling" por interface, ou seja, em um device podemos ter as interfaces LAN com pulling de 10min e as interfaces WAN com pulling de 1min.
- A solução precisa fornecer as métricas padrão de mercado baseadas em NetFlow,sFlow, jFlow e IPFIX.

5.13. Monitoramento do Storage

- A solução deve monitorar storages dos seguintes fabricantes e modelos NetApp, DELL EMC, entre outros.
- A monitoração de Storage deve prover eventos, alarmes, dados de desempenho.
- Para NetAPP a monitoração deve ser feita por SNMP.
- Para VMAX a monitoração deve ser feita via CLI.
- A monitoração de Storage deve ser feita sem agentes (agentless).
- Os eventos e informações de monitoração de storage devem ser apresentadas no portal web e relatórios descritos na sessão “Painéis e Relatórios”.

5.14. Monitoramento de Máquinas Virtuais

- A solução deve monitorar os seguintes fabricantes de sistemas virtuais: VMware, Microsoft Hyper-V, Citrix Zen Server, Citrix Zen Desktop, Solaris Zones, IBM virtualization e RedHat Enterprise Virtualization (RHEV).
- A monitoração de sistemas virtuais deve ser realizada sem agente (agentless).
- Para sistema VMware a solução deve monitorar logs de eventos.
- Para a monitoração de sistemas virtuais a solução deve identificar recursos, máquinas virtuais, e coletar métricas de consumos relacionados a estes recursos e máquinas.
- Para a monitoração de sistemas virtuais a solução deve identificar o consumo de recursos físicos e virtuais.



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- ✓ Deve ser possível identificar visualmente se um dado servidor é físico ou virtual.
- ✓ Deve ser possível identificar qual o servidor que hospeda uma dada máquina virtual.
- ✓ Deve organizar a hierarquia de forma que as máquinas virtuais sejam separadas de acordo com os servidores físicos que as hospedam.
- ✓ Os eventos e informações de monitoração de virtualização devem ser apresentadas no portal web e relatórios descritos na sessão “Painéis e Relatórios”.

5.15. Monitoramento dos serviços em Nuvem

- A solução deve monitorar os seguintes fabricantes/serviços em nuvens publica: Amazon Web Services (EC2 and S3), Goggle App Engine e Microsoft Windows Azure.
- Para a monitoração de sistemas em nuvem a solução deve identificar recursos e coletar métricas de consumos relacionados a estes recursos.
- A monitoração de sistemas em nuvem deve ser realizada sem agente (agentless).

5.16. Monitoramento de Solução de segurança de perímetro - Firewall/UTM

- A solução deverá registrar em log de auditoria as ações dos usuários administradores, registrando todas as alterações realizadas em uma política de segurança, permitindo a identificação do responsável pela mudança, o horário e a origem;
- Possuir mecanismo que permita a realização de cópias de segurança (backups) e sua posterior restauração remotamente, através da interface gráfica, sem necessidade de se reinicializar o sistema;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- Possuir mecanismo para possibilitar a aplicação de correções e atualizações para o firewall remotamente através da interface gráfica;
- Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall e a remoção de qualquer uma destas sessões ou conexões;
- Permitir a visualização de estatísticas do uso de CPU, memória da máquina onde o firewall está rodando e tráfego de rede em todas as interfaces do Firewall através da interface gráfica remota, em tempo real e em forma tabular e gráfica;
- Prover mecanismo de visualização de eventos em tempo real das funções de segurança, com uma prévia sumarização para fácil visualização de no mínimo as seguintes informações:
 - ✓ Aplicações mais utilizadas;
 - ✓ Usuários com maior atividade;
 - ✓ Estatísticas de uso;
 - ✓ Ataques e eventos do IPS correlacionados com o CVE
 - ✓ Principais aplicações por taxa de transferência de bytes;
 - ✓ Principais hosts por número de ameaças identificadas;
- Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors);
- Possibilitar o registro de toda a comunicação realizada através do firewall, e de todas as tentativas de abertura de sessões ou conexões que forem recusadas pelo mesmo;
- Possuir sistema de respostas automáticas que possibilite alertar imediatamente o administrador através de e-mails, janelas de alerta na interface gráfica, execução de programas e envio de Traps SNMP;
- Possibilitar o armazenamento de seus registros (log e/ou eventos) na mesma plataforma de gerenciamento;
- Possuir mecanismo que permita inspecionar o tráfego de rede em tempo real (sniffer) via interface gráfica, podendo opcionalmente exportar os dados visualizados para arquivo formato PCAP e permitindo a filtragem dos pacotes por protocolo, endereço IP origem e/ou destino e porta IP origem e/ou destino, usando uma linguagem textual;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- Permitir a visualização do tráfego de rede em tempo real tanto nas interfaces de rede do Firewall quando nos pontos internos do mesmo: anterior e posterior à filtragem de pacotes, onde o efeito do NAT (tradução de endereços) é eliminado.

5.17. Monitoramento de infraestrutura física de Data Center

- Deve permitir visualizar os diferentes equipamentos (UPS, CRAC, PDU) a partir de uma só interface gráfica;
- Deve suportar diferentes modelos de Hardware e ser independente do fornecedor do Hardware;
- Deve suportar pelo menos os seguintes protocolos para coleta de dados:
 - ✓ SNMP;
 - ✓ MODBUS RTU;
 - ✓ MODBUS TCP;
 - ✓ BACNET;
 - ✓ OPC;
- Este mecanismo de coleta deve permitir, além da coleta através dos protocolos acima, a importação de dados externos via importação de arquivos;
- Deve possuir capacidade de monitorar diferentes tipos de equipamento como:
 - ✓ Quadros de energia (PDU), No-breaks(UPS);
 - ✓ Geradores;
 - ✓ Circuitos (BCMS);
 - ✓ Equipamentos de refrigeração / CRAC;
 - ✓ Sensores de ambiente (ex. Temperatura, humidade e pressão);
 - ✓ Utilidades (gás natural / água);
 - ✓ Deve realizar cálculo de métricas como PUE e DCiE em tempo real;
 - ✓ Deve permitir a criação de métricas customizadas a partir dos dados coletados;
 - ✓ Deve permitir consultar métricas em tempo real;



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE - SEA
INSTITUTO ESTADUAL DO AMBIENTE - INEA

- ✓ As métricas devem ser armazenadas na base de dados e devem poder gerar relatórios;
- ✓ As métricas devem ficar armazenadas na base de dados histórica, se houver degradações, indicá-las com alertas visuais e/ou notificar via trap, e-mail ou executar alguma outra ação;
- ✓ Apresentar dashboard online em interface web para cada equipamento, apresentando através de gráficos as métricas mais relevantes para o equipamento.



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE - SEA
INSTITUTO ESTADUAL DO AMBIENTE - INEA

5.18. Acordo de Nível de Serviço (ANS)

5.18.1. Os serviços serão medidos com base em indicadores de níveis de serviço específicos, para os quais serão estabelecidas metas e faixas de atendimento.

5.18.2. A apuração dos indicadores será feita a partir de relatórios baseados em informações do sistema de gerenciamento de chamados, fornecidos pela CONTRATADA.

5.18.3. As medições serão realizadas ao final de cada mês, compreendendo o período entre o primeiro e o último dia, exceto no mês de assinatura do contrato, no qual a medição compreenderá os serviços realizados entre a data de assinatura do instrumento contratual e o último dia do mês, bem como no último mês de vigência do contrato, em que se medirá o serviço prestado entre o primeiro dia deste mês e a data de encerramento do contrato.

5.18.4. A CONTRATADA será responsável pela elaboração do Relatório Mensal de Indicadores que conterá, dentre outras informações, a tabela de consolidação das medições dos indicadores definidos neste termo de referência, a partir dos dados dos sistemas supracitados e as eventuais justificativas no caso de desempenho inferior ao padrão esperado.

5.18.5. Fica a critério do INEA a realização de auditorias periódicas dos relatórios elaborados pela CONTRATADA.

5.18.6. Quaisquer indicadores influenciados negativamente por problemas ou por outros motivos os quais comprovadamente foram causados pelo INEA ou outro fornecedor não relacionado a este edital, não serão motivos de ajustes no pagamento ou de aplicação de penalidades à CONTRATADA.



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE - SEA
INSTITUTO ESTADUAL DO AMBIENTE - INEA

5.18.7. Gerenciamento de Eventos

Item	Indicadores de níveis de serviço	Meta
MO-01	<p>Tempo de detecção de eventos críticos na infraestrutura de TI do INEA, classificados como prioridade 1 (P1) na ferramenta de gerenciamento de chamados</p> <p>Razão entre o tempo de detecção do evento na ferramenta de monitoramento e abertura automática na ferramenta de gestão de gerenciamento de chamados, em até 5 (cinco minutos), e o total de eventos críticos gerados na ferramenta de monitoramento, em termos percentuais (%).</p>	99,5%
MO-02	<p>Tempo de notificação de eventos de prioridade críticos (P1 – Prioridade 1)</p> <p>Razão entre o tempo para envio de mensagem de notificação de incidentes de prioridade 1, identificado na infraestrutura do INEA, em até 15 (quinze) minutos, e o total de notificações enviadas por e-mail e SMS</p>	Maior ou igual a 85%



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

6. PAGAMENTO

6.1. O pagamento será realizado após apresentação da Nota Fiscal/Fatura, devidamente atestada por servidor designado ou comissão, mediante depósito em conta bancária indicada pela contratada, conforme o recebimento da nota de empenho, quantidade e prazos estipulados conforme demonstrado na tabela abaixo:

ITEM	DESCRIÇÃO	UNIDADE	QTD	PRAZO DE ENTREGA / INÍCIO
A	SOLUÇÃO DE SEGURANÇA DE PERÍMETRO – FIREWALL/UTM, COM SUBSCRIÇÃO DE 24 MESES, CONFORME DETALHADO NO ITEM 3.1.	UN	01	Deverá ocorrer no máximo até 30 dias após a data de emissão da Nota de Empenho.
B	SOLUÇÃO DE SEGURANÇA PARA PROTEÇÃO DE SERVIDORES VIRTUAIS E FÍSICOS, COM SUBSCRIÇÃO DE 24 MESES, CONFORME DETALHADO NO ITEM 3.2.	UN	60	Deverá ocorrer no máximo até 30 dias após a data de emissão da Nota de Empenho.
C	SERVIÇO DE INSTALAÇÃO, CONFIGURAÇÃO E SUPORTE POR 12 MESES – SOLUÇÃO DE SEGURANÇA DE PERÍMETRO – FIREWALL/UTM, CONFORME DETALHADO NO ITEM 4.1.	UN	01	Em até 5 dias corridos após a entrega do ITEM A.
D	SERVIÇO DE INSTALAÇÃO, CONFIGURAÇÃO E	UN	01	Em até 5 dias corridos após a



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE - SEA
INSTITUTO ESTADUAL DO AMBIENTE - INEA

	SUPOORTE POR 12 MESES – SOLUÇÃO DE SEGURANÇA DE SERVIDORES VIRTUAIS E FÍSICOS, CONFORME DETALHADO NO ITEM 4.2.			entrega do ITEM B.
E	SERVIÇO DE MONITORAMENTO DO AMBIENTE, CONFORME DETALHADO NO ITEM 5	SERVIÇO CONTINUADO	12 Meses	Em até 5 dias corridos após a data de emissão da Nota de Empenho

Tabela 1

- 6.2.** 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 iniciará-se após a comprovação da regularização da situação, não acarretando qualquer ônus para ao CONTRATANTE.
- 6.3.** Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.
- 6.4.** Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.
- 6.5.** A Contratada regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.
- 6.6.** Será verificada, ainda, a regularidade fiscal, através de consulta “on-line” ao Sistema de Cadastramento Unificado de Fornecedores – 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 8.666/93.



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE - SEA
INSTITUTO ESTADUAL DO AMBIENTE - INEA

- 6.7.** Quando da ocorrência de eventuais atrasos de pagamento provocados exclusivamente pelo CONTRATANTE, o valor devido deverá ser acrescido de atualização financeira, e sua apuração se fará desde a data de seu vencimento até a data do efetivo pagamento, em que os juros de mora serão calculados à taxa de 0,5% (meio por cento) ao mês, ou 6% (seis por cento) ao ano, mediante aplicação da seguinte fórmula: $I = (TX/100) \times 365 \times EM = I \times N \times VP$, onde: I = Índice de atualização financeira; TX = Percentual de taxa de juros de mora anual; EM = Encargos moratórios; N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento; VP = Valor da parcela em atraso.
- 6.8.** Na hipótese de pagamento de juros de mora e demais encargos por atraso, os autos devem ser instruídos com as justificativas e motivos, e ser submetidos à apreciação da autoridade superior competente, que adotará as providências para verificar se é ou não caso de apuração de responsabilidade, identificação dos envolvidos e imputação de ônus a quem deu causa.



7. HABILITAÇÃO TÉCNICA

- Atestado de capacidade técnica, emitido por pessoa jurídica de direito público ou privado, que comprove que a licitante executou de forma satisfatória, a prestação de serviços de monitoramento, gerenciamento de administração e suporte de infraestrutura de TI e dispositivos de segurança.

Será considerado o Atestado que verse sobre os seguintes serviços:

- Monitoramento contínuo de redes, servidores e aplicações, em regime 24x7, utilizando de equipe, processos e ferramentas, com a execução de rotinas de produção, a partir do seu NOC – Network Operation Center.
 - Administração e Suporte especializado a servidores e ativos de rede, prestados por Analista(s) prestados de forma remota e/ou presencial.
 - Administração e Suporte especializado de equipamentos de segurança em regime 24x7, prestados por analistas de forma remota e/ou presencial.
 - Gestão de incidentes de links de comunicação de dados incluindo a abertura e acompanhamento dos chamados junto a operadores de telecomunicação.
 - Gestão integrada do serviço envolvendo acompanhamento e controle de todas as atividades de manutenção, suporte e administração técnica, seguindo as boas práticas de gerenciamento de serviços de TI, criação e manutenção de processos e procedimentos, incluindo o acompanhamento e a manutenção de indicadores de qualidade.
- Atestado de capacidade técnica, emitido por pessoa jurídica de direito público ou privado, que comprove que a licitante forneceu e implantou solução de segurança de perímetro – Firewall/UTM de forma satisfatória, compatível com o objeto deste contrato.
 - Atestado de capacidade técnica, emitido por pessoa jurídica de direito público ou privado, que comprove que a licitante forneceu e implantou solução de proteção de servidores de forma satisfatória, compatível com o objeto deste contrato.



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- Atestado de capacidade técnica, emitido por pessoa jurídica de direito público ou privado, que comprove que a licitante forneceu e implantou solução de segurança para servidores físicos e virtuais de forma satisfatória, compatível com o objeto deste contrato.

O(s) atestado(s) de prestação de serviços contínuo apresentado(s) deve(m) cobrir período ininterrupto de 36 (trinta e seis) meses para que fique demonstrada a efetividade da CONTRATADA na prestação de atividades por período razoável.

- ✓ Ainda, com o objetivo de aferir a experiência do fornecedor na execução dos serviços de forma integrada, não será permitida a soma qualitativa de Atestados de Capacidade Técnica requisitados, ou seja, soma de tipos de serviços diferentes. Somente será permitida a soma de Atestados de Capacidade Técnica para demonstração quantitativa do total de parque de informática suportado e quantidade de atendimentos técnicos realizados.

O(s) Atestado(s) de Capacidade Técnica para fins de habilitação deverão ser apresentados em documento timbrado, atestando ainda que os serviços foram executados com bom desempenho e cumprimento a contento das obrigações contratuais, sendo apresentado(s) em via original ou cópia autenticada.

Apresentar, para a assinatura do contrato, comprovação de que a empresa possua em seu quadro de colaboradores no mínimo 01 (um) técnico treinado e certificado pelo fabricante para prestação do serviço de suporte técnico da solução de segurança de perímetro – Firewall/UTM.

A CONTRATADA deverá comprovar, para a assinatura do contrato, por qualquer meio, a autorização do(s) fabricante(s) para comercialização e implementação e suporte de toda a solução de segurança de perímetro – Firewall/UTM, objeto deste contrato.



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

8. HOMOLOGAÇÃO

A homologação do produto e prestação dos serviços, consiste em avaliar tecnicamente:

- Performance em teste de bancada;
- Homologação da Infraestrutura de Monitoramento;
- Software de Monitoramento;
- Processo de notificação;
- Redundância de Comunicação de Dados;
- Infraestrutura Física (painéis de monitoramento, mobiliário, espaço dedicado para a atividade de monitoramento).



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

9. DEVERES E RESPONSABILIDADES DO CONTRATANTE

- 9.1.** O CONTRATANTE designará uma comissão, de no mínimo 3 (três) membros do efetivo, para fiscalizar, acompanhar e receber o instrumento contratual.
- 9.2.** O objeto será aceito por uma Comissão de Fiscalização e Recebimento, genericamente chamada de equipe de fiscalização.
- 9.3.** A equipe de fiscalização representará o CONTRATANTE e terá as atribuições delegadas em ato específico e, ainda, as que se seguem: a) tomar todas as providências necessárias ao imediato acionamento do representante da CONTRATADA, logo que constatada qualquer irregularidade por parte da mesma, a fim de solucionar os problemas detectados; b) registrar todas as ocorrências relacionadas com a execução do objeto desta licitação, determinando o que for necessário à regularização dos defeitos observados; c) certificar faturas correspondentes e encaminhá-las ao setor responsável do CONTRATANTE, após constatar o fiel cumprimento das obrigações contratuais; d) calcular e propor, nos termos contratuais, a(s) multa(s) devida(s) pela CONTRATADA; e e) realizar o exame quantitativo e qualitativo em até 20 (vinte) dias úteis, recebendo e aceitando o objeto.
- 9.4.** Prestar as informações necessárias e relevantes, bem como os esclarecimentos que venham a ser solicitados pela empresa contratada ou pelo seu preposto.
- 9.5.** Efetuar o pagamento à CONTRATADA de acordo com os serviços prestados e nas condições estabelecidas no edital.
- 9.6.** Permitir o acesso dos técnicos da empresa CONTRATADA, para execução dos serviços previstos, desde que previamente identificados e credenciados.
- 9.7.** Relacionar-se com a CONTRATADA, exclusivamente através de pessoa por ela indicada.
- 9.8.** Assegurar-se da boa realização da prestação do serviço verificando sempre os níveis de serviço do presente Termo de Referência.
- 9.9.** Assegurar-se que os preços contratados estão compatíveis com aqueles praticados no mercado.



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- 9.10.** Documentar as ocorrências decorrentes de sua Fiscalização, verificar o cumprimento das obrigações da Empresa Contratada, aplicando-lhe as penalidades cabíveis quando do descumprimento daquelas, ressalvados os casos de força maior, justificados e aceitos pelo Ordenador de Despesa.
- 9.11.** Proporcionar todas as condições e prestar as informações necessárias para que a CONTRATADA possa cumprir com suas obrigações, dentro das normas e condições contratuais.
- 9.12.** Comunicar oficialmente à CONTRATADA quaisquer falhas verificadas no cumprimento do contrato.
- 9.13.** Definir, controlar e cobrar a execução das atividades dos técnicos disponibilizados pela CONTRATADA.
- 9.14.** Encaminhar para o atesto dos gestores as faturas emitidas e produtos dos serviços prestados.
- 9.15.** Registrar e oficializar à CONTRATADA, as ocorrências de desempenho ou comportamento insatisfatório, irregularidades, falhas, insuficiências, erros e omissões constatados, durante a execução do Contrato, para as devidas providências.

10. DEVERES E RESPONSABILIDADES DA CONTRATADA

- 10.1.** Fornecer o objeto deste Termo de Referência dentro dos padrões e requisitos estabelecidos e realizar entrega dos itens, estritamente de acordo com as especificações. Todos os itens fornecidos deverão ser originais de fábrica, da marca do produto, não sendo de forma alguma reconicionados, remanufaturados, reutilizados, de demonstração, gateways, protótipos ou composições feitas única e exclusivamente para o presente certame. Não será aceito o emprego de item usado, danificado, improvisado e adaptado, tampouco oriundo de estande de venda (colocado em exposição).
- 10.2.** Apresentar à equipe de fiscalização, por escrito, antes do início da execução do instrumento contratual, e sempre que solicitado, o representante credenciado para atuar em seu nome e representá-la junto ao CONTRATANTE, com autoridade para resolver problemas relacionados com o seu cumprimento, que doravante será denominado PREPOSTO.



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- 10.3.** Manter durante toda a execução do contrato as condições de habilitação e qualificação exigidas na licitação. Cumprir todas as leis e posturas federais, estaduais e municipais pertinentes e vigentes, bem como assegurar os direitos, sendo a única responsável por prejuízos decorrentes de infrações a que houver dado causa.
- 10.4.** Reparar, corrigir, remover ou substituir, no prazo que lhe for determinado, sem ônus para o CONTRATANTE sem prejuízo das sanções cabíveis, no todo ou em parte, o objeto do instrumento contratual ou equivalente, que se verificarem pela equipe de fiscalização, vícios, defeitos ou incorreções resultantes da fabricação ou da execução do serviço de suporte técnico.
- 10.5.** Providenciar as correções/substituições necessárias em quaisquer produtos rejeitados pela equipe de fiscalização e que não satisfaçam aos níveis de qualidade previstos.
- 10.6.** Responsabilizar-se pelas despesas decorrentes da rejeição, pela equipe de fiscalização, dos itens, e pelos atrasos acarretados por esta rejeição.
- 10.7.** Comunicar ao 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.
- 10.8.** Alertar o CONTRATANTE, através da equipe de fiscalização, por escrito e com a urgência necessária, sobre as deficiências ou erros verificados nas especificações e nos demais documentos técnicos, que possam pôr em risco a segurança dos serviços, torná-los inadequados às suas finalidades ou onerar desnecessariamente seus custos.
- 10.9.** Prestar toda assistência técnico-administrativa necessária junto à equipe de fiscalização, verificando discrepâncias, esclarecendo dúvidas, estabelecendo prioridades, enfim, mantendo todos os entendimentos capazes de conduzir a perfeita execução do instrumento contratual ou instrumento equivalente.
- 10.10.** Solicitar, previamente e formalmente, autorização à equipe de fiscalização sempre que necessitar executar atividades especiais ou não previstas.



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

- 10.11.** Observar, rigorosamente, toda a regulamentação aplicável, especificações, detalhes e normas existentes, respondendo por quaisquer falhas e outras faltas, que serão sanadas sem ônus adicionais para o CONTRATANTE.
- 10.12.** Não transferir a outrem, no todo ou em parte, o objeto do instrumento contratual ou instrumento equivalente.
- 10.13.** Facilitar à equipe de fiscalização o pleno exercício de suas funções, prestando-lhe todos os esclarecimentos e informações administrativas e/ou técnicas que lhe forem solicitadas, exibindo-lhe todos os documentos e dados de interesse para acompanhamento e fiscalização da execução do instrumento contratual ou instrumento equivalente.
- 10.14.** O exercício das funções da equipe de fiscalização não desobriga a CONTRATADA de sua própria responsabilidade, quanto à adequada, pronta e fiel execução do objeto contratado.
- 10.15.** Responsabilizar-se civilmente por seus funcionários, bem como por qualquer dano que, direta ou indiretamente, ocasionar a bens do CONTRATANTE ou sob a sua responsabilidade, ou ainda, a terceiros, durante a execução do instrumento contratual. Recolher, ao Órgão as importâncias referentes às multas que lhe forem aplicadas ou às indenizações devidas, no prazo de 5 (cinco) dias úteis, a contar da notificação de multa ou solução definitiva de recurso.
- 10.16.** Solicitar, previamente e formalmente, autorização ao CONTRATANTE na veiculação, publicidade ou qualquer outra informação acerca das atividades objeto do Contrato.
- 10.17.** Ter pleno conhecimento de todas as condições e peculiaridades inerentes ao objeto não podendo invocar posteriormente desconhecimento para cobrança de serviços extras.
- 10.18.** Zelar para que os itens solicitados sejam 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 o armazenamento.
- 10.19.** Respeitar as Normas Brasileiras – NBR publicadas pela Associação Brasileira de Normas Técnicas sobre resíduos sólidos.



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE - SEA
INSTITUTO ESTADUAL DO AMBIENTE - INEA

10.20. Entregar o objeto deste Termo de Referência, no prazo máximo de 30 (trinta) dias corridos, a contar da data de recebimento da Ordem de Fornecimento de Bens.

11. DA GARANTIA

11.1. No prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do INEA, contados da data da assinatura do contrato, o licitante vencedor prestará garantia de 5% (cinco por cento) sobre o valor global do contrato, podendo optar por quaisquer das seguintes modalidades (§ 1º do art. 56 da Lei nº 8.666/93):

I - Caução em Dinheiro – a garantia em dinheiro deverá ser efetuada, obrigatoriamente, na Caixa Econômica Federal (Decreto-Lei nº 1.737/79, art. 1º, inciso IV), pelo interessado, em conta específica em favor do contratante, com correção monetária, vinculada ao INEA;

II – Caução em Títulos da Dívida Pública – o depósito em títulos da dívida pública será efetuado em conta de custódia, aberta na Caixa Econômica Federal, vinculada ao INEA, devidamente escriturados em sistema centralizado de liquidação e custódia, considerados, obrigatoriamente, por seu valor econômico informado pelo Tesouro Nacional;

III – Fiança Bancária – será realizada mediante entrega de carta de fiança fornecida por estabelecimento bancário, devidamente registrada em cartório de registro de títulos e documentos, conforme determinado pela Lei nº 6.015/73, art. 129 e deverá vir acompanhada de: a) cópia autenticada do estatuto social do banco; b) cópia autenticada da ata da assembleia que elegeu a última diretoria do banco; c) cópia autenticada do instrumento de procuração, em se tratando de procurador do banco; d) reconhecimento de firmas das assinaturas constantes da carta de fiança. IV – Seguro Garantia – será realizado mediante a entrega da apólice, inclusive digital, emitida por empresa em funcionamento no Brasil, legalmente autorizada, sendo o INEA o único beneficiário do seguro.





GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE - SEA
INSTITUTO ESTADUAL DO AMBIENTE - INEA

- 11.2.** A garantia será considerada extinta: a) com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da Administração, mediante termo circunstanciado, de que a contratada cumpriu todas as cláusulas do contrato; e b) após o término da vigência do contrato acrescido de 3 (três) meses.
- 11.3.** O prazo de extinção da garantia poderá ser estendido em caso de ocorrência de sinistro. A perda da garantia em favor do INEA, em decorrência de rescisão unilateral do contrato, far-se-á de pleno direito, independentemente de qualquer procedimento judicial e sem prejuízo das demais sanções previstas no contrato.
- 11.4.** Não serão admitidas outras hipóteses de não execução da garantia, que não as previstas no subitem.



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE - SEA
INSTITUTO ESTADUAL DO AMBIENTE - INEA

ANEXO I

RELAÇÃO DE ATIVOS

NOME DO SERVIDOR	SISTEMA OPERACIONAL
VXRail - NODE 1	VSPHERE 6.x / VSAN
VXRail - NODE 2	VSPHERE 6.x / VSAN
VXRail - NODE 3	VSPHERE 6.x / VSAN
VXRail - NODE 4	VSPHERE 6.x / VSAN
PRAIADOSUL	Windows 2008 Server Enterprise R2
MASSAMBABA	AIX 5.3
IPCOPY	Linux
ITATIAIA2	Oracle Enterprise Linux 6.4
ITATIAIA1	Oracle Enterprise Linux 6.4
AVENTUREIRO1	Oracle VM Server
AVENTUREIRO2	Oracle VM Server
AVENTUREIRO3	Oracle VM Server
AVENTUREIRO4	Oracle VM Server
AVENTUREIRO5	Oracle VM Server
GUANDU	Redhat 5.7
ARARAS	Ubuntu 16.04
SAPIATIBA	Windows 2003 Server Standard
FRADES	Windows 2008 Server Enterprise R2
GERICINO	Windows 2008 Server Enterprise R2
MACACU	Windows 2008 Server Enterprise R2
MANGARATIBA	Windows 2008 Server Enterprise R2
MENDANHA	Windows 2008 Server Enterprise R2
PAUBRASIL	Windows 2008 Server Enterprise R2
TAMOIOS	Windows 2008 Server Enterprise R2
VENEZUELA	Windows 2008 Server Enterprise R2
GUARATIBA	Windows 2008 Server Standard
JACARANDA	Windows 2008 Server Standard



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

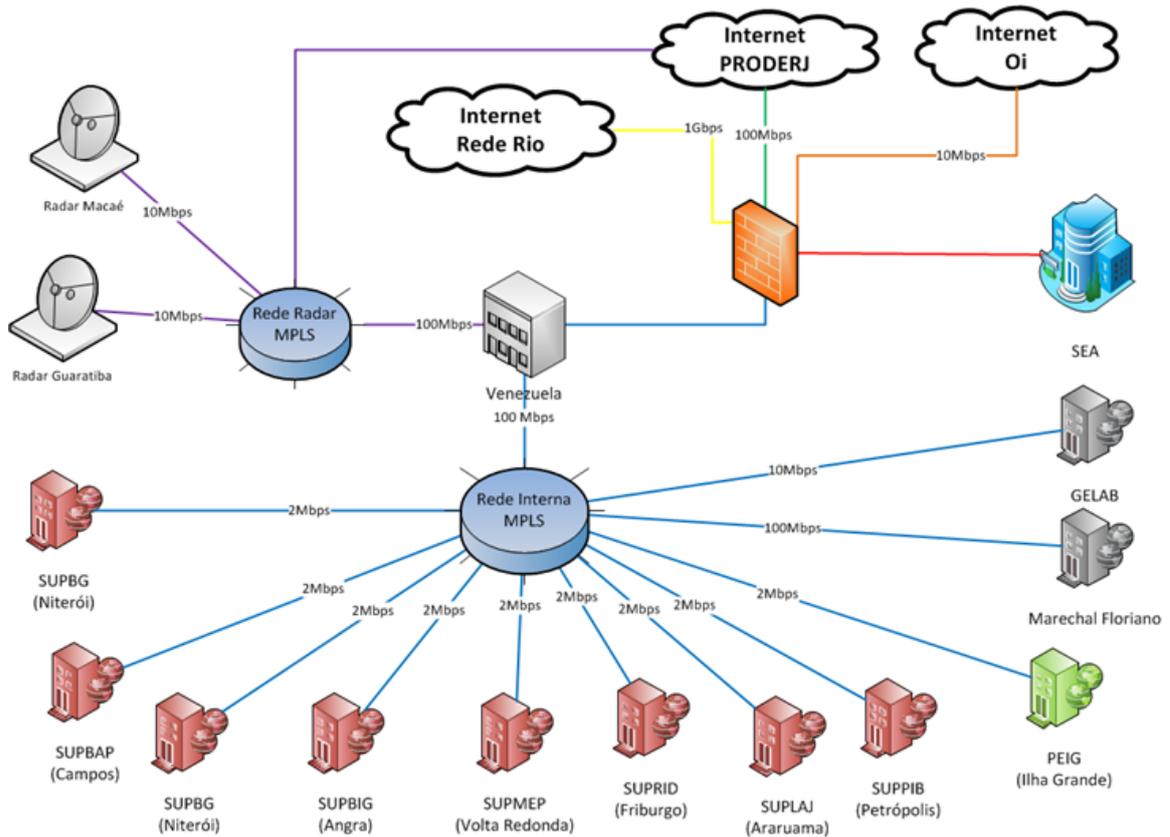
JURUBATIBA	Windows 2008 Server Standard R2
SERVER-ALMOX	Windows 7 Profissional
GEAR1TELE06	Windows XP Professional
PC-BP005367	Windows XP Professional
CONCORDIA2	CentOS 6.7
RECEP	CentOS 6.8
BOCAINA	Oracle Enterprise Linux 6.4
DESENGANO	Oracle Enterprise Linux 6.4
GRAJAU	Oracle Enterprise Linux 6.4
GUANABARA	Oracle Enterprise Linux 6.4
GUAXINDIBA	Oracle Enterprise Linux 6.4
MARICA	Oracle Enterprise Linux 6.4
PEDRABRANCA1	Oracle Enterprise Linux 6.4
PEDRABRANCA2	Oracle Enterprise Linux 6.4
TIJUCA	Oracle Enterprise Linux 6.4
TRESPICOS	Oracle Enterprise Linux 6.4
TINGUA	Oracle Enterprise Linux 6.5
RESTINGA	Oracle Enterprise Linux 6.6
CONCORDIA	Redhat 5.7
CAGARRAS	Ubuntu 14.04
SERVER-VIRUS2	Windows 2003 Server Standard R2
SRV-TFS	Windows 2008 Server Enterprise R2

- Obs.: Serão monitorados ainda os 02 Switches “Top of Rack” da Solução de Hiperconvergência, modelo DELL EMC S4048T-ON



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE - SEA
INSTITUTO ESTADUAL DO AMBIENTE - INEA

Diagrama de Topologia Lógica





GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE - SEA
INSTITUTO ESTADUAL DO AMBIENTE - INEA

Links de Internet:

Descrição/Provedor	Localização	Banda/Tecnologia
Externo/Oi	Venezuela	10 Mbps / IP Connect
Principal/PRODERJ	Venezuela	100 Mbps / MPLS
Radar/PRODERJ	Venezuela	100 Mbps / MPLS
Rede Rio/FAPERJ	Venezuela	1000 Mbps / MPLS

Links MPLS

Descrição	Localização	Banda
Rede INEA	Venezuela	100 Mbps
Radar Guaratiba	Fazenda Modelo	16 Mbps
Radar Macaé	UENF Macaé	16 Mbps
Rede INEA	GELAB	16 Mbps
Rede INEA	SUPLAJ	16 Mbps
Rede INEA	SUPBIG	16 Mbps
Rede INEA	SUPBAP	16 Mbps
Rede INEA	SUPMA	16 Mbps
Rede INEA	SUPRID	16 Mbps
Rede INEA	SUPBG	16 Mbps



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE - SEA
INSTITUTO ESTADUAL DO AMBIENTE - INEA

Rede INEA	SUPPIB	16 Mbps
Rede INEA	SUPMEP	16 Mbps
Rede INEA	PEIG	16 Mbps
Rede INEA	MARECHAL	100Mbps



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

ANEXO 2

MOLDELO DE PROPOSTA DE PREÇOS PROPOSTA DE PREÇOS DE PRESTAÇÃO DE SERVIÇOS

IDENTIFICAÇÃO DO PROPONENTE:
RAZÃO SOCIAL:
CNPJ e INSCRIÇÃO ESTADUAL:
ENDEREÇO e TELEFONE:
RESPONSÁVEL:
AGÊNCIA e Nº DA CONTA CORRENTE:

1. APRESENTAÇÃO

1.1. Apresentamos nossa Carta-Proposta para todos os itens descritos abaixo:

2. CONDIÇÕES GERAIS

2.1. O PROPONENTE declara conhecer os termos do instrumento do Termo de Referência em questão.

3. PREÇO DO SERVIÇO

Pela prestação dos serviços, cobraremos a importância total de R\$..... (.....) (Em algarismos e por extenso), observado a planilha abaixo:





GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

Item	Denominação	Unid.	Qtde	Valor Unitário (R\$)	Valor Total (R\$)
1	SOLUÇÃO DE SEGURANÇA DE PERÍMETRO – FIREWALL/UTM, COM SUBSCRIÇÃO DE 24 MESES, CONFORME DETALHADO NO ITEM 3.1.	UN	01		
2	SOLUÇÃO DE SEGURANÇA PARA PROTEÇÃO DE SERVIDORES VIRTUAIS E FÍSICOS, COM SUBSCRIÇÃO DE 24 MESES, CONFORME DETALHADO NO ITEM 3.2.	UN	60		
3	SERVIÇO DE INSTALAÇÃO, CONFIGURAÇÃO E SUPORTE POR 12 MESES – SOLUÇÃO DE SEGURANÇA DE PERÍMETRO – FIREWALL/UTM, CONFORME DETALHADO NO ITEM 4.1.	UN	1		
4	SERVIÇO DE INSTALAÇÃO, CONFIGURAÇÃO E SUPORTE POR 12 MESES – SOLUÇÃO DE SEGURANÇA DE SERVIDORES VIRTUAIS E FÍSICOS, CONFORME DETALHADO NO ITEM 4.2.	UN	1		
5	SERVIÇO DE MONITORAMENTO DO AMBIENTE, CONFORME DETALHADO NO ITEM 5	Serviço Mensal	12		
				TOTAL GLOBAL:	



GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

ANEXO III

TERMO DE COMPROMISSO DE CONFIDENCIALIDADE

De um lado a (nome empresarial), com sede (endereço completo), inscrita no CNPJ/MF sob o nº (.....), neste ato representada legalmente por (nome e CPF), doravante designada COMPROMITENTE; de outro, o INEA, com sede na [ENDEREÇO], inscrito no CNPJ/MF sob o nº XXXXXXXXXX, neste ato representado por seu Presidente XXXXXXXX, doravante designado INEA.

CONSIDERANDO que na execução do contrato nº (.....), decorrente do processo administrativo nº (.....), tendo por objeto (.....), a COMPROMITENTE terá acesso a informações contidas em processos e/ou documentos, ou armazenadas em meio físico, magnético ou eletrônico e/ou outros meios, as quais podem ter caráter sigiloso ou confidencial, as partes celebram o presente TERMO DE COMPROMISSO DE CONFIDENCIALIDADE, doravante designado TERMO, regido por disposições da Constituição Federal, da Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil Brasileiro), da Lei nº 11.111, de 5 de maio de 2005 (sobre informações sigilosas) e pelas cláusulas e condições a seguir estabelecidas.

CLÁUSULA PRIMEIRA – OBJETO

Constitui objeto do presente TERMO a proteção das informações de caráter sigiloso e/ou confidencial disponibilizadas pelo INEA para a COMPROMITENTE em razão do contrato nº (.....), que tem por objeto (.....).

Parágrafo primeiro - O compromisso de confidencialidade assumido pela COMPROMITENTE através deste TERMO é extensivo aos seus representantes, prepostos, administradores, consultores, funcionários e terceiros que tiverem acesso às informações mencionadas no *caput* desta cláusula.

Parágrafo segundo – O compromisso de confidencialidade abrange todos os produtos, atuais e futuros; informações assistenciais, resultados de exames, mapas; informações contábeis, financeiras, técnicas, estratégicas ou negociais; nomes de clientes, endereços e outros dados afins; contratos, práticas, procedimentos e outras informações comerciais; softwares, relatórios, estratégias, planos, documentos, desenhos, máquinas, ferramentas, modelos, descrições de patentes, amostras e materiais, quando relacionados ao objeto descrito no *caput* desta cláusula.





GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DO AMBIENTE – SEA
INSTITUTO ESTADUAL DO AMBIENTE – INEA

CLÁUSULA SEGUNDA – DEFINIÇÃO

Entende-se por informação confidencial toda informação classificada sob a rubrica *'acesso restrito a determinadas categorias específicas de pessoas, por força de lei ou de regulamento'*, contida em qualquer documento ou gravada em qualquer meio físico, magnético ou eletrônico, ou, ainda, aquela informação contida em qualquer documento ou gravada em qualquer meio físico, magnético ou eletrônico, cuja revelação ou divulgação afete a privacidade, o bem-estar e a segurança de indivíduos, de grupos e de instituições.

CLÁUSULA TERCEIRA – INFORMAÇÕES EXCLUÍDAS DA CONFIDENCIALIDADE

Não são consideradas confidenciais:

- 3.1. Informações cujo uso for expressamente autorizado pelo INEA, sem restrição.
- 3.2. Informações que se tornaram de domínio público, sem qualquer ação ou omissão da COMPROMITENTE.
- 3.3. Informações obtidas de forma independente e disponibilizadas pela própria COMPROMITENTE, sem qualquer referência ou vínculo com as informações consideradas confidenciais.

CLÁUSULA QUARTA – FORO

Fica eleito o foro da XXXXXXXXXXXXXXXX, RJ, para dirimir eventual controvérsia relativa ao presente compromisso de confidencialidade.

Rio de Janeiro, xx de xxxxxxxxxxxx de 201x.

(Nome)

Representante Legal da COMPROMITENTE

