1-NOME DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO

1.1 DESCRIÇÃO DA SOLUÇÃO ESCOLHIDA

Aquisição de 2 (dois) *switches* de camada 7, do tipo *appliance*, com garantia de 3 (três) anos, para otimização de aplicações *web*, balanceamento de aplicações e servidores, segurança e aceleração de aplicações web, acompanhados de todos os softwares, licenças de uso de software, serviços necessários à instalação, configuração, testes, suporte técnico e banco de horas.

Bens Que Compõem a Solução

Todos os elementos, suas especificações e suas respectivas propriedades abaixo relacionadas são requisitos mínimos de atendimento obrigatório para cada switch camada 7 a ser fornecido.

Características de Hardware:1

O equipamento oferecido deverá possuir no mínimo 4 (quatro) portas 10/100/1000Base-T. Não serão aceitas combinações de equipamentos para atingir o número mínimo de portas;

O equipamento deverá possuir no mínimo 8 (oito) slots SFP+ para utilização de portas de 10Gbps em fibra óptica;

O equipamento deverá possuir no mínimo 4 (quatro) portas de 10Gbps SR em fibra óptica disponíveis para uso;

O equipamento oferecido deverá possuir fonte AC com voltagem 110-220 automático;

O equipamento será instalado em rack padrão 19" e deve ser apropriado para estas instalações;

O equipamento deverá possuir fonte de alimentação redundante;

O equipamento oferecido deverá possuir no mínimo 30 Gbps de tráfego em camada 4;

O equipamento oferecido deverá possuir no mínimo 15 Gbps de tráfego de Camada 7;

O equipamento oferecido deverá possuir no mínimo 750.000 e deverá suportar expansão para no mínimo 1,5 Milhões de requisições por segundo na Camada 7;

O equipamento oferecido deverá possuir no mínimo 350.000 e deverá suportar expansão para no mínimo 700.000 conexões por segundo na camada 4;

O equipamento oferecido deverá possuir no mínimo 10.000 e deverá suportar expansão para no mínimo 21.000 transações por segundo (tps) de SSL com chaves de 2K;

O equipamento deverá ser fornecido com proteção DDoS em hardware de 20 Milhões SYN-Cookies por segundo e podendo suportar expansão para no mínimo 40 Milhões;

O equipamento oferecido deverá suportar upgrade para realizar compressão em hardware com throughput de 12Gbps.

Características de Redundância e Funcionalidades Gerais

O equipamento oferecido deverá suportar e garantir a instalação em ambiente de alta disponibilidade;

O equipamento deverá ser capaz de trabalhar no modo Ativo/Standby;

O equipamento deverá ser capaz de trabalhar no modo Ativo/Ativo, mantendo o status das conexões. Aceita-se como Ativo-Ativo a utilização de dois endereços Virtuais, onde cada endereço fica ativo em um elemento e standby no outro;

Deverá suportar sincronismo de sessão entre os dois membros. A falha do equipamento principal não deverá causar a interrupção das sessões balanceadas;

Fornecer todos os recursos possíveis de redundância sem nenhuma despesa com licenças adicionais;

O equipamento deverá ser capaz de compor uma configuração de cluster com dois ou mais equipamentos da mesma família. Quando nesta configuração de cluster, um dos equipamentos deverá poder ser configurado como contingência N+1 para os demais;

O equipamento oferecido deverá fornecer recurso de agregação de portas baseado no protocolo LACP;

Fornecer recurso para suportar até 8 portas em um mesmo conjunto agregado;

O equipamento oferecido deverá fornecer recurso para o transporte de múltiplas VLAN por uma única porta (ou por um conjunto agregado de portas) utilizando o protocolo 802.1q;

O equipamento deve oferecer suporte a IPv6;

O equipamento oferecido deverá suportar múltiplas tabelas de rotas independentes;

O equipamento oferecido deverá fornecer recursos para o uso de servidores (reais) no mesmo Virtual Server; cada um server pode conter diversos grupos de servidores, cada grupo de servidores é chamado de pool, e cada pool pode possuir diversos servidores;

O equipamento, quando habilitado para mais de uma função (SLB, GSLB, Aceleração Web, etc) deverá permitir a importância da função, determinando quanta CPU e Memória será alocada para cada tipo de funcionalidade;

Deverá possuir certificação ICSA Network Firewall.

Características de Camada 7

O equipamento deverá suportar todas as aplicações comuns de um Appliance Layer 7:

- Server Load-Balancing;
- Firewall Load-Balancing;
- Proxy Load-Balancing;

Suportar balanceamento apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;

A solução deve permitir o encapsulamento, em camada 3, do tráfego entre o balanceador e o servidor para tráfego IPv4 e IPv6, quando o balanceamento é realizado apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;

O equipamento oferecido deverá ser capaz de balancear servidores com qualquer hardware, sistema operacional e tipo de aplicação;

O equipamento oferecido deverá ser capaz de abrir um número reduzido de conexões TCP com o servidor e inserir os HTTP requests gerado pelos clientes nestas conexões, reduzindo a necessidade de estabelecimento de conexões nos servidores e aumentando a performance do serviço;

O equipamento oferecido deverá suportar os seguintes métodos de balanceamento:
- Round Robin;
- Least Connections;
- Weighted Percentage (por peso);

- Servidor ou equipamento com resposta mais rápida baseado no tráfego real;
- Weighted Percentage dinâmico (baseado no número de conexões);

- Dinâmico, baseado em parâmetros de um determinado servidor ou equipamento, coletados via SNMP ou WMI;

O equipamento oferecido deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência de sessão dos seguintes tipos:

- por cookie – inserção de um novo cookie na sessão;
- por cookie – utilização do valor do cookie da aplicação, sem adição de cookie;
- por endereço IP destino;
- por Endereço IP origem;
- por sessão SSL;
- por análise da URL acessada;
- por análise de qualquer parâmetro no header HTTP;
- por análise do MS Terminal Services Session (MSRDP);
- por análise do SIP Call ID ou Source IP;
- por análise de qualquer informação da porção de dados (camada 7);

O equipamento oferecido deverá suportar os seguintes métodos de monitoramento dos servidores reais:

- Layer 3 – ICMP;
- Conexões TCP e UDP pela porta respectiva no servidor;

Devem existir monitores predefinidos para, no mínimo, os seguintes protocolos: ICMP, HTTP, HTTPS, Diameter, FTP, SASP, SMB, RADIUS, SMTP, MSSQL, ORACLE, RPC, LDAP, IMAP, NNTP, SMTP, POP3, SIP, Real Server, SOAP, SNMP e WMI;

O equipamento oferecido deverá possuir recursos balanceamento de carga de servidores SIP para VoIP (equipamento SIP Proxy);

O equipamento oferecido deverá ser capaz de limitar o número de sessões estabelecidas com cada servidor real;

O equipamento oferecido deverá ser capaz de limitar o número de sessões estabelecidas com cada servidor virtual;

O equipamento oferecido deverá possuir recursos para limitar o número de sessões estabelecidas com cada grupo de servidores;

O equipamento oferecido deverá possuir recursos para limitar o número de sessões estabelecidas com cada servidor físico;

Realizar Network Address Translation (NAT);

Realizar proteção contra Denial of Service (DoS);

Realizar proteção contra Syn flood;

Realizar limpeza de cabeçalho HTTP;

O equipamento deve permitir o controle de resposta ICMP por servidor virtual;

Implementar Listas de Controle de Acesso (ACL);

A configuração do equipamento deve ser baseada em perfis, permitindo fácil administração;

Os perfis devem ser hierarquizados, permitindo maior facilidade na administração de políticas similares;

O equipamento deve permitir que os Virtual Servers sejam criados com endereço IPv4 e os servidores reais utilizem endereços IPv6;

O equipamento deverá ser capaz de fazer compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente;

Deve ser possível definir qual tipo de compressão será habilitada (gzip1 a gzip9, deflate);

Deve ser possível definir compressão especificamente para certos tipos de objetos;

O equipamento deverá ser capaz de fazer aceleração de SSL, onde os certificados digitais são instalados no equipamento e as requisições HTTP são enviadas aos servidores sem criptografia;

Na aceleração de SSL, tanto a troca de chaves quanto a criptografia dos dados devem ser feitas com aceleração em hardware, para não onerar o sistema;

Deve ser possível configurar o equipamento para recriptografar em SSL a requisição ao enviar para o servidor, permitindo as demais otimizações em ambiente 100% criptografado;

O equipamento oferecido deverá suportar a utilização de memória RAM como cache de objetos HTTP, para responder às requisições dos usuários sem utilizar recursos dos servidores;

O recurso de cache deverá permitir a definição de quais tipos de objeto serão armazenados em cache e quais nunca devem ser cacheados;

O recurso de cache deve permitir o ajuste de quanta memória será utilizada para armazenar objetos;

Suporte a otimização do protocolo TCP para ajustes a parâmetros das conexões clientes e servidor;

A solução deve suportar Internet Content Adaptation Protocol (ICAP);

Deve ser capaz de realizar DHCP relay;

Deve ser capaz de permitir a criação de instâncias virtuais, com as seguintes características:
- Cada instância possuirá seu próprio sistema operacional;
- A versão de cada sistema operacional em cada instância poderá ser diferente;
- Reiniciar uma instância sem afetar as demais;
- No caso de utilizar licenciamento, cada instância poderá ter seu próprio conjunto de licenças;
- Deve possuir CPU dedicada a cada instância;
- Deve possuir interface se rede dedicadas a cada instância;
- No caso de falha em alguma instância essa falha deve permanecer isolada nesta instância;

Deve possuir relatórios em tempo real das aplicações, com pelos menos os seguintes gráficos:
- Tempo de resposta da aplicação;
- Latência de rede;
- Conexões para conjunto de servidores, servidores individuais;
- Por URL;
- Deve possuir framework unificado para configuração da aplicação;

Deve possuir criptografia IPSEC para comunicação entre os balanceadores;

Deve possuir suporte a Link Layer Discovery Protocol (LLDP);

Deve ser possível enviar, pelo menos, as seguintes informações via LLDP: Port ID, TTL, Port Description, System Name, System Description, Management Address, Port VLAN ID, Port and Protocol VLAN ID, VLAN Name, Protocol Identity, Link Aggregation, Maximum Frame Size;

Quando licenciada, a solução deve ter a capacidade de realizar cache transparente das respostas DNS;

A Solução deve ter a capacidade de permitir a criação de MIBs customizadas;

A Solução deve ter suporte a sFlow;

A solução deve possuir múltiplos domínios de roteamento em IPv4 e IPv6;

A solução deve permitir que cada domínio de roteamento utilize BGP, OSPF e RIP em IPv4 e IPv6;

A solução deve suportar Equal Cost Multipath (ECMP);

A solução deve realizar Bidirectional Forward Detection (BFD);

A solução deve ter suporte a Stream Control Transmission Protocol (SCTP);

A solução deve possuir lista dinâmica de endereços IP globais com atividades maliciosas;

A solução deve ser capaz de criar filtros de endereços IPs baseados em reputação, com no mínimo as seguintes categorias: Windows Exploits, Web Attacks, Botnets, Scanners, Denial of Service, Reputation, Phishing, Proxy;

Deve ter suporte a Transport Layer Security (TLS) Server Name Indication (SNI);

A solução deve possuir monitor HTTP/HTTPS com autenticação NTLM embutida, que permita verificar se o HTTP/HTTPS está operando assim como a plataforma de autenticação;

A solução deve realizar SSL Forward Proxy;

A solução deve ter suporte a TLS 1.2, SHA 2 Cipher e SHA256 hash;

A solução deve ser capaz de colocar em fila as requisições TCP que excedam a capacidade de conexões do grupo de servidores ou de um servidor. O balanceador não deverá descartar as conexões que excedam o número de conexões do servidor ou do grupo de servidores;

Deve ser possível configurar o tamanho máximo da fila;

Deve ser possível configurar o tempo máximo de permanência na fila;

A solução deve realizar Controle de Banda Estático para grupos de aplicações e rede;

A solução deve realizar Controle de Banda Dinâminco para grupos de aplicações e rede;

A solução deve realizar Controle de Banda baseado em domínio de roteamento;

A solução deve permitir a criação de túneis IP por domíno de roteamento utilizando GRE, IPIP, EtherIP, PPP;

A solução deve permitir a criação de túneis IP transparente utilizando GRE e IPIP;

Possuir suporte ao protocolo SPDY.

Aceleração Web

Deverá ser possível adicionar o mecanismo de garantia de aceleração web apenas com a adição de licença de software;

O equipamento deverá oferecer suporte a aceleração de aplicações HTTP realizada de forma simétrica ou assimétrica;

Quando implementada de forma simétrica, é exigido que se tenham appliances e licenças de aceleração web nas duas localidades;

Implementar mecanismo que aumente o número de conexões paralelas abertas por um único browser, sem utilização de plug-ins ou java/javascript;

Implementar controle de conteúdo dinâmico, permitindo que conteúdo dinâmico seja armazenado no cache do browser do usuário;

Uma vez implementado, o browser deverá dinamicamente solicitar objetos que não estejam mais válidos, sem validar todos os objetos da página. Apenas os objetos inválidos deverão ser re-solicitados;

Realizar a linearização de documentos pdf de forma dinâmica, de acordo com as necessidades do usuário, servindo páginas individuais e fora de ordem, para garantir que arquivos do tipo PDF sejam mais rapidamente vistos;

Oferecer os seguintes recursos de cache, uso de memória RAM e disco local:
- Suporte a cache dinâmico;
- O equipamento deverá ser capaz de armazenar várias cópias de um mesmo objeto em RAM ou Disco local;
- O recurso de cache deverá permitir a definição de quais tipos de objeto serão armazenados em cache e quais nunca devem ser cacheados;
- O equipamento oferecido deverá suportar a utilização de memória RAM como cache de objetos HTTP, para responder às requisições dos usuários sem utilizar recursos dos servidores;
- O equipamento deverá ter controle de sessão e servir a o objeto correto ao usuário correto, ainda que todos os objetos tenham o mesmo nome (ex: extrato.php);
- O equipamento deve implementar controle de conteúdo dinâmico, permitindo que o conteúdo dinâmico seja armazenado em cache;

- O equipamento deverá prover a funcionalidade de eliminar a necessidade de downloads de dados repetidos pelo browser cliente que deverá dinamicamente solicitar objetos;
- Ações do usuário deverão ser capazes de seletivamente invalidar o cache em RAM ou disco local, apagando apenas os objetos que fazem referência àquele usuário ou sessão;
- Ações do usuário deverão ser capaz de seletivamente invalidar o cache em RAM ou disco local, apagando TODAS as cópias daquele objeto em cache, quando a ação de um usuário afeta a informação dos outros;
- O cache em RAM ou disco local deverá ser apagado através de uma chamada externa segura. Esta chamada deverá poder ser integrada às aplicações através de uma API fornecida pelo fabricante da solução;
- Essa API deverá ser fornecida sem custo;

Todas as funcionalidades que acelerem as aplicações web não devem alterar a aparência ou funcionalidade dos sites;

Possibilitar a compressão de dados dinâmicos de aplicações web;

Otimizar os protocolos TCP e HTTP para a condição de cada usuário;

Possuir políticas de aceleração de aplicações pré-configuradas no equipamento;

Políticas deverão existir ao menos para SharePoint 2003 e 2007, Outlook Web Access 2003 e 2007, SAP, e Oracle Applications;

Suporte a multiplexação HTTP em topologia roteada e em topologia com tradução de endereço origem;

A multiplexação HTTP deverá funcionar também em aplicações onde haja autenticação NTLM;

Otimizar imagens eliminando metadados desnecessários e conversão do formato da imagem;

Ser capaz de remover espaços em branco e comentários nos arquivos JS e CSS, a fim de reduzir o tamanho do arquivo;

Ser capaz de acelerar a renderização da página mudando ordem de quando JavaScripts e Cascading Style Sheets (CSS) são carregados.

Características de Segurança Web e da Aplicação

Deverá possuir o mecanismo de segurança web e da aplicação;

O produto oferecido deverá identificar, isolar e bloquear ataques sofisticados sem impactar nas transações das aplicações;

Permitir que apenas transações de aplicações validadas sejam aceitas, o restante das transações deverá ser bloqueada, utilizando bloqueio por nível de aplicação baseado no contexto da sessão do usuário, com privilégios de autorização diferente, entradas de usuários e tempo de resposta de aplicação;

Permitir a utilização de um modelo positivo de segurança para proteger contra ataques às aplicações HTTP e HTTPS, além de proteger contra os ataques conhecidos aos protocolos HTTP e HTTPS;

Possuir política de segurança de aplicações pré-configuradas no equipamento para pelo menos as seguintes aplicações:
- Microsoft Outlook Web Access;
- Microsoft ActiveSync;
- Oracle Applications;
- Microsoft Office SharePoint;

Deverá permitir a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;

Deverá possuir mecanismo para criação dinâmica de política de segurança, com aprendizado automático de padrão de utilização da aplicação, realizado sobre o fluxo de tráfego bi-direcional atravessando o equipamento;

Possuir firewall XML integrado – suporte a filtro e validação de funções XML específicas da aplicação;

Deverá possibilitar atualização de novas assinaturas para ataques conhecidos;

Apresentar proteção positiva e segura contra ataques, como:
- Manipulação de entradas inválidas;
- Controle de Acesso Bruto (Ataque bruto via browser) na camada 7 da pilha OSI;
- Buffer Overflow;
- Cross-Site Script;
- Cross-site request forgery – CSRF;
- SQL/SO injection;
- Cookie poisoning;
- HTTP Request Smuggling;
- Manipulação de campos escondidos no HTTP;
- Trojan, backdoor e spyware;
- Detecção de evasão;
- LDAP injection;
- HTTP parameter pollution;

Deverá permitir a criação de assinaturas de ataques;

A criação das políticas deverá possuir pelo menos as formas:
- Automático através observação do tráfego para a aplicação;
- Automático através da observação do tráfego de teste;
- Manual;

Deverá reconhecer assinaturas seletivas, e filtros de ataque que devem proteger contra:
- Ataques de negação de serviços automatizados;
- Worms e vulnerabilidades conhecidas;
- Requests em objetos restritos e tipos de arquivos;
- Cloaking;

Esconder qualquer mensagem de erro http dos usuários;

Remover as mensagens de erro às paginas que serão enviadas aos usuários;

Prevenir contra vazamentos dos códigos dos servidores;

O equipamento oferecido deverá identificar, isolar e bloquear ataques sofisticados para pelo menos os seguintes protocolos: FTP, HTTP, HTTPS e SMTP;

Proteger contra as 10 maiores vulnerabilidades da lista OWASP;

Deverá emitir, pelo menos, os relatórios:
- Tabela de adequação ao PCI-DSS
- Gráfico indicando tipo de ataque;
- Gráfico indicando tipo de violação;
- Gráfico indicando quais URLs foram atacadas;
- Gráfico indicando severidade;
- Gráfico indicando os endereços IPs de origem;
- Gráfico indicando a localização geográfica dos endereços IPs de origem;

Deverá enviar automaticamente os relatórios via e-mail com a periodicidade determinada;

Deverá exportar as requisições que contem os ataques, pelo menos nos formatos PDF e binário;

Deverá realizar a localização geográfica do IP, identificando pais de origem da requisição;

Deverá detectar ataques de força bruta na camada 7 da pilha OSI através dos seguintes métodos:
- Latência da resposta do servidor;
- Monitorando o tempo de resposta com base na variação percentual do tempo;
- Monitorando o tempo de resposta com base na variação em segundos do tempo;
- Quantidade de transações por segundo (TPS);
- Monitorando a quantidade de transações por segundo com base na variação percentual das transações;
- Monitorando a quantidade de transações por segundo com base na quantidade de transações por endereço IP;

Deverá mitigar ataques de força bruta na camada 7 da pilha OSI através dos seguintes métodos:
- Limitação de banda do atacante;
- Bloqueio do acesso;
- Deve ser possível configurar o tempo que a mitigação estará em uso;

A solução deve ser capaz de aprender o comportamento da aplicação:
- Deve aprender os campos, os valores, os cookies e as URLs;
- As políticas sugeridas somente devem ser aplicadas após um período configurável de dias;

Deverá ter integração, via ICAP, com servidor de anti-vírus para verificação dos arquivos a serem carregados nos servidores;

Assinar e verificar assinaturas digitais de mensagens SOAP, possuir pelo menos as seguintes características:
- Nas requisições SOAP verificar partes das mensagens;
- Nas requisições SOAP verificar e decriptografar partes das mensagens;
- Nas repostas SOAP criptografar as mensagens;
- Nas repostas SOAP criptografar e assinar digitalmente as mensagens;

Deverá realizar log das alterações nas políticas:
- Deverá indicar o nome do usuário que realizou a mudanças;
- Deverá indicar as mudanças realizadas;

Deverá salvar automaticamente as políticas configuradas em arquivos diferentes a cada mudança realizada, permitindo assim o retorno a política anterior de forma fácil e rápida;

Deverá permitir a associação de administradores da solução a partições, sendo que o administrador somente terá acesso a partição associada a ele;

Deverá possuir proteção contra bots e web scraping e identificar automaticamente comportamento não-humano, navegadores operados por scripts ou qualquer outra forma que não operados por humanos;

Deverá identificar e armazenar o ataque acontecido com detalhes, no mínimo através de:

- Nome do ataque;
- Qual campo foi atacado;
- Quantas vezes esse ataque foi realizado;
- Cópia da tentativa do ataque;
- Horário do ataque;

Visando a redução dos falsos positivos, deverá permitir que as políticas sejam testadas antes de serem implementadas:

- A solução deverá permitir que as novas políticas fiquem apenas monitorando o tráfego, sem bloqueá-lo, indicando caso aconteça algum evento;

Para fins de auditoria externa, deverá ser possível exportar as políticas em arquivo XML;

Caso as políticas sejam alteradas no arquivo XML deverá ser possível o carregamento do novo arquivo XML para alteração nas políticas;

Deverá ser possível escrever políticas através do uso de linguagem de programação aberta, como por exemplo TCL;

Suportar Cache de Conteúdo para HTTP, permitindo que objetos sejam armazenados em RAM e requisições HTTP sejam respondidas diretamente pela solução;

O recurso de cache deverá permitir a definição de quais tipos de objeto serão armazenados em cache e quais nunca devem ser cacheados;

O recurso de cache deve permitir o ajuste de quanta memória será utilizada para armazenar objetos;

Permitir a criação de políticas automáticas que bloqueiem o endereço IP que realizar violações;

Deverá ser configurável o número de violações por minuto que cada endereço IP;

Devera ter integração com a ferramenta de detecção de vulnerabilidade da WhiteHat;

Permitir que o WhiteHat configure automaticamente o firewall de aplicação quando uma nova vulnerabilidade for detectada;

Permitir o uso do parâmetro HTTP X-Forwarded-For como parte da política de controle;

Esse parâmetro permite a diferenciação em ambientes que possuem NAT e as requisições chegam com o mesmo endereço IP de origem;

Deverá proteger o protocolo FTP com pelo menos os seguintes métodos:
- Determinar os comandos FTP permitidos;
- Limitar a quantidade de conexões;

Suporte a IPv6;

Suporte a SSL offload;

Suportar a implementação em modo Bridge e explícito.

Deverá proteger o protocolo SMTP com pelo menos os seguintes métodos:
- A comunicação deve ser aderente a RFC 2821;
- Limitar banda;
- Validar registro SPF do DNS;
- Determinar quais métodos SMTP podem ser utilizados;

Deverá possuir o recurso de response scrubbing, visa prevenir que a resposta do servidor exponha informações confidenciais;

Deverá armazenar os log localmente ou exportar para Syslog server;

Devera ter certificação ICSA para WAF (Web Application Firewall).

Acesso e Gerência

Implementar uma configuração de endereçamento IP estático ou dinâmico (DHCP/BOOTP) para o gerenciamento.

Implementar o SNTP (Simple Network Time Protocol) ou NTP (Network Time Protocol);

Fornecer ferramenta de gerenciamento centralizado da solução proposta, com todas as funcionalidades e licenças disponíveis, sem custos adicionais. Esta é uma ferramenta que deve permitir configurar, monitorar, gerenciar, inventariar e realizar troubleshooting na rede composta pelos equipamentos e seus elementos de forma centralizada;

Permitir acesso in-band via SSH;

Manter internamente múltiplos arquivos de configurações do sistema;

Utilizar SCP ou HTTPS como mecanismo de transferência de arquivos de configuração e Sistema Operacional;

Possuir auto-complementação de comandos na CLI;

Possuir ajuda contextual;

Interface por linha de comando (CLI – Command Line Interface) que possibilite a configuração dos equipamentos;

Possuir, no mínimo, Três níveis de usuários na GUI – Super-Usuário, Usuário com permissões reduzidas, e usuário Somente Leitura;

Os usuários de gerência deverão poder ser autenticados em bases remotas. No mínimo RADIUS, LDAP e TACACS+ deverão ser suportados;

Deverá ser possível receber da base RADIUS, LDAP e TACACS+ o nível de acesso (Grupo ou Permissões);

Possuir Interface Gráfica via Web;

A interface Gráfica deverá permitir a atualização do sistema operacional e/ou a instalação de patches ou Hotfixes sem o uso da linha de comando;

A interface gráfica deverá permitir a configuração de qual partição o equipamento deverá dar o boot;

Possuir um comando, via CLI, que mostre o tráfego de utilização das interfaces (bps e pps);

Suportar a rollback de configuração e imagem;

Possuir e fornecer MIBs compiláveis na plataforma HP Open View Network Node Manager;

Possuir e fornecer geração de mensagens de syslog para eventos relevantes ao sistema;

Possuir configuração de múltiplos syslog servers para os quais o equipamento irá enviar as mensagens de syslog;

Possuir armazenamento de mensagens de syslog em dispositivo interno ao equipamento;

A interface Gráfica deverá permitir a reinicialização do equipamento;

Reinicialização do equipamento por comando na CLI;

Possuir recurso de gerência via SNMP e implementar SNMPv1, SNMPv2c e SNMPV3;

Possuir traps SNMP;

Possui suporte a monitoração utilizando RMON atr avés de pelo menos 4 grupos:
- statistics, history, alarms e events;

Os logs de sistema devem ter a opção de ser armazenados internamente ao sistema ou em servidor externo;

Implementar Debugging: CLI via console e SSH.

Serviços Que Compõem a Solução

1. Instalação, configuração e testes

Instalar, configurar e testar todos os componentes de hardware, software e sistema operacional, necessários ao completo funcionamento dos objetos contratados, acompanhado por equipe técnica do TJERJ;

O técnico da empresa licitante responsável por participar da implementação conjunta, mencionada no item 2.2.1.1, deverá apresentar certificação de capacidade técnica de instalação e configuração pelo próprio fabricante. As equipes técnicas do TJERJ definidas no item citado terão liberdade de escolha ou rejeição do técnico disponibilizado pela empresa;

A empresa licitante deverá responsabilizar-se pelo fornecimento de todos os dispositivos necessários ao perfeito funcionamento dos equipamentos, bem como substituir todo equipamento ou componente que apresentar dano de transporte ou mau funcionamento que seja detectado durante a fase de instalação e configuração, no prazo máximo de 7 (sete) dias úteis, contado da notificação que lhe for entregue oficialmente;

2. Suporte Técnico

Atendimento on-site e suporte telefônico prestado pelo fornecedor, 24 x 7 (vinte e quatro horas, sete dias na semana), sem limite de horas ou chamados, com direito à resolução de dúvidas pertinentes ao produto e abertura de chamados para solução de problemas;

O suporte telefônico deverá ser realizado mediante número do Município do Rio de Janeiro (código 21) ou por ligação gratuita (código 0800);

Adicionalmente, deverão ser disponibilizados site e e-mail para abertura de chamados;

A CONTRATADA garantirá o direito à atualização de licenças de software utilizadas;

A Contratada deverá disponibilizar em sua página na internet um sistema próprio de controle de chamados com, no mínimo, hora de abertura do chamado, hora de fechamento do chamado, descrição e solução do problema, nome do responsável da contratante pela abertura e acompanhamento do chamado, nome do(s) responsável (is) da contratada pela solução do problema;

O prazo máximo para que se inicie o atendimento técnico será de 2 (duas) horas, contado do registro do chamado técnico, devidamente formalizado;

Será de 4 (quatro) horas após a chegada do técnico, o prazo máximo para que a CONTRATADA restabeleça o funcionamento pleno do equipamento ou software com problema;

3. Garantia

A garantia dos equipamentos deverá ser de 36 (trinta e seis) meses, na modalidade on-site, nas dependências do TJERJ, na cidade do Rio de Janeiro, por meio de assistência técnica da empresa licitante ou de terceiros, devidamente credenciada pelo fabricante dos equipamentos ofertados;

A empresa licitante deverá substituir qualquer bem que esteja apresentando excesso de defeitos, até o final do período de garantia, inclusive defeitos provenientes de erro de projeto. A substituição do equipamento prevista far-se-á sem ônus de qualquer espécie para o TJERJ;

A empresa licitante deverá garantir o funcionamento e o desempenho normais dos bens fornecidos, conforme especificações técnicas constantes nos seus respectivos manuais técnicos;

A empresa licitante deverá garantir a substituição do bem defeituoso, sem ônus para o TJERJ;

A empresa licitante deverá assegurar ao TJERJ a manutenção de estoque de reposição das peças e dos componentes dos equipamentos fornecidos. Em caso de descontinuidade da fabricação desses equipamentos, a empresa licitante garantirá a reposição de peças no período de dois anos após a referida descontinuidade, que poderão ser adquiridas pelo TJERJ, caso haja interesse.

Tratando-se da aquisição de 2 (dois) equipamentos, a CONTRATADA deverá garantir o funcionamento de no mínimo um equipamento, nas condições estabelecidas no item 2.2.1.3 e, no caso de falhas de ambos concomitantemente, poderá o segundo equipamento ter seu defeito solucionado no prazo máximo de 2 (dois) dias úteis, inclusive no caso em que seja necessária sua substituição por um equipamento novo.

4. Licenciamento;

A CONTRATADA deverá fornecer todas as licenças necessárias ao funcionamento da solução, conforme especificação técnica constante neste Termo de Referência, na modalidade de licenciamento perpétuo, ou seja, todas as licenças fornecidas serão de propriedade do Tribunal, independente de renovações futuras de contrato ou da assinatura de novos contratos de suporte ou garantia;

A CONTRATADA deverá prover garantia de atualização de licenças do software por meio da disponibilização de programas, correções, atualizações críticas de segurança dentre outros;

As licenças serão garantidas e atualizadas (subscription) pelo prazo de 36 (vinte e quatro) meses, contados a partir do termo de aceite definitivo;

Durante a vigência do contrato, a CONTRATADA fornecerá ao Tribunal de Justiça mídias em CD-ROM, contendo todas as atualizações lançadas pelos fabricantes, sempre que as mesmas não forem disponibilizadas para download na página do fabricante;

As mídias que apresentarem defeito deverão ser substituídas imediatamente;

5. Banco de Horas

Quatrocentas e oitenta horas de suporte presencial, para tarefas de projeto, ou seja, aquelas, que requerem maior dedicação, mais tempo de desenvolvimento e estudo da nossa infraestrutura. São as migrações de versões, migrações de servidores, situações de melhora de desempenho e segurança, dentre outras;

Para cada serviço realizado, a CONTRATADA deverá fornecer um Relatório de Atendimento Técnico (RAT) contendo a data e hora do chamado, a data e hora de início e término do atendimento, a descrição do serviço efetuado e a conclusão do serviço;

As horas de Suporte On-Site efetivamente utilizadas serão faturadas por período não inferior a um mês, mediante apresentação de RAT, atestado por um funcionário da DGTEC responsável pelo Suporte aos Servidores e Rede;

A CONTRATADA deverá comprovar que os profissionais alocados para o atendimento relacionado ao banco de horas possuem certificação do fabricante nos produtos e serviços para os quais prestarão o atendimento;

A Solicitação para uso das horas do Banco de Horas será através da abertura de chamado telefônico por um número do tipo 0800, isto é, sem custo de ligação para o Contratante, ou por número da área do Municipio do Rio de Janeiro (código 21), devendo ser no idioma português brasileiro;

Adicionalmente, deverão ser disponibilizados site e e-mail para solicitação de atendimento relativo ao Banco de Horas;

A utilização das horas ficará a critério do Contratante que poderá utilizá-las ou não, parcial ou completamente, durante a vigência do contrato.

1.2 – DEFINIÇÃO DA SOLUÇÃO

Critério	Atendimeto da Solução	
	SIM	NÃO
É possível especificar o serviço usando parâmetros usuais de mercado?	☐	
É possível medir o desempenho da qualidade usando parâmetros usuais de mercado?	☐	
O objeto da contratação se estende necessariamente por mais de um ano?	☐	
O objeto da contratação é essencial para o negócio?	☐	

1- RESPONSABILIDADES DO PJERJ E DA CONTRATADA

2.1 – DEVERES E RESPONSABILIDADES DO PJERJ

Dever/Responsabilidade (enumerar os deveres e responsabilidades do contratante)
1. Permitir o livre acesso dos profissionais da CONTRATADA às dependências do órgão CONTRATANTE, com a finalidade exclusiva de exercer atividades relacionadas à execução do contrato e desde que estejam devidamente identificados;
2. Efetuar o pagamento devido à CONTRATADA pela execução dos serviços, após terem sido estes devidamente atestados e visados pelo fiscal, nos termos e prazos previstos na legislação pertinente;

fls. 48

3. Exercer a efetiva fiscalização do cumprimento às leis, normas e regulamentos ambientais, sanitários, trabalhistas, previdenciário, tributário, fiscais e de defesa do consumidor, que se apliquem à prestação de serviços objeto deste contrato.

2.2 – DEVERES E RESPONSABILIDADES DA CONTRATADA

Dever/Responsabilidade

(enumerar os deveres e responsabilidades da contratada)

1. A CONTRATADA deverá fornecer mão-de-obra técnica própria, não terceirizada, para prestação dos serviços especificados nesse Projeto;
2. A CONTRATADA deverá observar rigorosamente todos os itens do Termo de Referência, executando os serviços de acordo com as especificações e normas aplicáveis, utilizando ferramental apropriado e dispondo da infraestrutura e equipe técnica, exigidas para a perfeita execução do objeto desta contratação;
3. A CONTRATADA indicará um preposto como responsável pelo gerenciamento dos serviços, autorizado a tratar com o CONTRATANTE a respeito de todos os aspectos que envolvam a execução do contrato;
4. A CONTRATADA, independentemente da atuação do Fiscal do Contrato, não se eximirá de suas responsabilidades quanto à execução dos serviços, responsabilizando-se pelo fiel cumprimento das obrigações constantes no termo de referência;
5. A CONTRATADA, independentemente da atuação do Fiscal do Contrato, deverá reparar, corrigir, substituir, total ou parcialmente, às suas expensas, serviços objeto do contrato em que se verifiquem vícios, defeitos ou incorreções resultantes de execução irregular ou de emprego de material ou equipamentos inadequados ou não correspondentes às especificações;
6. A CONTRATADA responderá civil e administrativamente, sem prejuízo de medidas outras que possam ser adotadas, por quaisquer danos causados ao Poder Judiciário do Estado do Rio de Janeiro ou a terceiros, em razão da execução dos serviços;
7. A CONTRATADA deverá atender com presteza as reclamações sobre a qualidade dos serviços executados, providenciando a sua imediata correção, sem ônus para a Administração Judiciária;
8. A CONTRATADA deverá facilitar a ação da fiscalização do Poder Judiciário do Estado do Rio de Janeiro, fornecendo informações ou promovendo acesso à documentação dos serviços em execução, e atender prontamente às observações e exigências por ela apresentada;
9. A CONTRATADA deverá estar ciente de que quaisquer entendimentos com o Fiscal ou o Gestor do Contrato serão feitos sempre por escrito, não sendo consideradas quaisquer alegações com fundamento em ordens ou declarações verbais;
10. A CONTRATADA deverá dar ciência ao Poder Judiciário do Estado do Rio de Janeiro, imediatamente e por escrito, de qualquer anormalidade que verificar na execução dos serviços;
11. A CONTRATADA deverá dispor de pessoal e equipamentos necessários de forma a manter contínua a prestação de serviço;
12. A CONTRATADA se responsabilizará pela permanente manutenção da validade da documentação Jurídica, Fiscal, Técnica e Econômico-Financeira da empresa assim como pela atualização de formação de seus profissionais;
13. A CONTRATADA assumirá como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução das obrigações contratadas;
14. À CONTRATADA serão vedados, sob pena de rescisão e aplicação de qualquer outra pena cabível, a divulgação e o fornecimento de dados e informações referentes aos serviços objeto do contrato;
15. A CONTRATADA não poderá se valer do contrato para assumir obrigações perante terceiros, dando-o como garantia, nem utilizar os direitos de crédito a serem auferidos em função dos serviços prestados, em quaisquer operações de desconto bancário, sem prévia autorização do Poder Judiciário do Estado do Rio de Janeiro;

ESTRATÉGIA DA CONTRATAÇÃO

16. Durante toda a execução do contrato, deverão ser mantidas em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na contratação;
17. A CONTRATADA deverá respeitar os critérios de sigilo aplicáveis aos dados, informações e às regras de negócios relacionados a prestação do serviço contratado;
18. A CONTRATADA firmará, através de seus representantes, antes do início da execução do Contrato, Termo de Compromisso de Manutenção de Sigilo, nos termos do formulário FRM-DGTEC-041-09;
19. A CONTRATADA deverá prestar os serviços nos locais, horários e parâmetros de qualidade estabelecidos neste Termo de Referência, de forma a assegurar plena eficácia na execução, sob inteira responsabilidade da CONTRATADA;
20. A CONTRATADA deverá prestar, sempre por escrito, todos os esclarecimentos que forem solicitados pelo PJERJ, cujas reclamações atinentes a quaisquer aspectos da execução contratual se obriga prontamente a atender;
21. A CONTRATADA deverá recompor o valor da garantia contratual sempre que a anterior vença ou tenha o seu valor reduzido em razão de aplicação de quaisquer penalidades, ou ainda sempre que ocorrer modificação no valor do contrato, durante a sua vigência;
22. Todas as informações transmitidas do CONTRATANTE para a CONTRATADA e seus funcionários são de caráter confidencial e não poderão ser transmitidas ou facilitadas a quem quer que seja, sem expressa autorização do CONTRATANTE;
23. A CONTRATADA cumprirá e fará cumprir por seus profissionais as normas e os regulamentos disciplinares do CONTRATANTE, bem como quaisquer determinações das autoridades competentes, sem quaisquer ônus para o CONTRATANTE;
24. A CONTRATADA se responsabilizará pela idoneidade e pelo comportamento de seus profissionais, prepostos ou subordinados, e, ainda, por quaisquer prejuizos que por eles sejam causados ao CONTRATANTE;
25. A CONTRATADA responderá objetivamente pela má utilização dos bens (materiais, utensílios e equipamentos) disponibilizados pelo CONTRATANTE para a realização dos serviços, obrigando-se a repor quaisquer desvios, desperdícios, perdas ou danos que venham a ocorrer;
26. A CONTRATADA preservará o CONTRATANTE, mantendo-o salvo de quaisquer demanda, reivindicações, queixas e representações de qualquer natureza, decorrentes de ação da CONTRATADA;
27. A CONTRATADA deverá executar serviços de alta qualidade, de modo a atender as exigências do CONTRATANTE, utilizando profissionais próprios, especializados, cabendo-lhe total e exclusiva responsabilidade pelo integral atendimento de toda legislação que rege a execução deste contrato, com ênfase na constitucional, tributária, civil, previdenciária e trabalhista, em especial, na segurança e higiene do trabalho;
28. A CONTRATADA deverá obedecer às determinações do PGRS (Plano de Gerenciamento de Resíduos Sólidos), e de seus desdobramentos como o PGRSS, o PGRCC, entre outros, do Poder Judiciário do Estado do Rio de Janeiro.

3. INDICAÇÃO DOS TERMOS CONTRATUAIS

3.1 – PROCEDIMENTOS E CRITÉRIOS DE ACEITAÇÃO DO OBJETO A SER RECEBIDO

Etapa / Fase / Item	Indicador	Limite Mínimo Aceitável
1. **Recebimento dos bens** A entrega dos equipamentos, de seus acessórios e periféricos deverá obedecer às seguintes condições: I. Ser efetuada em entrega única;	Características do equipamento (Hardware, Camada Redundância e Funcionalidades Gerais e Segurança Web e da Aplicação)	Deverão ser entregues dois equipamentos idênticos com as características determinadas no Indicador do critério de aceitação de recebimento.

II. Ser efetuada no prazo máximo de 30 (trinta) dias corridos após a assinatura do contrato; III. Os equipamentos fornecidos deverão ser novos, de primeiro uso e em linha de fabricação; IV. Todos os equipamentos, peças e componentes de cada item devem ser iguais e do mesmo fabricante; V. Cada um dos equipamentos deverá ser entregue em embalagem lacrada, com todos os folhetos ou manuais originais atualizados e respectivas especificações técnicas, acompanhado de todos os cabos conectivos e de força e todos os drivers e utilitários necessários a sua completa instalação, configuração, funcionamento e controle; VI. Cada equipamento deverá ter o número de série — em algarismos numéricos, alfabéticos e em código de barras — impresso em etiqueta não removível fixada na parte traseira do equipamento. O número de série deve ser único para cada equipamento; VII. Os bens devem ser 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; VIII. A embalagem devera exibir o número de série e código de barras do equipamento embalado; IX. Os equipamentos serão entregues no Datacenter do TJRJ (Av. Erasmo Braga, 111 – Lâmina I – Sala 111 – Centro – Cep: 20020-903), na presença de um representante da Diretoria Geral de Tecnologia da Informação. A empresa deverá avisar a data de entrega do material com 72 (setenta e duas) horas de antecedência, através dos telefones (21) 3133-4070 ou 3133-2799;		

X. A entrega deverá ser acompanhada de Nota Fiscal de Venda discriminando o número de série de cada equipamento no corpo da nota ou em relação anexa e Guia de Importação, quando for o caso; XI. A entrega dos equipamentos deverá ser realizada pela empresa licitante sem nenhum ônus adicional para o PJERJ, sendo o contratado responsável pelo descarregamento da mercadoria no local determinado; XII. Os equipamentos entregues devem ter, no momento da entrega, todas as características exigidas neste documento sem a necessidade de inclusão de nenhum componente, módulo ou dispositivos extra; XIII. O Poder Judiciário do Rio de Janeiro se reserva o direito de devolver qualquer equipamento que não atenda às especificações deste edital, o que poderá vir a ser detectado somente no momento da instalação e utilização do equipamento; XIV. A CONTRATADA, na hipótese prevista no item acima, obrigar-se-á a substituir o equipamento, arcando com todas as despesas decorrentes. 2. Instalação, configuração e testes O técnico da empresa licitante responsável por participar da implementação conjunta, mencionada no item 2.2.1.1, deverá apresentar certificação de capacidade técnica de instalação e configuração pelo próprio fabricante 3. Suporte técnico		

fls. 52

A Contratada deverá disponibilizar telefone do Rio de Janeiro (código 21) com a finalidade de suporte telefônico prestado pelo fornecedor, 24 x 7 (vinte e quatro horas, sete dias na semana), sem limite de horas ou chamados, com direito à resolução de dúvidas pertinentes ao produto e abertura de chamados para solução de problemas; A Contratada deverá disponibilizar endereço na Internet e email para abertura de chamados; A Contratada deverá disponibilizar em sua página na internet um sistema próprio de controle de chamados com, no mínimo, hora de abertura do chamado, hora de fechamento do chamado, descrição e solução do problema, nome do responsável da contratante pela abertura e acompanhamento do chamado, nome do(s) responsável (is) da contratada pela solução do problema; 4. Licenciamento; A CONTRATADA deverá fornecer todas as licenças		

necessárias ao funcionamento da solução, conforme especificação técnica constante neste Termo de Referência, na modalidade de licenciamento perpétuo, ou seja, todas as licenças fornecidas serão de propriedade do Tribunal, independente de renovações futuras de contrato ou da assinatura de novos contratos de suporte ou garantia; Durante a vigência do contrato, a CONTRATADA fornecerá ao Tribunal de Justiça mídias em CD-ROM, contendo todas as atualizações lançadas pelos fabricantes, sempre que as mesmas não forem disponibilizadas para download na página do fabricante; 5. Banco de Horas Para cada serviço realizado, a CONTRATADA deverá fornecer um Relatório de Atendimento Técnico (RAT) contendo a data e hora do chamado, a data e hora de início e término do atendimento, a descrição do serviço efetuado e a conclusão do serviço; A CONTRATADA deverá comprovar que os profissionais		

alocados para o atendimento relacionado ao banco de horas possuem certificação do fabricante nos produtos e serviços para os quais prestarão o atendimento; A Solicitação para uso das horas do Banco de Horas será através da abertura de chamado telefônico por um número do tipo 0800, isto é, sem custo de ligação para o Contratante, devendo ser no idioma português brasileiro; Adicionalmente, deverão ser disponibilizados site e e-mail para solicitação de atendimento relativo ao Banco de Horas;		

3.2 – ESTIMATIVA DE VOLUME DE SERVIÇOS OU BENS

Serviço/Bens	Estimativa	Forma de Estimativa
1-Equipamentos	2	Aquisição contratual

3.3 – METODOLOGIA DE AVALIAÇÃO DA QUALIDADE E DA ADEQUAÇÃO

Etapa / Fase / Item	Método de Avaliação
1. Recebimento provisório	Verificação do cumprimento das condições de entrega especificadas na seção 3.1 (PROCEDIMENTOS E CRITÉRIOS DE ACEITAÇÃO DO OBJETO A SER RECEBIDO), item 2 (Recebimento dos bens). Conferência das quantidades entregues.
2. Recebimento definitivo	Verificação do funcionamento dos appliances após a execução do serviço de instalação, configuração e testes iniciais, realizada pela Contratada com o acompanhamento do TJRJ.

3.4 – INSPEÇÕES E DILIGÊNCIAS

Tipos	Forma de Exercício
1. Não se aplica a esta contratação	-

3.5 – FORMA DE PAGAMENTO

fls. 55

Até 30 dias a contar da data de autuação da Nota Fiscal no Protocolo do Tribunal de Justiça do Estado do Rio de Janeiro, desde que acompanhada de toda a documentação necessária, em observância aos procedimentos apresentados a seguir:

- A prestação do serviço de suporte técnico será faturado em valor fixo mensal, por período não inferior a um mês, mediante a comprovação dos mesmos;

- O pagamento dos equipamentos será realizado em parcela única;

- Os serviços de 1.Instalação, configuração e testes, 2.Garantia dos equipamentos e 3.Licenciamento dos softwares serão pagos em parcela única;

- O serviço de Banco de Horas será pago sob demanda do TJRJ, mediante solicitação do TJRJ à CONTRATADA, conforme a utilização das horas dentro do mês a ser faturado.

3.6- CRONOGRAMA DE EXECUÇÃO FÍSICO-FINANCEIRA

Entrega 1

2 (dois) equipamentos do tipo appliance

Data de Entrega	Percentual Pago	Valor Estimado
1 – Máximo de 30 dias corridos da assinatura do contrato	100%	R$
Total:	100%	R$

3.7- MECANISMOS FORMAIS DE COMUNICAÇÃO

1. A CONTRATADA deverá prover um canal de comunicação, sem ônus para o PJERJ, para recebimento de solicitações de solução de problemas, com disponibilidade de atendimento das 8 horas até às 20 horas, de segunda a sexta-feira;
2. A CONTRATADA deverá fornecer um número de protocolo para todos os chamados abertos, para facilitar seu acompanhamento;

Função de Comunicação: (Descrição do que será comunicado formalmente)

Entrega dos equipamentos, necessidade de utilização da garantia (problemas com os equipamentos), execução de serviços de garantia, descumprimento de cláusulas contratuais.

Documento	Emissor	Destinatário	Meio	Periodicidade
Plano de Inserção (FRM-DGTEC-041-07)	PJERJ (Equipe de Gestão da Contratação)	Contratada	Entrega pessoal/ Correio/ Internet	Única
Ata de Reunião Inaugural (FRM-DGLOG-005-06)	PJERJ (Equipe de Gestão da Contratação)	Contratada	Entrega pessoal/ Correio/ Internet	Única
Termo de Compromisso de Manutenção de Sigilo (FRM-DGTEC-041-09)	PJERJ Contratada	PJERJ (Gestor do Contrato)	Entrega pessoal/ Correio	Única
Termo de Ciência (FRM-DGTEC-041-08)	Contratada	PJERJ (Gestor do Contrato)	Entrega pessoal/ Correio	Eventual
Ordem de serviço ou de fornecimento de bens (FRM-DGTEC-041-10)	PJERJ (Gestor do Contrato)	Contratada (Preposto)	Entrega pessoal/ Correio/ Internet	Única

fls. 56
Ctl.

Termo de recebimento provisório (FRM-DGTEC-041-11)	PJERJ (Fiscal Técnico)	Contratada (Preposto)	Entrega pessoal	Única
Termo de recebimento definitivo (FRM-DGTEC-041-12)	PJERJ (Gestor do Contrato)	Contratada (Preposto)	Entrega pessoal	Única
Nota Fiscal	Contratada	PJERJ	Entrega pessoal	Única
Relação de números de série	Contratada	PJERJ	Entrega pessoal/ Correio/ Internet	Única
Termo de Garantia	Contratada	PJERJ	Entrega pessoal/ Correio	Única
Solicitação de Serviços	PJERJ	Contratada	Canal de comunicação, sem ônus para o PJERJ, provido pela Contratada	Eventual
Relatório Mensal de Serviços	Contratada (Preposto)	PJERJ (Fiscal Demandante)	Entrega pessoal/ Correio/ Internet	Mensal
Solicitações de Serviços atendidas	Contratada (Preposto)	PJERJ (Fiscal Demandante)	Internet	Mensal
Ofício: quaisquer questões administrativas durante a execução do contrato, inclusive descumprimento de cláusula contratual (Acordo de Nível de Serviço)	PJERJ	Contratada	Entrega pessoal/ Correio	Eventual
Mensagem eletrônica: questões administrativas ou técnicas durante a execução do contrato	PJERJ	Contratada	Internet	Eventual

3.8 – REGRAS PARA APLICAÇÃO DE MULTAS E SANÇÕES

Ocorrência	Sanção
1- Inexecução total ou parcial do contrato	Advertência
	Multa de até 20% do valor total do contrato
	Suspensão temporária de participação em licitação e impedimento de contratar com a Administração, por prazo não superior a 2 (dois) anos
	Multa diária de 0,5% do valor total do contrato

ESTRATÉGIA DA CONTRATAÇÃO

ATENÇÃO: A cópia impressa a partir da *intranet* é cópia não controlada.

2- Descumprimento dos prazos estabelecidos para entrega dos equipamentos	Rescisão unilateral do contrato por parte do PJERJ
3- Descumprimento dos prazos estabelecidos para prestação dos serviços relacionados à garantia	Multa diária de 0,03% do valor total do contrato. (A multa estabelecida para essa ocorrência poderá não ser aplicada, caso o PJERJ aceite a justificativa apresentada pela Contratada)

4 – ORÇAMENTO DETALHADO

Bens / Serviços	Valor Estimado
1 – 2 (dois) equipamentos do tipo appliance	R$
VALOR ESTIMADO TOTAL:	**R$**

5- ADEQUAÇÃO ORÇAMENTÁRIA

5.1 – FONTE DE RECURSOS

Valor	Fonte (Programa/Ação)
1-	Fonte: 10 – Recurso próprio do PJERJ Programa: 0361.02.061.0141.1648 – Aperfeiçoamento e sustentação da tecnologia da informação Ação: 1648107-4-10
Total = R$	

5.2 – ESTIMATIVA DE IMPACTO ECONÔMICO-FINANCEIRO

Valor	Exercício Financeiro	Porcentual do Orçamento	Análise e Conclusão
1-			
2-			

6- CRITÉRIOS TÉCNICOS DE JULGAMENTO DAS PROPOSTAS

6.1 – PROPOSTA TÉCNICA

6.1.1 – Organização da Proposta (descreve como as propostas devem estar formatadas para avaliação)

ANEXO I – A

PROPOSTA DE PREÇOS DETALHADA

LICITAÇÃO Nº ___/2010

PROPOSTA ESTIMATIVA DE PREÇOS DE MERCADO

RAZÃO SOCIAL DA PROPONENTE:

CNPJ:

fls. 58

ENDEREÇO:

PESSOA DE CONTATO:

TELEFONE / FAX / E-MAIL:

VALIDADE: 90 (noventa dias)

Switch de Camada 7	Preço unitário
Switch do tipo appliance, para otimização de aplicações web, balanceamento de servidores e segurança	R$
Descrição dos Serviços	
Instalação, configuração e testes dos componentes de hardware, do sistema operacional, software de configuração e todos os demais softwares necessários	R$
Licenciamento dos Softwares	R$
Suporte Técnico 24x7 (vinte e quatro horas, sete dias por semana)	R$
Garantia dos equipamentos e licenças de software	R$
Banco de horas de consultoria para suporte on-site (480 horas)	R$

4.1 Deverá ser apresentado pelo licitante:

4.1.1 A empresa deverá apresentar declaração firmada por representante legal do licitante contendo a descrição: a) do serviço de instalação, configuração e testes, b) do licenciamento dos Softwares, d) do suporte técnico Standard 24x7; c) do banco de horas. Tudo conforme tabela do anexo A;

4.1.2 O "Termo de Garantia", emitido por representante legal do licitante, em papel timbrado, endereçado explicitamente ao TJERJ, contendo:

4.1.3.1 Prazo de garantia de 36 (trinta e seis) meses, para cada equipamento, a contar do termo de aceite definitivo;

4.1.3.2	Prazo de garantia de 36 (trinta e seis) meses, para cada licenciamento de software, a contar do termo de aceite definitivo;
4.1.3.3	Suporte técnico: presencial, telefônico, internet e e-mail 24X7 (vinte e quatro horas por dia e sete dias por semana);
4.1.3.4	O número do telefone da central de atendimento tipo 0800, ou compromisso que o número será disponibilizado na data de assinatura do memorando de início, com as orientações para abertura de chamado, onde conste, no mínimo, site e e-mail para registro de chamados;
4.1.3	Atestado de capacidade técnica firmado por órgão do poder público ou por pessoa jurídica de direito privado, comprovando haver licenciado softwares iguais ou similares aos do objeto desta contratação;
4.1.4	Atestado de capacidade técnica emitido por órgão do poder público ou por pessoa jurídica de direito privado, que comprove ter a empresa realizado satisfatoriamente serviços iguais ou similares, de natureza pertinente e compatível com o objeto desta contratação;
4.1.5	Declaração firmada pelo representante legal do licitante de que é autorizado do fabricante dos equipamentos, onde deverá vir mencionado o seu nível de certificação;
4.1.6	Planilha totalizadora com a descrição do serviço de instalação, configuração e testes, suporte técnico, garantia, licenciamento e banco de horas.

ESTRATÉGIA DA CONTRATAÇÃO

ATENÇÃO: A cópia impressa a partir da *intranet* é cópia não controlada.

6.1.2 – Critérios Técnicos Pontuáveis – não se aplica a esta contratação			
Critério	Pontuação	%	Justificativa
1-			
2-			
3-			

6.2 – CRITÉRIOS DE SELEÇÃO

Licitação

Modalidade	Tipo
Pregão, em conformidade com a Lei nº 10.520/02.	Menor preço por item.

6.3 – QUALIFICAÇÃO TÉCNICA

Não se aplica a esta contratação

6.3.1 – Requisitos de Capacitação e Experiência
1-
2-

6.3.2 – Requisitos de Qualificação das Equipes Técnicas
1-
2-

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO		
Integrante Técnico	Integrante Demandante	Integrante Administrativo
SELMO MANACUSANSCH CHEFE DE SERVIÇO-SEFER Matr: 01/33001	Marcos Stallone Santos TJERJ/DGTEC/ Dep. de Infraestrutura de TI Divisão de Redes Diretor - Matr. 10/19816	Eliane S. B. Ourique Chefe do Serviço de Planejamento da Qualidade de Materiais Matr. 10/90.626
Rio de Janeiro, 22 de outubro de 2015		