ANEXO I - TERMO DE REFERÊNCIA

1. UNIDADE REQUISITANTE: ETICE

2. DO OBJETO

Contratação de empresa para prestação de serviços gerenciados de segurança da informação, de acordo com o seguinte escopo:

2.1. Serviços de Implantação da solução configurados em alta disponibilidade, para controle do tráfego na borda da rede corporativa do estado do Ceará;

2.2. Serviços de Implantação da solução configurados em alta disponibilidade, para prevenção de intrusão (IPS);

2.3. Serviços técnicos em Segurança Corporativa e Controles Internos, Serviços de operação de recursos de Segurança Corporativa e monitoramento especializado (incluindo os itens 2.1 e 2.2), e outros serviços operacionais.

O modelo de contratação ocorrerá através da aquisição de 4.000 (quatro mil) USEs (Unidade de Serviço da Etice). Para compor tal quantitativo, há dois grupos conforme ilustra a tabela abaixo:

Grupo	Descrição	Quantidade USE (máxima anual)
1	– Serviços de Implantação da solução configurados em alta disponibilidade, para controle do tráfego na borda da rede corporativa do estado do Ceará (item 2.1). – Serviços de Implantação da solução configurados em alta disponibilidade, para prevenção de intrusão (IPS) (item 2.2).	2.000
2	– Serviços técnicos em Segurança Corporativa e Controles Internos; – Serviços de operação de recursos de Segurança Corporativa e monitoramento especializado; – Serviços de análise em Segurança Corporativa; – Outros serviços operacionais.	2.000
	Total do montante anual	**4.000**

A Execução da Continuidade dos Serviços está plenamente orientada ao cumprimento do ANEXO A – Nível de Acordo de Serviços (SLA), deste termo. Mensalmente, um quantitativo deverá ser utilizado e poderá ser glosado conforme casos do descumprimento de um ou mais itens do SLA, em conjunto com as penalidades e sanções.

O valor de cada USE é único para todos os grupos (e níveis de atendimento).

3. DA JUSTIFICATIVA

3.1 O data center da Etice tem uma fundamental função no Cinturão Digital do Ceará(CDC), provendo o acesso à Internet e a necessária segurança da informação, portanto faz-se necessário prover excelência na alta disponibilidade dos recursos de TI.

3.2 Os equipamentos responsáveis pelo controle do tráfego na borda da rede corporativa e controle de prevenção de intrusão já se encontram fora do período de garantia.

3.3 O crescimento do tráfego da internet e somado a tudo isto a crescente necessidade de prevenção de intrusão, faz-se necessária a atualização dos equipamentos e de serviços de operação dos recursos de segurança corporativa.

3.4 O método de contratação escolhido foi de contratação de serviços, com acompanhamento da qualidade dos serviços, o que garante um nível de serviço constante ao longo do tempo, não sofrendo com a obsolescência dos equipamentos.

4. DAS ESPECIFICAÇÕES E QUANTITATIVOS

4.1. Serviços de Implantação da solução configurados em alta disponibilidade, para controle do tráfego na borda da rede corporativa do estado do Ceará

4.1.1. Dois Switches L3 para Borda Internet 24 portas 1 GBE (1000BASE-T), 24 portas (SFP), 6 portas 10 GBE com capacidade para 2,5 milhões de rotas BGP-4 e fonte redundante 110/220 AC;

4.1.2. Switch de Borda para estabelecer a conexão da rede governamental com os provedores de backbone Internet. Deverá suportar protocolo BGP-4 e memória capaz de receber full-routing;

4.1.3. Características Gerais:

4.1.3.1. Switch Ethernet de camada 3, compatível com as tecnologias Ethernet, Fast Ethernet e Gigabit Ethernet, com pelo menos 24 (vinte e quatro) portas 10/100/1000 Mbps UTP, 24 (quatro) portas óticas, com suporte a módulos de fibra multimodo e monomodo (SFP), sendo admitida interface combo;

4.1.3.2. Possuir pelo menos 6 (seis) portas 10 Gigabit Ethernet UTP ou Direct Attach com cabo de 10 m;

4.1.3.3. Possuir fonte de alimentação redundante;

4.1.3.4. Implementar encaminhamento IPv6 em hardware;

4.1.3.5. Roteamento e comutação de jumbo frames (pelo menos 9000 bytes).

4.1.4. Protocolos e padrões requeridos

4.1.4.1. Ethernet 10BaseT (IEEE 802.3);

4.1.4.2. Fast Ethernet 100BaseTX (IEEE 802.3u);

4.1.4.3. Gigabit Ethernet 1000BaseT (IEEE 802.3ab);

4.1.4.4. Gigabit Ethernet (IEEE 802.3ae);

4.1.4.5. RSTP Rapid Spanning Tree Protocol (IEEE 802.1w);

4.1.4.6. MSTP Multiple Spanning Tree Protocol (IEEE 802.1s);

4.1.4.7. VLANs (IEEE 802.1Q);

4.1.4.8. Link Aggregation (IEEE 802.3ad);

4.1.4.9. Priority Queue (IEEE 802.1p);

4.1.4.10. VMAN Q-in-Q VLAN Tag (QinQ) (IEEE 802.1ad) e/ou M-in-M VLAN Tag (MinM) (IEEE 802.1ah);

4.1.4.11. Routing Information Protocol RIPv2 (RFC2453);

4.1.4.12. Open Shortest Path First OSPFv2 (RFC2328);

4.1.4.13. Border Gateway Protocol Version 4 BGP-4 (RFC4271);

4.1.4.14. BGP Confederations (RFC 5065);

4.1.4.15. BGP Route Reflection (RFC 2796);

4.1.4.16. BGP Route Flap Dampening (RFC 2439);

4.1.4.17. TCP MD5 Authentication for BGP (RFC 2385);

4.1.4.18. Internet Group Management Protocol – IGMPv1 (RFC 1112);

4.1.4.19. Internet Group Management Protocol - IGMPv2 (RFC 2236);

4.1.4.20. Internet Group Management Protocol - IGMPv3 (RFC 3376);

4.1.4.21. Protocol Independent Multicast Sparse Mode - PIM-SM (RFC 2362);

4.1.4.22. Network Time Protocol - NTP (RFC1305) e/ou Simple Network Time Protocol - SNTP (RFC2030);

4.1.4.23. An Architecture for Differentiated Services (RFC2475);

4.1.4.24. DiffServ Expedited Forwarding EF (RFC3246) e DiffServ Assured Forwarding AF (RFC2597);

4.1.4.25. Link Layer Discovery Protocol - LLDP (IEEE 802.1AB);

4.1.4.26. Virtual Router Redundancy Protocol - VRRP (RFC 3768);

4.1.4.27. RIPng for IPv6 (RFC 2080);

4.1.4.28. OSPFv3 for IPv6 (RFC 2740);

4.1.4.29. BGP-MP for IPv6 (RFC 2545).

4.1.4.30. Gerenciamento

4.1.4.31. Protocolo de Gerenciamento SNMPv1, SNMPv2, SNMPv3;

4.1.4.32. Suporte a 4 grupos de RMON (estatísticas, histórico, alarmes e eventos);

4.1.4.33. Interface de gerenciamento baseada em WEB (HTTP) e/ou CLI;

4.1.4.34. Porta do console para gerenciamento e configuração via linha de comando com conector RJ-45 e/ou RS-232. (Os cabos e eventuais adaptadores necessários para acesso à porta de console devem ser fornecidos.);

4.1.4.35. Suporte a SSL e/ou SSHv2;

4.1.4.36. Permitir atualização de firmware via TFTP;

4.1.4.37. Possuir suporte a espelhamento de portas para uma porta específica de modo a permitir a conexão de um analisador externo;

4.1.4.38. Implementa recursos de análise de rede e serviços de monitoração de tráfego, em todas as portas, utilizando como base e tecnologia sFLOW (RFC 3176), IPFIX (RFC 3917).

4.1.4.39. Desempenho

4.1.4.40. Possuir desempenho de no mínimo 100 Mpps considerando pacotes de 64 bytes;

4.1.4.41. Possuir matriz de comutação de pelo menos 128 Gbps;

4.1.4.42. Suportar um mínimo de 2.500.000 (dois milhões e quinhentas mil) entradas na tabela de rotas IPv4 em memória de encaminhamento em hardware (FIB).

4.1.4.43. Suportar um mínimo de 256.000 (duzentos e cinquenta e seis mil) entradas na tabela de rotas IPv6 em memória de encaminhamento em hardware (FIB).

4.1.4.44. Suportar no mínimo 256 peers BGP-4.

4.1.4.45. Deve implementar no mínimo 4000 VLANs segundo o protocolo IEEE 802.1Q;

4.1.4.46. Suportar quantidade mínima de 128.000 MAC addresses.

4.1.4.47. Quantidade mínima de 8 filas segundo o protocolo IEEE 802.1p.

4.1.5. Qualidade de Serviço

4.1.5.1. Mecanismos de classificação, marcação, priorização de tráfego, aplicáveis por interfaces físicas ou lógicas, sem impacto no desempenho de encaminhamento de pacotes;

4.1.5.2. Mecanismos de limitação de tráfego (rate-limit), aplicáveis sem impacto no desempenho de encaminhamento de pacotes e com granularidade mínima de 100 Kbps para portas de 1 GE e 1 Mbps nas portas de 10 GE.

4.1.6. Segurança

4.1.6.1. Filtros de camada 2, 3 e 4 aplicáveis em interfaces físicas ou lógicas sem impacto no desempenho de encaminhamento de pacotes;

4.1.6.2. Deve implementar network login através do padrão IEEE 802.1x;

4.1.6.3. Possuir suporte a associação de um endereço MAC específico a uma dada porta do Switch, de modo que somente a estação que tenha tal endereço possa usar a referida porta para conexão;

4.1.6.4. Suporte ao protocolo de autenticação, autorização e accounting (AAA) TACACS+ e/ou RADIUS para controle do acesso administrativo, por usuário, ao equipamento. Deve ser possível fazer a autenticação, autorização de comandos e “accounting” de comandos em qualquer acesso administrativo ao equipamento;

4.1.6.5. Implementar SSHv2 para acesso remoto;

4.1.6.6. Implementar controle e contenção de broadcast storm;

4.1.6.7. Implementar mecanismos de proteção contra ataque DoS e/ou DDoS.

4.1.7. Generalidades

4.1.7.1. Deverá possuir estrutura apropriada para acondicionamento em armário de fiação (rack) padrão 19 polegadas e vir acompanhado do respectivo kit de suporte específico para montagem;

4.1.7.2. A fonte alimentação deverá funcionar com tensão elétrica nominal de 110V~220V AC, 50~60Hz, de modo automático;

4.1.7.3. Possuir fonte de alimentação redundante suficiente para a configuração proposta;

4.1.7.4. Deverá ser acompanhado, ou disponibilizado on-line, de documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento;

4.1.7.5. Deverá ser fornecido com todos os acessórios necessários para operacionalização do equipamento, tais como software, cabos lógicos, cabos de interface de configuração e cabos de energia elétrica.

4.1.7.6.

4.2. Serviços de Implantação da solução configurados em alta disponibilidade, para prevenção de intrusão (IPS);

4.2.1. Solução de Gerência de IPS

4.2.1.1. Características Mínimas

4.2.1.1.1. Hardware dedicado tipo appliance com Sistema Operacional customizado para garantir segurança e melhor desempenho;

4.2.1.1.2. Possuir quantidade de memória e processamento mínima suficiente para atendimento de todas as funcionalidades e desempenho solicitados neste documento;

4.2.1.1.3.

4.2.1.1.4. Appliance para instalação em rack padrão 19 polegadas, devendo possuir altura máxima de 2U (unidade de rack);

4.2.1.1.5. Deve ser acompanhada de todos os cabos e suportes (gavetas e braços) necessários para a instalação do equipamento;

4.2.1.1.6. Possuir no mínimo 1 TB de disponibilidade de armazenamento em disco;

4.2.1.1.7. Deve ser fornecido com fontes internas de alimentação redundante do tipo hot-swap com capacidade para suportar toda a solução, sem perda de funcionalidade ou capacidade, no caso de falha das fontes principais;

4.2.1.1.8. Deve possuir fonte de alimentação com chaveamento automático 110/220V – 50/60Hz;

4.2.1.1.9. Deverá suportar o armazenamento mínimo de 20.000.000 (vinte milhões) de eventos.

4.2.1.2. Interfaces da Solução

4.2.1.2.1. Possuir no mínimo duas interfaces de gerência Ethernet 10/100/1000Base-T em modo full-duplex.

4.2.1.3. Funcionalidades Gerais

4.2.1.3.1. A plataforma de gerenciamento deve ser baseada em um sistema operacional customizado e seguro;

4.2.1.3.2. A plataforma de gerenciamento deve ser capaz de fazer a gestão centralizada da saúde física dos sensores monitorados;

4.2.1.3.3. A plataforma de gerenciamento deve ser capaz de agregar e centralizar os eventos IDS / IPS monitorando em tempo real e permitir a análise forense de eventos detectados;

4.2.1.3.4. A plataforma de gerenciamento deve permitir a visualização de indicadores de desempenho do tráfego de rede e nos principais eventos de segurança;

4.2.1.3.5. A plataforma de gerenciamento deve possibilitar o agendamento de tarefas rotineiras, como cópias de segurança, atualizações e geração de relatórios;

4.2.1.3.6. A plataforma de gerenciamento deve ser capaz de criar grupos usando os seguintes parâmetros:

4.2.1.3.6.1. Sensores;

4.2.1.3.6.2. Conjunto de Interfaces de um único equipamento;

4.2.1.3.6.3. Conjunto de Interfaces de equipamentos distintos;

4.2.1.3.6.4. Deverá permitir aplicar políticas de segurança de forma coletiva (por grupo).

4.2.1.3.7. A plataforma de gestão deve possuir a capacidade de visualizar, habilitar, desabilitar e modificar regras individuais, bem como grupos ou categorias de regras;

4.2.1.3.8. A plataforma de gerenciamento deve ser capaz de receber automaticamente as atualizações disponibilizadas pelo fabricante e permitir que sejam distribuídas e aplicadas nos sensores manualmente ou automaticamente;

4.2.1.3.9. A plataforma de gerenciamento deve ser capaz de realizar o backup das configurações dos sensores e da própria plataforma de gerencia, quando necessário ela deve ser capaz de reverter os sensores/solução de gerência com base no backup realizado;

4.2.1.3.10. A plataforma de gerenciamento deve ser capaz de gerenciar o ciclo de vida completo de um evento, a partir da notificação inicial, até quaisquer atividades de resposta e resolução que possam ser necessárias;

4.2.1.3.11. A plataforma de gerenciamento deve possibilitar a edição por completo da regra de detecção correspondente a cada incidente detectado, sejam aquelas criadas pelo usuário ou aquelas fornecidas pelo fabricante;

4.2.1.3.12. A plataforma de gerenciamento deve suportar múltiplas opções de resposta automaticamente às ameaças detectadas;

4.2.1.3.13. A plataforma de gerencia deve ser capaz de habilitar ou desabilitar regras de IDS / IPS existente nos sensores de forma automática a partir da análise de um evento detectado sem a intervenção humana;

4.2.1.3.14. Deverá identificar aplicações conhecidas em portas não-padrão;

4.2.1.3.15. A plataforma de gerenciamento deverá possuir relatórios pré-definidos, possibilitando alterá-los conforme a necessidade do administrador do equipamento ou criar novos de acordo com a demanda;

4.2.1.3.16. A plataforma de gerenciamento deve ser capaz de monitorar e enviar alertas após um limite preestabelecido do uso dos recursos físicos do equipamento, tais como, memória, CPU e disco, além de identificar se o sensor está ativo ou inativo (heartbeat);

4.2.1.3.17. A plataforma de gerencia deve possuir scanner de vulnerabilidade proprietário ou prover integração nativa com scanner de mercado ou open source;

4.2.1.3.18. A plataforma de gerência deve permitir a inclusão de informações oriundas de ferramentas de varredura externas;

4.2.1.3.19. A plataforma de gerenciamento deve ser capaz de ser configurada em alta disponibilidade;

4.2.1.3.20. Permitir atribuir nomes a critério da Contratante para cada interface ou par monitorado;

4.2.1.3.21. Permitir a criação de políticas (conjunto de regras) de monitoração a critério da Contratante;

4.2.1.3.22. Permitir a nomenclatura de políticas de monitoração, a critério da Contratante;

4.2.1.3.23. Deve realizar as seguintes ações em resposta à inspeção de tráfego:

4.2.1.3.23.1. Bloquear;

4.2.1.3.23.2. Bloquear + Notificar;

4.2.1.3.23.3. Bloquear + Notificar + Captura do ataque;

4.2.1.3.23.4. Bloquear + Notificar + TCP Reset;

4.2.1.3.23.5. Permitir + Notificar;

4.2.1.3.23.6. Permitir + Notificar + Captura do ataque.

4.2.1.3.24. Deve permitir criar regras de restrições para endereços IP cujo tráfego será inspecionado;

4.2.1.3.25. Deve possuir classificação de filtros através de categorias;

4.2.1.3.26. Não possuir limitação de usuários simultâneos para filtragem e funcionalidades de IPS;

4.2.1.3.27. Prover estatística de pacotes descartados;

4.2.1.3.28. Permitir a configuração remota dos segmentos e suas respectivas portas de inspeção;

4.2.1.3.29. Deve ser capaz de realizar notificações de eventos de segurança através de e-mail, traps snmp, syslog e scripts;

4.2.1.3.30. Permitir que se descubra a ameaça quando elas ocorrerem, alertar e determinar o impacto e severidade;

4.2.1.3.31. Possuir gerência em tempo real da rede;

4.2.1.3.32. Deve permitir que sejam configurados pelo menos 3 perfis de acesso ao equipamento:

4.2.1.3.32.1. Operador: Acesso básico para visualização do sistema;

4.2.1.3.32.2. Administrador: Acesso avançado para monitorar e gerenciar as funções do sistema;

4.2.1.3.32.3. Super-Usuário: Acesso completo para monitorar e gerenciar as funções do sistema.

4.2.1.3.33. Deve permitir a segregação de tarefas administrativas de acordo com o perfil de usuário;

4.2.1.3.34. Implementar a sincronização entre os equipamentos redundantes, assegurando que não haverá “downtime” em caso de falha de uma das unidades;

4.2.1.3.35. Suportar os protocolos TACACS+ e ou RADIUS e ou LDAP e ou AD de forma a implementar a arquitetura de AAA (Authentication, Authorization and Accounting);

4.2.1.3.36. Suportar o protocolo NTP para sincronização de hora da solução, principalmente para o registro de eventos;

4.2.1.3.37. Deve possuir capacidade de armazenamento de logs de auditoria, para registro de todas as atividades dos usuários da ferramenta;

4.2.1.3.38. Suportar o gerenciamento através de interface de linha de comando (CLI) da solução, através de porta console e por SSH versão 2;

4.2.1.3.39. Suportar o registro de toda a comunicação realizada através da solução e de todas as tentativas de abertura de conexões ou sessões que forem recusadas pelo mesmo;

4.2.1.3.40. Deve permitir identificar sessões de gerenciamento ativas;

4.2.1.3.41. Suportar a exportação em tempo real de logs através de syslog em conformidade com o padrão IETF RFC 5424;

4.2.1.3.42. Deve suportar interface de gerenciamento baseado em protocolo http seguro (https), acessível por navegador de Internet como MS Internet Explorer, Mozilla Firefox, entre outros ou operar em modo cliente-servidor e vir acompanhado de cliente gráfico (GUI), compatível com os sistemas operacionais Windows XP, Windows 7, Windows 2003 server, Windows 2008 e Linux;

4.2.1.3.43. Não efetuar o download de regras e assinaturas de ataques da internet diretamente ao cluster de IPS;

4.2.1.3.44. A comunicação entre os sensores e o appliance de gerenciamento deverá ser criptografada;

4.2.1.3.45. A console gráfica deve notificar a disponibilidade de novas versões do software de gerenciamento, realizar o download e instalação do produto;

4.2.1.3.46. Deve possuir ferramenta de administração do banco de dados capaz de realizar as seguintes tarefas: backup do banco de dados (agendado ou sob demanda), restore do banco de dados e limpeza do banco de dados;

4.2.1.3.47. Deve ser capaz de realizar o downgrade (rollback) do sistema de gerenciamento para versões anteriores;

4.2.1.3.48. Suportar o gerenciamento por SNMPv2 e SNMPv3, a critério da Contratante;

4.2.1.3.49. Gerar relatórios em formato PDF, HTML e CSV;

4.2.1.3.50. Manter estatísticas dos ataques identificados;

4.2.1.3.51. Alertar o mau funcionamento dos sensores;

4.2.1.3.52. Deve possuir mecanismo de substituição de sensores, transferindo-se configurações e dados históricos (arquivo de backup) de um equipamento para outro;

4.2.1.3.53. Os equipamentos deverão ser fornecidos com seu software com licença irrestrita, em sua versão mais atual e completa. O fornecimento deverá incluir todas as licenças de software necessárias para a implementação de todas as funcionalidades disponibilizadas pelo fabricante para os equipamentos fornecidos.

4.2.1.4. Licenciamento de Hosts

4.2.1.4.1. Caso necessário a solução deverá contar com licenças para scan passivo em tempo real para armazenar informações sobre inventário de rede e usuários para pelo menos 1.000 hosts possibilitando obter informações do tipo:

4.2.1.4.1.1. Sistema operacional utilizado;

4.2.1.4.1.2. Vulnerabilidades existentes;

4.2.1.4.1.3. Endereçamento IP;

4.2.1.4.1.4. Protocolos utilizados.

4.2.2. Sensores de Prevenção de Intrusão

4.2.2.1. Características Mínimas

4.2.2.1.1. Possuir no mínimo capacidade de inspeção de tráfego de 10 Gbps em um único equipamento.

4.2.2.1.2. Possuir latência de rede máxima de 150 microssegundos;

4.2.2.1.3. Possuir mecanismo de acionamento interno automático (bypass) para o caso de falhas no equipamento.

4.2.2.1.4. Gabinetes para instalação em rack padrão 19 polegadas;

4.2.2.1.5. Deve ser acompanhada de todos os cabos e suportes (gavetas e braços) necessários para a instalação do equipamento;

4.2.2.1.6. Deve ser fornecido com fontes internas de alimentação redundante do tipo hot-swap com capacidade para suportar toda a solução, sem perda de funcionalidade ou capacidade, no caso de falha das fontes principais ou falta de energia;

4.2.2.1.7. Deve possuir fonte de alimentação com chaveamento automático 110/220V – 50/60Hz;

4.2.2.1.8. Possuir no mínimo dispositivo de armazenamento em disco magnético, no mínimo de 1 TB ou qualquer dispositivo de armazenamento interno com possibilidade de replicar os registros de forma automática e em tempo real dos Logs para um SGDB externo;

4.2.2.1.9. Para atendimento das funcionalidades relacionadas à análise de fluxo, admite-se o acréscimo de um segundo dispositivo igualmente redundante.

4.2.2.2. Interfaces

4.2.2.2.1. Possuir no mínimo 4 interfaces de monitoramento 1000BASE-T, e 8 interfaces 10GBASE-SR;

4.2.2.2.2. A porta de gerência deve ser fisicamente isolada das portas de monitoração, não sendo aceitas portas comuns às duas funções;

4.2.2.2.3. Deve possuir 1 porta serial (RS232) ou RJ-45 para gerenciamento.

4.2.2.3. Funcionalidades Gerais

4.2.2.3.1. Solução de prevenção de intrusão de rede (IPS) de alto desempenho do tipo cluster com hardware dedicado;

4.2.2.3.2. Deve contemplar os equipamentos de hardware e software necessários para o seu funcionamento autônomo, de maneira a atender todas as especificações constantes neste documento;

4.2.2.3.3. Deve permitir operar em alta disponibilidade com manutenção e compartilhamento do estado de sessão TCP dentro do mesmo par de nós do cluster, através de interface(s) de alta disponibilidade;

4.2.2.3.4. Deve implantar alta disponibilidade, com a utilização de uma segunda unidade (secundária) idêntica em standby (ativa/standby) ou de forma ativa/ativa, a critério da Contratante;

4.2.2.3.5. Quando operando em uma configuração de alta disponibilidade, deve ser capaz de manter sincronismos dos fluxos bloqueados;

4.2.2.3.6. Tanto na implantação ativa/ativa ou ativa/standby, não poderá haver perda de nenhuma das conexões ativas (stateful failover) e a transição destas conexões entre as duas unidades deve ser completamente transparente para o usuário final, inclusive em redes de roteamento / tráfego simétrico e assimétrico;

4.2.2.3.7. Todas as interfaces de detecção/prevenção de intrusos, quando configuradas em linha (par de interface), deverão oferecer suporte a bypass automático ou block-all automático, em caso de falha do sensor ou necessidade, a critério da Contratante;

4.2.2.3.8. Suportar IPv6 nativo e tráfego de IPv6 tunelado em pacotes IPv4;

4.2.2.3.9. Possuir suporte a IPv4 e IPv6 nativo, inclusive na detecção e prevenção de ataques;

4.2.2.3.10. Funcionar em modo passivo ou ativo simultaneamente em portas distintas;

4.2.2.3.11. Deve possuir capacidade de no mínimo 2.000.000 (dois milhões) conexões simultâneas;

4.2.2.3.12. Deve possuir capacidade de estabelecer no mínimo 100.000 (cem mil) conexões por segundo;

4.2.2.3.13. A empresa vencedora do certame deve possuir no mínimo dois técnicos certificados na solução ofertada;

4.2.2.3.14. Permitir atribuir nomes a critério da Contratante para cada interface ou par monitorado;

4.2.2.3.15. Suportar a exportação em tempo real de logs através de syslog em conformidade com o padrão IETF RFC 5424;

4.2.2.3.16. Os nós do cluster deverão funcionar independentes de vínculo/conexão com o fornecedor/fabricante;

4.2.2.3.17. Não deve ser necessária nenhuma modificação de arquitetura ou instalação de software em ativos da Contratante, exceto caso a Contratante julgue necessário;

4.2.2.3.18. Todas as licenças que compõem o item adquirida pela Contratante deverão permitir a plena continuidade de utilização e operação mesmo após o término do contrato, de forma perpétua;

4.2.2.3.19. Caso algum dos componentes da solução esteja limitado à utilização de senhas (chaves) de ativação / funcionamento, a contratada deverá fornecer, junto com a entrega da solução, uma senha (chave) ou conjunto de senhas (chaves) de utilização sem vencimento (perpétua), incondicionada à renovação do contrato.

4.2.2.4. Funcionalidades

4.2.2.4.1. Operar em camada 2 OSI (Layer2), span-mode ou bridge-mode (segmento), sendo vedada a alocação de IP válido nas interfaces física de rede;

4.2.2.4.2. Possuir mecanismo de inspeção em nível de aplicação: Inspeciona as camadas 2 a 7 do modelo OSI;

4.2.2.4.3. Possibilitar agregar pares de interfaces para detecção / prevenção em modo em linha (in-line) denominado segmento;

4.2.2.4.4. Deve possuir capacidade de criar regras independentes para cada segmento monitorado ou grupos de segmentos;

4.2.2.4.5. Possibilitar agregar pares de segmentos entre equipamentos distintos do cluster (para redes assimétricas e alta disponibilidade);

4.2.2.4.6. Possibilitar a implantação com as seguintes formas de detecção / bloqueio de tráfego:

4.2.2.4.6.1. Em linha com bloqueio ativo;

4.2.2.4.6.2. Em linha sem bloqueio ativo com emissão de alertas;

4.2.2.4.6.3. Em linha com bloqueio ativo e sem bloqueio ativo, customizado por regra de detecção.

4.2.2.4.7. Possuir detecção e prevenção do tipo stateful, inclusive em interfaces agregadas entre nós distintos do cluster;

4.2.2.4.8. Deverá construir registro dos fluxos de dados relativos a cada sessão iniciada, armazenando para cada uma destas sessões informações tais como: endereços de origem e destino dos pacotes, portas TCP e UDP de origem e destino, bem como os números de sequência dos pacotes TCP e UDP, status dos flags “ACK”, “SYN” e “FIN”, facilitando assim a varredura de todo tráfego que passa pelo IPS e a inspeção com as assinaturas de ataques que dependem de flags TCP de conexão iniciada (stateful);

4.2.2.4.9. Possuir detecção e prevenção não orientada a conexão (stateless);

4.2.2.4.10. Deve possuir filtros para proteção de aplicações, proteção da infraestrutura e proteção da performance.

4.2.2.4.11. Possuir detecção e prevenção para os protocolos TCP, UDP e ICMP, sobre IP;

4.2.2.4.12. Possuir técnica de detecção e prevenção contra evasão por ofuscação de URL;

4.2.2.4.13. Possuir técnica de detecção e prevenção contra evasão por fragmentação RPC;

4.2.2.4.14. Possuir técnica de detecção e prevenção contra evasão FTP / Telnet;

4.2.2.4.15. Possuir técnica de detecção e prevenção contra evasão por segmentação TCP;

4.2.2.4.16. Proteção positiva e segura contra ataques, como:

4.2.2.4.16.1. Ataques de Worm, Trojan, Backdoors, Portscans, IP Spoofing, DoS, DDoS e Spywares.

4.2.2.4.16.2. Ataques a comunicações VoIP;

4.2.2.4.16.3. Ataques e utilização de tecnologia P2P;

4.2.2.4.16.4. Ataques de estouro de pilha (buffer overflow);

4.2.2.4.16.5. Ataques do tipo dia-zero (zero-day);

4.2.2.4.16.6. Tráfego mal formado;

4.2.2.4.16.7. Cabeçalhos inválidos de protocolo.

4.2.2.4.17. Deve possuir filtros de normalização de tráfego, que bloqueiem tráfego malicioso ou que apresente comportamento anormal. Deve possuir a capacidade de bloquear os seguintes tipos distintos:

4.2.2.4.17.1. IP Header Incomplete;

4.2.2.4.17.2. IP Fragment Invalid;

4.2.2.4.17.3. IP Fragment Out of Range;

4.2.2.4.17.4. IP Duplicate Fragment;

4.2.2.4.17.5. IP Length Invalid;

4.2.2.4.17.6. IP Fragment Total Length Mismatch;

4.2.2.4.17.7. IP Fragment Overlap;

4.2.2.4.17.8. IP Fragment Bad MF Bits;

4.2.2.4.17.9. IP Fragment Expired;

4.2.2.4.17.10. TCP Segment Overlap With Different Data;

4.2.2.4.17.11. TCP Header Length Invalid;

4.2.2.4.17.12. TCP Flags Invalid;

4.2.2.4.17.13. TCP Header Incomplete;

4.2.2.4.17.14. TCP Length Invalid;

4.2.2.4.17.15. TCP Reserved Flags Invalid;

4.2.2.4.17.16. ICMP Header Incomplete;

4.2.2.4.17.17. UDP Header Incomplete;

4.2.2.4.17.18. UDP Length Invalid;

4.2.2.4.17.19. Ethernet Header Incomplete;

4.2.2.4.17.20. ARP Address Invalid;

4.2.2.4.17.21. ARP Header Incomplete;

4.2.2.4.17.22. ARP Length Invalid.

4.2.2.4.18. Deve possibilitar identificação de todos os fluxos de dados bloqueados, consulta a um determinado endereço IP bloqueado, desbloqueio de um único IP ou desbloqueio de todos os endereços IP;

4.2.2.4.19. Deve possibilitar armazenamento dos arquivos de configuração diretamente no sensor, permitindo rolagem de retorno para a configuração prévia quando for necessário;

4.2.2.4.20. Possuir técnica de detecção e prevenção contra anomalias de protocolos de aplicação (HTTP, SMTP, NetBIOS, HTTPS, FTP, DNS, SMB, RPC, SSH e Telnet);

4.2.2.4.21. Implementar proteção contra ataques DDoS;

4.2.2.4.22. Permitir à Contratante definir o sentido de inspeção (“inbound”, “outbound” ou “inbound e outbound”) do tráfego por grupo de sensor/par de interface de monitoração/prevenção;

4.2.2.4.23. Possuir no mínimo 3.000 regras nativas com assinaturas de detecção;

4.2.2.4.24. Suportar o gerenciamento através de interface de linha de comando (CLI) da solução, através de porta console e por SSH versão 2;

4.2.2.4.25. Possibilitar a criação de assinaturas customizadas com o uso de expressões regulares;

4.2.2.4.26. Deve possuir capacidade de armazenamento de logs do sistema, para identificação de funcionamento dos principais componentes de gerenciamento e armazenar logs de auditoria, para registro de todas as atividades dos usuários da ferramenta;

4.2.2.4.27. Suportar o gerenciamento por SNMPv2 e SNMPv3, a critério da Contratante;

4.2.2.4.28. Permitir a inclusão de informações oriundas de ferramentas de varredura externa;

4.2.2.4.29. Deverá suportar a identificação de anomalia de rede observando o tráfego ou informações do flow de ativos da rede de forma nativa;

4.2.2.4.30. A solução deve fornecer uma completa análise do comportamento da rede a fim de detectar ameaças com origem na rede interna. Isto inclui a capacidade de estabelecer padrões "normais" de tráfego através de técnicas de análise de fluxo e a capacidade de detectar desvios dos padrões considerados normais;

4.2.2.4.31. A solução deve ser capaz de passivamente coletar informações sobre hosts da rede e suas atividades, tais como sistema operacional, serviços, portas em uso, aplicativos e vulnerabilidades;

4.2.2.4.32. É necessário armazenar informações de 1.000 hosts da rede;

4.2.2.4.33. A solução deve ser capaz de detectar passivamente serviços pré-definidos, tais como FTP, HTTP, HTTPS, POP3, Telnet, SSH, etc, bem como serviços personalizados;

4.2.2.4.34. A solução deve ser capaz de armazenar atributos de hosts definidos pelo usuário, assim como a criticidade dos hosts ou informações de administração;

4.2.2.4.35. A solução deve permitir criar e implementar políticas de segurança, identificar todos os hosts que apresentam um determinado atributo ou condição de não conformidade e alertar sobre as violações das mesmas;

4.2.2.4.36. A solução deverá gerar alertas automaticamente priorizados de acordo com a criticidade do incidente;

4.2.2.4.37. Possuir ferramenta para medir o tempo total gasto para processar pacotes e capacidade de paralisar a inspeção de pacotes, caso o tempo de processamento seja superior ao limite configurado;

4.2.2.4.38. Possuir mecanismos de redução de falsos-positivos associados com detecção de assinatura procurando por um ataque somente quando ocorrer um tráfego relevante ou através de mecanismo de correlação;

4.2.2.4.39. O fornecedor da solução de IPS deve possuir time de pesquisa especializado e dedicado a capturar vulnerabilidades e criar novas regras;

4.2.2.5. A solução deve possuir garantia, licenciamento e suporte por no mínimo 60 (sessenta) meses contados a partir do recebimento definitivo para a solução adquirida fruto deste certame.

4.2.2.5.1. Durante todo o prazo mencionado, a solução deverá contar com atualização de versão de software, patches, assinaturas, base de aplicações e outras melhorias inerentes à solução contratada.

4.3. Serviços técnicos em Segurança Corporativa e Controles Internos; Serviços de operação de recursos de Segurança Corporativa e monitoramento especializado; Serviços de análise em Segurança Corporativa; Outros serviços operacionais.

O detalhamento das atividades a serem desenvolvidas, bem como o perfil dos profissionais que deverão ser alocados em cada um dos itens de serviço estão descritos a seguir

4.3.1. Serviços técnicos em Segurança Corporativa e Controles Internos.

4.3.1.1. Desenvolvimento e suporte em ferramentas tecnológicas;

4.3.1.2. Apoio na elaboração de alertas, avisos e instruções, direcionadas ao usuário, para utilização das ferramentas tecnológicas;

4.3.1.3. Triagem dos incidentes, com respectiva categorização, priorização e direcionamento correto ao tratamento;

4.3.1.4. Tratamento do incidente, envolvendo coleta de evidências necessárias, identificação da origem, identificação da causa e análise de artefatos;

4.3.1.5. Acionamento dos responsáveis, em casos de incidentes, envolvendo restauração e recuperação dos recursos atingidos;

4.3.1.6. Apoio na elaboração de notificações aos usuários, como resposta a incidentes cadastrados, dúvidas ou outras solicitações;

4.3.1.7. Auxiliar na prospecção de soluções de segurança;

4.3.1.8. Suporte na conformidade de recursos de Segurança Corporativa;

4.3.1.9. Suporte aos usuários internos a Recursos de Segurança Corporativa;

4.3.1.10. Categorizar a informação sobre incidentes e problemas nos recursos de segurança;

4.3.1.11. Fornecer informações gerenciais para o Ambiente de Segurança Corporativa acerca dos recursos de segurança.

4.3.2. Serviços de operação de recursos de Segurança Corporativa e monitoramento especializado.

4.3.2.1. Monitoramento da ocorrência de incidentes de segurança, por meio da análise de logs de dispositivos e da utilização de ferramentas de segurança e auditoria (firewall / IPS / antimalware);

4.3.2.2. Monitoramento da infraestrutura de segurança para avaliar a aderência das configurações às Políticas, Normas ou Diretrizes de segurança definidas pela Etice;

4.3.2.3. Levantamento de vulnerabilidades de hardware e software, realizando avaliação da natureza, mecanismos e efeitos para o desenvolvimento de estratégias de detecção e reparação;

4.3.2.4. Envio de alertas de segurança para os gestores dos recursos de infraestrutura, com vistas a proceder aos ajustes em configurações de segurança dos dispositivos;

4.3.2.5. Triagem e suporte no tratamento de incidentes de segurança, envolvendo coleta de evidências necessárias, identificação da origem, identificação da causa e análise de artefatos;

4.3.2.6. Acionamento dos responsáveis pela solução de incidentes, envolvendo restauração e recuperação dos recursos atingidos;

4.3.2.7. Captura de logs e coleta de informações, para viabilização de tratamento de artefatos maliciosos, para que seja desenvolvida, ou sugerida, estratégia de detecção, remoção e defesa;

4.3.2.8. Monitoramento e suporte na análise do uso da Internet Corporativa para garantir aplicabilidade das Normas e Diretrizes da Política de Acesso Internet;

4.3.2.9. Captura de logs e coleta de informações para subsídio da análise de servidores, estações, software básico e aplicativos;

4.3.2.10. Coleta de dados para viabilizar o acompanhamento da conformidade dos recursos computacionais, em conformidade com as recomendações da Política de Segurança estabelecidas pela Etice, incluindo: incidência de malwares, incidência de softwares não homologados para uso corporativo, normalidade de serviços de prevenção a incidentes de Segurança Corporativa (solução antimalware, antispam, filtro de conteúdo, dentre outros);

4.3.2.11. Monitoramento de softwares não homologados, para garantir aplicabilidade das Normas e Diretrizes da Política de Segurança.

4.3.2.12. Monitoramento de acessos indevidos à Internet, para garantir aplicabilidade das Normas e Diretrizes da Política de Segurança Corporativa;

4.3.2.13. Monitoramento de uso indevido do Correio Eletrônico Corporativo, para garantir aplicabilidade das Normas e Diretrizes da Política de Segurança Corporativa.

4.3.2.14. Análise de alertas da ferramenta IPS com vista a identificar e iniciar procedimentos de respostas a incidentes de Segurança Corporativa.

4.3.3. Serviços de análise em Segurança Corporativa.

4.3.3.1. Apoio na prospecção de novos conhecimentos (ameaças, ataques, vulnerabilidades, legislação relacionada a crimes digitais, tecnologias emergentes e tendências) relativos à Segurança em Arquitetura e Infraestrutura de Rede;

4.3.3.2. Apoio na prospecção de novas ferramentas de Segurança em Arquitetura e Infraestrutura de Rede;

4.3.3.3. Coleta de dados e levantamentos estatísticos para viabilizar identificação de futuras ameaças;

4.3.3.4. Suporte no uso de soluções de segurança implantadas pelo Ambiente de Segurança Corporativa;

4.3.3.5. Captura de logs e levantamentos estatísticos para viabilização de análise periódica e detalhada da configuração de servidores, estações, dispositivos da rede, software básico e aplicativos, com a finalidade de prevenir incidentes futuros;

4.3.3.6. Levantamentos estatísticos para acompanhamento da conformidade dos recursos computacionais com as recomendações da política de Segurança Corporativa estabelecidas pela Etice;

4.3.3.7. Apoio na identificação de vulnerabilidades em servidores, estações, dispositivos de rede e de segurança perimetral e de sistemas de detecção de intrusão;

4.3.3.8. Apoio na análise de incidentes envolvendo ativos computacionais como: Firewall, Proxies, IDS/IPS, VPN, Antimalware e AntiSpam e AD – Active Directory do Windows;

4.3.3.9. Suporte na implantação e manutenção de soluções de segurança perimetral – Firewall, Prevenção a Intrusão, VPN – comunicação segura, Antimalware e AntiSpam;

4.3.3.10. Auxílio na definição de controles e padrões de segurança de configuração de artefatos de rede para garantir aplicabilidade das normas e diretrizes da Política de Segurança Corporativa;

4.3.3.11. Apoio na elaboração de padrões mínimos de segurança para sistemas operacionais – baseline;

4.3.3.12. Suporte de Segurança às atividades de planejamento, implantação e gerenciamento de infraestrutura de rede corporativa abrangendo arquitetura e topologia;

4.3.3.13. Auxílio nas definições de requisitos de segurança relacionadas com implantação de soluções de segurança de redes;

4.3.3.14. Coleta de informações para subsidiar elaboração de avisos, alertas, artigos técnicos, divulgação de vulnerabilidades e orientações de segurança para usuários da rede corporativa;

4.3.3.15. Captura de logs e coleta de Informações para apoio na realização de Análise Forense de eventos de Segurança;

4.3.3.16. Coleta de informações para viabilizar análise de desempenho dos sistemas relacionados com Segurança de Redes;

4.3.3.17. Apoio no processo de implantação de controles relacionados com Segurança em Arquitetura e Infraestrutura de Rede, verificação de conformidade e melhoria contínua para segurança dos ativos da organização, em conformidade com normas NBR ISO/IEC 27001 - Sistemas de gestão de Segurança Corporativa, NBR ISO/IEC 27002 – Código de Prática para a Gestão de Segurança Corporativa;

4.3.3.18. Coleta de informações para viabilizar análise de coerência de ações e de procedimentos internos, objetivando minimizar riscos e garantir o cumprimento dos normativos de Segurança de Redes;

4.3.3.19. Coleta de informações para viabilizar elaboração de informações de Segurança Corporativa a serem encaminhadas a diversos públicos internos e externos, a exemplo de Auditores Internos e Órgãos Reguladores;

4.3.3.20. Apoio na prospecção de novos conhecimentos (ameaças, ataques, vulnerabilidades, legislação relacionada a crimes digitais, tecnologias emergentes e tendências) relativos à Segurança em Internet.;

4.3.3.21. Apoio na prospecção de novas ferramentas de Segurança em Internet;

4.3.3.22. Coleta de dados e levantamentos estatísticos para viabilizar identificação de futuras ameaças de Segurança em Internet;

4.3.3.23. Suporte no uso de soluções de Segurança em Internet;

4.3.3.24. Suporte de segurança às atividades de planejamento, implantação e gerenciamento de Controle de Acesso à Internet;

4.3.3.25. Auxílio na definição de Políticas, Controles e Padrões de Segurança em Internet;

4.3.3.26. Captura de logs e coleta de Informações para garantir aplicabilidade das normas e diretrizes da Política de Segurança Corporativa;

4.3.3.27. Captura de logs e coleta de Informações para viabilização da análise de incidentes envolvendo ativos computacionais como: Controle de Acesso e Conteúdo à Internet, Serviço de Proxy, Firewall de Aplicação;

4.3.3.28. Captura de logs e coleta de Informações para apoio na realização de Análise Forense de eventos de Segurança;

4.3.3.29. Auxílio nas definições de requisitos de segurança relacionadas com implantação de soluções de segurança em Internet;

4.3.3.30. Coleta de informações para subsidiar elaboração de avisos, alertas, artigos técnicos, divulgação de vulnerabilidades e orientações de segurança para usuários da rede corporativa;

4.3.3.31. Coleta de informações para viabilizar análise de desempenho dos sistemas relacionados com Segurança em Internet;

4.3.3.32. Apoio no processo de implantação de controles relacionados com Segurança em Internet, verificação de conformidade e melhoria contínua para segurança dos ativos da organização, em conformidade com normas NBR ISO/IEC 27001 - Sistemas de gestão de Segurança Corporativa, NBR ISO/IEC 27002 – Código de Prática para a Gestão de Segurança Corporativa;

4.3.3.33. Coleta de informações para análise de coerência de ações e de procedimentos internos, objetivando minimizar riscos e garantir o cumprimento dos normativos de Segurança em Internet;

4.3.3.34. Coleta de informações para viabilizar elaboração de informações de Segurança Corporativa a serem encaminhadas a diversos públicos internos e externos, a exemplo de Auditores Internos e Órgãos Reguladores.

4.3.4. Outros Serviços Operacionais

4.3.4.1. Segurança

4.3.4.1.1. Gerenciamento de políticas de acesso de Firewall;

4.3.4.1.2. Gerenciamento de políticas de segurança de IPS;

4.3.4.1.3. Gerenciamento de políticas de acesso HTTP;

4.3.4.1.4. Gerenciamento de políticas de acesso a redes privadas (VPN).

4.3.4.2. Rede (segurança)

4.3.4.2.1. Troubleshooting de rede TCP/IPv4 e IPv6;

4.3.4.2.2. Configuração e gerenciamento de redes SAN;

4.3.4.2.3. Análise de tráfego avançada.

4.3.4.3. Rede (conectividade)

Rede (conectividade) engloba: PTT, links de Internet (Intelig, L3 e futuramente Oi), DWDM, Rádios WiMax e ponto-a-ponto, Wi-FI, GPON, FRAME-RELAY, MPLS, IPS, Firewall de evento, monitoramento, autenticação, servidor de log, faturamento, hands-on para servidores do NIC.Br que contém o SIMET, IX.ce, INMETRO que tem os servidores da EAQ instalados com o PTT, DNS raiz .BR anycast E e L, switches de borda. Diagnóstico de rompimento de fibra englobando CDC/RNP/Telebras/consórcio BWM, transporte de dados para as prefeituras (interior)/RNP/TRE/SERPRO.

4.3.4.3.1. Detecção de falhas e apoio na resolução de problemas;

4.3.4.3.2. Análise periódica através das ferramentas disponibilizadas pela ETICE sugerindo correções e melhorias;

4.3.4.3.3. Geração de relatório para faturamento de link a partir da ferramenta disponibilizada pela ETICE;

4.3.4.3.4. Apoio técnico nos casos de contestação sobre faturamento;

4.3.4.3.5. Aprovisionamento de faixas Ipv4 / Ipv6 conforme definição de blocos fornecidos pela ETICE;

4.3.4.3.6. Configuração de equipamentos de rede de acesso e backbone conforme solicitação da ETICE;

4.3.4.3.7. Auxílio na instalação física e lógica dos equipamentos de rede;

4.3.4.3.8. Auxílio na instalação de módulos adicionais quando solicitados pela ETICE;

4.3.4.3.9. Apoio na configuração dos equipamentos de videoconferência;

4.3.4.3.10. Sugestão de medidas de restrição / segurança para acesso à rede;

4.3.4.3.11. Configuração do equipamento de backbone para comunicação entre as redes legadas (RIGAV/FRAME-RELAY) e MPLS com o CDC;

4.3.4.3.12. Implementação de controle de banda à clientes quando solicitado pela ETICE;

4.3.4.3.13. Apoio no monitoramento da rede;

4.3.4.3.14. Auxílio na montagem e configuração de equipamentos na realização de eventos sob responsabilidade da ETICE;

4.3.4.3.15. Apoio na detecção de rompimento de fibra;

4.3.4.3.16. Sob solicitação da ETICE realizar a prospecção de solução e/ou resolução de problemas de rede* em outros clientes

4.3.4.3.17. Troubleshooting de rede TCP/IPv4 e IPv6;

4.3.4.3.18. Configuração e gerenciamento de redes SAN;

4.3.4.3.19. Análise de tráfego avançada.

4.3.4.4. Sistemas

4.3.4.4.1. Gerenciamento de sistemas Unix/Linux;

4.3.4.4.2. Gerenciamento de sistemas Windows;

4.3.4.4.3. Gerenciamento de domínios Samba e LDAP;

4.3.4.4.4. Gerenciamento de ativos de rede por plataforma de monitoramento de rede;

4.3.4.4.5. Gerenciamento de infraestrutura de resolução de nomes (DNS);

4.3.4.4.6. Gerenciamento de servidores HTTP;

4.3.4.4.7. Gerenciadores de servidores de tempo (NTP);

4.3.4.4.8. Gerenciamento de plataformas de mensagens (SMTP, POP, IMAP, XMPP);

4.3.4.4.9. Gerenciamento de plataformas de aplicações JAVA;

4.3.4.4.10. Gerenciamento de plataformas de aplicações PHP;

4.3.4.4.11. Gerenciamento de sistemas de orquestração de configuração de servidores.

4.3.4.4.12. Configuração de servidores e serviços tais como: Cacti,Tacacs, PADTEC, IMC, RADWIN, ALVARION, host srv-management, softrouter VyOS, entre outros.

4.3.4.5. Infraestrutura

4.3.4.5.1. Gerenciamento de unidades de armazenamento (Storage);

4.3.4.5.2. Gerenciamento de soluções de Virtualização;

4.3.4.5.3. Gerenciamento de soluções de computação distribuída de alta disponibilidade (clusters);

4.3.4.5.4. Gerenciamento de soluções de replicação de áreas de armazenamento distribuídas e em alta disponibilidade.

4.3.5. Local de Funcionamento

Os serviços serão prestados na Etice, situada na Av. Pontes Vieira, nº 220, São do Tauape, Fortaleza, Ceará.

Todos os colaboradores das equipes devem estar alocados fisicamente nas dependências da Etice.

É vedada a subcontratação destes serviços, visto que os trabalhos deverão ser desenvolvidos por profissionais alocados na Etice, contratados em regime CLT, pelo CONTRATADO.

4.3.6. Horário de Trabalho

Os serviços técnicos realizados nas instalações da Etice serão executados, em dias úteis, no horário de expediente normal de trabalho da Etice, entre 8h e 17h. As horas de trabalho efetivamente executadas deverão ser registradas diariamente em formulários próprios e apresentadas mensalmente quando da consolidação da medição dos serviços. O registro das horas de trabalho se faz necessário para que a Etice possa avaliar o esforço demandado nas atividades do Contrato e obter a série histórica destes esforços.

Nos casos em que houver necessidade de execução de atividades, fora do horário de expediente normal de trabalho, em finais de semana ou feriados, a execução das respectivas horas somente será permitida se previamente aprovadas pela Etice. A CONTRATADA ficará responsável pelo planejamento dessas atividades, incluindo o regime de sobreaviso.

Para a manutenção dos serviços críticos poderá ser necessário a utilização de serviços especializados, através do mecanismo do sobreaviso, estando sujeitos à realização de atendimentos extraordinários em virtude de alguns serviços serem 24/7 em concordância com o Nível de Acordo de Serviços.

Os Atendimentos Preventivos repercutem não apenas na rápida correção de incidentes em horários extraordinários, mas principalmente evitam o desencadeamento de outros incidentes ou problemas.

Todos esses custos deverão constar na planilha de preço da CONTRATADA.

4.3.7. Recursos Necessários

Toda a infraestrutura de rede e computacional necessária à prestação dos serviços, não citada neste documento, será fornecida pela Etice.

4.3.8. Qualificação Profissional

A empresa deverá apresentar currículos dos técnicos que serão destacados para a execução dos serviços, bem como declarações e atestados comprobatórios da formação e experiência profissional destes, em conformidade com as exigências constantes deste documento. À Etice se reserva o direito de avaliar a adequação dos profissionais apresentados às exigências do Edital, podendo solicitar a substituição daqueles que não atenderem aos referidos requisitos.

Os profissionais indicados deverão estar aptos a executar as atividades descritas neste documento admitindo-se, durante a execução do Contrato, a substituição de técnicos por profissionais de experiência equivalente ou superior, com a anuência formal da Etice.

Para a execução dos serviços previstos neste Anexo, deverão ser alocados profissionais com as competências a serem discriminadas neste item, as quais deverão ser atestadas pelo CONTRATADO, mediante o encaminhamento e apresentação dos seguintes documentos comprobatórios de qualificação para cada profissional a ser alocado aos serviços:

i. cópia autenticada dos diplomas e certificados de conclusão de cursos necessários para comprovação da formação e conhecimentos específicos;

ii. cópia autenticada de certificações profissionais;

iii. currículo do profissional incluindo declaração do CONTRATADO, conforme modelo apresentado no Anexo ___. O currículo deverá ser assinado pelo profissional e representante legal do CONTRATADO;

A alocação de profissionais aos serviços contratados deverá ser previamente aprovada pela Etice após o recebimento e aceitação dos documentos comprobatórios acima descritos, que ficarão sob sua guarda.

O ambiente computacional da Etice é dinâmico, estando sujeito a evoluções e atualizações. Desta forma, será de responsabilidade do CONTRATADO manter sua equipe de profissionais tecnicamente capacitados para a prestação dos serviços contratados, devendo considerar na elaboração de sua proposta os custos para a manutenção dessa capacitação. Os custos com treinamentos de capacitação dos profissionais do CONTRATADO devem estar previstos nos preços propostos para execução dos serviços deste Anexo.

Os profissionais alocados aos serviços deverão possuir, entre si, capacitações diversificadas de forma a desempenhar corretamente os serviços solicitados pela Etice.

As despesas administrativas estarão a cargo do CONTRATADO, que deverá prover o pessoal próprio para o desempenho das atividades.

A política de remuneração dos profissionais alocados à prestação dos serviços é de total responsabilidade do CONTRATADO, devendo ser obedecidos os preceitos legais e os acordos coletivos de trabalho das respectivas entidades sindicais. A política de remuneração deverá levar em consideração os preços praticados no mercado por perfil profissional, bem como responsabilidades atribuídas para realização dos serviços junto à Etice.

Serviços extraordinários poderão ocorrer durante a execução dos serviços e deverão estar previstos no orçamento e planejamento apresentado, bem como as despesas extras por eles demandados, tais como refeições extras e transportes extraordinários.

Os preços propostos para execução dos serviços devem considerar todas as despesas e custos do CONTRATADO tais como mão de obra (incluindo horas-extras e encargos sociais), alimentação, despesas administrativas, impostos, lucros, treinamentos e capacitação dos profissionais, assim como também devem prever os custos necessários para atender a garantia dos serviços executados.

Para as atividades constantes neste documento, os colaboradores que desempenharão os serviços devem ter, no mínimo, as seguintes capacitações a serem comprovadas pela CONTRATADA:

Requisitos Obrigatórios	Comprovação
Nível superior completo, ou em curso, em uma das áreas de eletroeletrônica, mecatrônica, redes, informática, administração.	Certificado de conclusão ou declaração/histórico da Universidade.
Experiência comprovada de, no mínimo, 24 (vinte e quatro) meses na área de Segurança Corporativa.	Carteira profissional ou declaração de empregador que comprove a realização dos serviços conforme a experiência profissional exigida.
Experiência comprovada de, no mínimo, 24 (vinte e quatro) meses em Segurança de Arquitetura e Infraestrutura de Redes, sendo 12 (doze) meses em atividades de análise, implantação e configuração de soluções de Segurança Corporativa.	Carteira profissional ou declaração de empregador que comprove a realização dos serviços conforme a experiência profissional exigida.
Conhecimento de tecnologia de infraestrutura de rede, com experiência comprovada mínima de 24 (vinte e quatro) meses.	Carteira profissional ou declaração de empregador que comprove a realização dos serviços conforme a experiência profissional exigida.
Experiência comprovada em gerência e configuração de ativos Extreme, Datacom, Huawei e HP	Carteira profissional ou declaração de empregador que comprove a realização dos serviços conforme a experiência profissional exigida.
Experiência comprovada em gerência e configuração de tecnologia/equipamentos DWDM	Carteira profissional ou declaração de empregador que comprove a realização dos serviços conforme a experiência profissional exigida.
Experiência comprovada em gerência e configuração de redes sem fio	Carteira profissional ou declaração de empregador que comprove a realização dos serviços conforme a experiência profissional exigida.
Experiência comprovada em gerência e configuração de videoconferência	Carteira profissional ou declaração de empregador que comprove a realização dos serviços conforme a experiência profissional exigida.
Experiência comprovada em gerência e configuração de VoIP	Carteira profissional ou declaração de empregador que comprove a realização dos serviços conforme a experiência profissional exigida.
Experiência comprovada em gerência e configuração de rádios (Radwin, Alvarion, Motorola etc)	Carteira profissional ou declaração de empregador que comprove a realização dos serviços conforme a experiência profissional exigida.
Conhecimento de ferramentas de segurança de rede:	Carteira profissional ou declaração de

Firewall, VPN, IDS/IPS, Proxy, Antimalware, Anti-Spam, com experiência comprovada mínima de 24 (vinte e quatro) meses.	empregador que comprove a realização dos serviços conforme a experiência profissional exigida.
Experiência comprovada de, no mínimo, 24 (vinte e quatro) meses em Segurança Internet, sendo 12 (doze) meses em atividades de análise, implantação e configuração de soluções Internet.	Carteira profissional ou declaração de empregador que comprove a realização dos serviços conforme a experiência profissional exigida.
Conhecimento de ferramentas de segurança de rede: Firewall de aplicação, serviços e protocolos de conexão Internet, com a utilização de técnica de Proxy e filtro de conteúdo WEB com experiência comprovada mínima de 24 (vinte e quatro) meses.	Carteira profissional ou declaração de empregador que comprove a realização dos serviços conforme a experiência profissional exigida.
Proficiência na identificação e avaliação de falhas em softwares	Carteira profissional ou declaração de empregador que comprove a realização dos serviços conforme a experiência profissional exigida.
Proficiência na mitigação de riscos e resposta a incidentes	Carteira profissional ou declaração de empregador que comprove a realização dos serviços conforme a experiência profissional exigida.
Profundo entendimento de comunicações TCP/IP	Carteira profissional ou declaração de empregador que comprove a realização dos serviços conforme a experiência profissional exigida.
Profundo conhecimento em protocolos de rede e roteamento avançado	Carteira profissional ou declaração de empregador que comprove a realização dos serviços conforme a experiência profissional exigida.
Proficiência no desenho de soluções escaláveis, de alta disponibilidade de tolerantes a falhas	Carteira profissional ou declaração de empregador que comprove a realização dos serviços conforme a experiência profissional exigida.
Proficiência em pelo menos 2 linguagens de programação para criação de ferramentas com objetivo de auxiliar nas rotinas diárias ou específicas	Carteira profissional ou declaração de empregador que comprove a realização dos serviços conforme a experiência profissional exigida.
Requisitos Desejáveis	Comprovação
Cursos de aperfeiçoamento na área de Segurança Corporativa, com carga horária mínima de 80 (oitenta) horas.	Certificado(s) do(s) curso(s).
Curso na área de gerência e configuração de storages e redes SAN	Certificado(s) do(s) curso(s).
Conhecimento comprovado na língua inglesa de, no mínimo, 120 (cento e vinte) horas.	Certificado do curso ou histórico escolar com ementa de disciplina que comprove a capacitação
Certificações na área de Tecnologia Corporativa ou Administração de Sistemas – MCP / MCA / MCSP / CISSP.	Credencial da certificação.

Pós-graduação na área de Segurança Corporativa.	Diploma ou certificado de conclusão do curso.
Conhecimento na Norma NBR ISO/IEC 27002 (17799:2005) – Segurança Corporativa	Carteira profissional, certificado de curso ou declaração de empregador que comprove o conhecimento exigido.
Conhecimento na Norma NBR 15999-1: 2007 – Gestão de Continuidade de Negócios.	Carteira profissional, certificado de curso ou declaração de empregador que comprove o conhecimento exigido.
Outras certificações e cursos: RHCE - Red Hat Certified Engineer LPIC - Linux Professional Institute Certified CEH - Certified Ethical Hacker CISSP - Certified Information Security Professional CCNA - Cisco Certified Network Associate	Credencial da certificação.

Excepcionalmente, a critério da CONTRATANTE e no interesse da CONTRATADA em manter o pessoal atualmente contratado, que possua comprovada experiência, que atue em funções chaves que sejam necessários à manutenção do conhecimento e da experiência, poderá ser flexibilizada a exigência de algum requisito de qualificação para execução do serviço, respeitando minimamente o perfil técnico exigido. No entanto, a empresa deverá regularizar a exigência flexibilizada do profissional no prazo de 180 dias.

Muito excepcionalmente, em casos de comprovado notório saber, após criteriosa analise, aceite formal e sendo de interesse da CONTRATANTE, poderá haver exceções quanto a escolaridade mínima exigida nos perfis de especializações, de maneira que esta nunca deverá ser considerada por parte da CONTRATADA como pratica padrão a ser adotada. Podendo haver glosa no contrato em casos de má fé e/ou abusos por parte da CONTRATADA.

À CONTRATANTE reserva-se o direito de realizar auditorias a qualquer tempo para verificar se as competências mínimas solicitadas são atendidas pela CONTRATADA. Desta forma, quando solicitado, a CONTRATADA deverá apresentar os documentos comprobatórios da qualificação dos profissionais alocados na prestação dos serviços, além das certificações requeridas.

4.3.9. Volume Estimado

Caberá à CONTRATADA estimar a quantidade de horas necessárias de forma a manter o SLA exigido, porém, de acordo com o histórico, esse número deve girar em torno de 1.354 (um mil, trezentos e cinquenta e quatro), assim distribuídas:

4.3.9.1. 704 (setecentos e quatro) horas diárias normais

Correspondendo às horas diárias normais de alocação de equipe técnica especializada para Serviços técnicos em Segurança Corporativa e Controles Internos, Serviços de operação de recursos de Segurança Corporativa e monitoramento especializado, e Serviços de análise em Segurança Corporativa.

4.3.9.2. 600 (seiscentas) horas de sobreaviso

Correspondendo às horas de sobreaviso com plantões aos sábados, domingos e feriados (estaduais e municipais), bem como aquele realizado em dias úteis fora do horário núcleo da Contratante, que é das 8h às 17h. O total pode variar de acordo com a quantidade de sábado, domingos e feriados do mês.

4.3.9.3. 50 (cinquenta) horas para atividades sob demanda

Correspondendo às horas adicionais necessárias para suprir as necessidades em situações não previstas, em função de demandas extras, e que não podem ser realizados no horário normal de expediente.

4.3.10. Suporte Técnico de Planejamento e Supervisão de Serviços

O CONTRATADO deverá designar e alocar, desde o primeiro dia do Contrato, o Líder da Equipe de Segurança Corporativa, que será seu Preposto e Responsável Técnico pela realização dos serviços contratados, e desenvolverá no mínimo as seguintes atividades:

O CONTRATADO deverá designar um Preposto para:

a) definir o escopo e metodologia de trabalho para a equipe do CONTRATADO;

b) alocar os profissionais necessários para atendimento dos serviços tempestivamente, para fins de cumprimento dos prazos de início e fim, além do atendimento dos padrões de qualidade previamente estabelecidos;

c) acompanhar e supervisionar o andamento das atividades realizadas pela equipe do CONTRATADO na prestação dos serviços;

d) validar os produtos dos serviços executados pela equipe do CONTRATADO quanto aos requisitos de qualidade estabelecidos para os serviços;

e) elaborar e apresentar as propostas para execução dos serviços solicitados pela Etice;

f) ser ponto focal de contato entre CONTRATADO e a Etice;

g) elaborar e manter atualizados os cronogramas detalhados de atividades da equipe do CONTRATADO;

h) apresentar relatórios mensais de progresso das atividades executadas, organização, planejamento e realização dos serviços e profissionais alocados aos mesmos;

i) adotar providências quanto ao desempenho da equipe, informando à Etice quaisquer irregularidades relacionadas à postura dos Analistas, bem quanto ao cumprimento dos prazos estabelecidos;

j) assegurar que as políticas, normas e procedimentos da Etice sejam respeitados e acatados pelos profissionais do CONTRATADO;

k) informar à Etice sobre qualquer ocorrência ou problema que possa prejudicar o bom andamento na execução dos serviços contratados;

l) realizar outras atividades e apresentar relatórios que se façam necessários ao bom desempenho, transparência na execução e conclusão dos serviços contratados com resultados satisfatórios para a Etice;

m) no início do Contrato, deverá ser realizada uma série de reuniões entre a equipe do CONTRATADO e a da Etice, a fim de se ajustarem as expectativas e esclarecerem determinados pontos que porventura sejam necessários definir as principais premissas e restrições que irão

guiar a execução dos serviços, bem como definir os processos de comunicação, metodologias de trabalho, modelos de documentos, ferramentas de planejamento e registro de atividades, responsabilidades dos membros da equipe e demais requisitos necessários para a execução adequada e eficiente dos serviços contratados, os quais serão registrados em Atas de Reunião;

n) o Suporte Técnico de Planejamento dos serviços contratados contemplarão o gerenciamento dos níveis de serviços acordados, a atualização técnica dos profissionais alocados, a definição conjunta com a Etice dos projetos a serem conduzidos;

o) aprovado o Plano de Trabalho pela Etice e autorizado o início das atividades contratadas, será realizada uma reunião, na primeira semana de cada mês, para avaliação da execução dos serviços, avaliação e revisão do Plano de Trabalho, definição de metas e objetivos dos próximos períodos, bem como a entrega oficial dos produtos definidos para o período. A aceitação desses produtos será pré-requisito para a execução mensal dos serviços realizados pelo CONTRATADO.

ANEXO A
Acordo de Níveis de Serviço

1. **Introdução**

O presente Anexo descreve os requisitos técnicos relacionados à qualidade da prestação dos serviços objeto do Contrato.

O CONTRATADO compromete-se a prestar os serviços descritos no Edital e em seus Anexos, com base nos parâmetros de qualidade descritos neste documento.

O período de observação a ser considerado, para efeito de cálculo dos parâmetros elencados, será de 1 (um) mês, ou seja, será considerado o período compreendido entre o primeiro e o último dia do mês em que o serviço foi prestado à Etice. Caso não sejam atingidos os índices estabelecidos neste Anexo, o CONTRATADO estará sujeito às sanções administrativas previstas no Contrato.

O não atendimento de qualquer um dos requisitos dos níveis de serviço (SLA) descritos neste Anexo implicará na aplicação de multas e demais penalidades previstas, de acordo com a Minuta de Contrato.

2. **Serviços Contemplados no Acordo**

Os serviços a serem contratados estarão de acordo com o descrito no Anexo I – Termo de Referência.

3. **Objetivo**

Garantir a disponibilidade dos serviços prestados

4. **Meta**

O nível mínimo de serviço exigido é 99,9%, e no máximo 15 min por evento. Qualquer indisponibilidade maior que estes limites implicará na aplicação de redutores sobre o valor do faturamento mensal.

5. **Periodicidade**

Mensal

6. **Forma de Cálculo**

Apontar as horas de indisponibilidades do serviço e das equipes técnicas no período, segregadas em horas de indisponibilidade do serviço e de um técnico. Assim como apurar os redutores que serão aplicados ao faturamento mensal de cada item do serviço e aplicá-los sobre o faturamento total, conforme a seguir:

7. **Níveis de Criticidade**

C0 - indisponibilidade total da solução;

C1 - indisponibilidade parcial da solução;

C2 - degradação, solução apresenta algum erro de funcionamento, ou comportamento inesperado

8. **Planilha de Metas**

Indicador	Meta		Frequencia de Medição
DSP	**99,9%**		Mensal
TRO – Horário Comercial	**C1**	**4 horas**	Mensal, por Evento
	C2	**6 horas**	
TRO – Fora do Horário Comercial	**C1**	**6 horas**	Mensal, por Evento
	C2	**8 horas**	
ERG	**Até o 3º dia útil do mês seguinte à medição do serviço**		Mensal, por Evento
TEC	**720 horas**		Mensal
LIE	**<= 15 min**		Por Evento

9. **Métricas de Apuração e Descrição dos Indicadores**

Disponibilidade Total do Serviço – DSP – representa o tempo em que a solução esteve disponível para a CONTRATANTE durante o mês. O Objetivo deste indicador é definir um tempo máximo de tolerância de falha da solução por mês.

Tempo de Recuperação Operacional – TRO – representa o tempo máximo tolerado pela CONTRATANTE para restabelecimento operacional do serviço interrompido.

TEC – Número de horas trabalhadas dos técnicos.

LIE – Limite de tempo máximo para **C0**(indisponibilidade total do serviço) por evento.

TRO = DHR – DHA

onde:

DHR = Data, hora e minuto do encerramento da ocorrência.

DHA = Data, hora e minuto da abertura da ocorrência.

Considerando-se o sistema de monitoramento da ETICE

10. **Entrega de Relatórios – ERG –** O atraso ou retardo na entrega do relatório de acompanhamento de níveis de serviço resulta em impacto no acompanhamento de níveis de serviço resulta em impacto no acompanhamento da prestação dos serviços e sujeita a CONTRATADA à penalidade definida na tabela de descontos.

11. **Tabela de Redutores** – O somatório dos valores resultantes dos redutores aplicados a cada indicador não poderão ultrapassar os 25% do valor total da fatura de serviços.

Os redutores referentes à quebra de indicadores serão realizados mensalmente, sobre a parcela referente ao mês seguinte a medição.

Indicador	Redutores por quebra do indicador
DSP	5% por hora adicional
TRO	0,1% por hora adicional
ERG	0,05% por dia adicional
TEC	0,01% por hora
LIE	0,1% por 3 min adicionais

12. **Multas**

Uma vez apuradas as horas de indisponibilidade no período de medição(HI), será calculado o índice de disponibilidade total dos serviços, sendo exigido o mínimo de 99,9%(noventa e nove por cento) de disponibilidade. Além da redução sobre o faturamento mensal de que trata o subitem anterior, não sendo atingido o percentual mínimo de 99,9% de disponibilidade, incidirá multa, a qual será calculada sobre o valor total da fatura mensal, após a aplicação dos redutores, conforme os níveis de serviço, demonstrado abaixo:

DSPR = DSPP – HI + IDTJ

DSP = DSPR / DISPP

Onde:

HI – Horas de indisponibilidade no mês.

DSPR – Disponibilidade real

IDTJ – Indisponibilidade em virtude de manutenções programadas e paradas acordadas pela ETICE

DSPP – Total de horas previstas mensalmente de disponibilidade.

13. **Tabela de Multas**

Nível de Serviço	Multa
DSP > = 99,9%	Não se Aplica
98,9% <= **DSP** < 99,9%	30% sobre o valor do faturamento mensal
97,9% <= **DSP** < 98,9%	50% sobre o valor do faturamento mensal
93%<= **DSP** < 97,9%	80% sobre o valor do faturamento mensal
DSP < 93,3%	100% sobre o valor do faturamento mensal

14. **Comunicação da Apuração à Contratada**

Mensalmente a Etice comunicará, formalmente, ao CONTRATADO, o valor da redução sobre o faturamento mensal, decorrente da aplicação dos redutores referidos, bem como o índice de disponibilidade total – DSP do período, calculados conforme descrito neste subitem.

ANEXO B

Modelo do Currículo

Currículo de Profissional

1. Identificação do Profissional:

Nome:

CPF:

Data de Nascimento: / / Naturalidade: Naturalidade:

Identidade: Órgão Expedidor: Data Expedição: / /

Nome do Pai:

Nome da Mãe:

Endereço:

Cidade UF:

2. Formação Acadêmica:

Curso: Instituição: Data de Conclusão: / /

(repetir, se necessário)

Pós-Graduação:

(repetir, se necessário)

3. Formação Técnica:

Curso: Instituição: Carga Horária:

(repetir, se necessário)

4. Certificação Profissional:

Certificação: Instituição: Validade: / /

(repetir, se necessário)

5. Experiência Profissional:

Empresa: Período:

Atividades desempenhadas:

(repetir, se necessário)
Declaramos para os devidos fins, que as informações declaradas neste currículo são verdadeiras e seguem em anexo as comprovações devidamente autenticadas.

Local e data

(nome e assinatura do profissional)

(nome e assinatura do requerente legal do CONTRATRADO)