



TERMO DE REFERÊNCIA – ANEXO I

REQUISIÇÃO DE SERVIÇO - RS

N.: 20160005

DATA: 29/08/2016

ÓRGÃO: 8323EMERJ - SERVIÇO DE COMPRAS

PROGRAMA DE TRABALHO: 03620206101422296

PROCESSO: 2016125972

LICITAÇÃO N.º: 08/2016

PROCEDIMENTO ADOTADO: LICITAÇÃO

ÓRGÃO FISCAL: 8325 - EMERJ - DEPARTAMENTO DE TEC DE INF E COMUNICACAO

MEMORANDO: 02/2015 ORIGEM: EMERJ - DEPARTAMENTO DE TEC DE INF E COMUNICACAO

PRAZO: 24 meses, a contar do memorando de início, a ser expedido pelo Órgão Fiscal.

PREÇO ESTIMADO DA RS: 549.998,08 – QUINHENTOS E QUARENTA E NOVE MIL, NOVECENTOS E NOVENTA E OITO REAIS E OITO CENTAVOS

OBJETO: Prestação dos serviços de conexão com a internet de 30 Mbps full duplex, gerenciamento de rede wireless, segurança de acesso à internet UTM e suporte técnico e garantia de equipamentos de rede Wi-Fi

1 DEFINIÇÃO DO OBJETO

Contratação de empresas especializadas para a prestação de serviço de comunicação de dados, fornecimento de segurança e gerenciamento de rede Wi-Fi e, provimento de suporte técnico e garantia dos equipamentos da Escola da Magistratura do Estado do Rio de Janeiro a fim de prover acesso continuado à internet pública a partir da rede Wi-Fi proprietária.

2 DESCRIÇÃO DA SOLUÇÃO DE TI

2.1 Descrição

- 2.1.1 Visa o presente procedimento à contratação de serviço de conexão dedicada à internet com a velocidade mínima de 30 Mbps para a interligação da rede Wi-Fi existente nas dependências da Escola da Magistratura do Estado do Rio de Janeiro - EMERJ.
- 2.1.2 Deverão ser fornecidos serviço de segurança (UTM), além de serviço de operação, suporte e gerenciamento da rede wireless (Wi-Fi) de propriedade da CONTRATANTE, já implantada no local.
- 2.1.3 O gerenciamento da rede de que trata o item anterior deverá contemplar no mínimo os subitens abaixo:
 - 2.1.3.1 Gerenciamento total da rede Wi-Fi
 - 2.1.3.2 Configuração completa da rede de acordo com as orientações da EMERJ.
- 2.1.4 Deverá ser fornecido suporte técnico e garantia para os equipamentos pelo prazo de 24 (vinte e quatro) meses.
- 2.1.5 O certame será dividido em 2 (dois) lotes segundo segue abaixo:
 - 2.1.5.1 O Lote 1 conterá os serviços descritos nos itens 2.1.1, 2.1.2 e 2.1.3.
 - 2.1.5.2 O Lote 2 conterá o serviço descrito no item 2.1.4.

- 2.1.6 Os serviços serão prestados nas dependências da Escola da Magistratura do Estado do Rio de Janeiro – EMERJ, em sua sede, situada na rua Dom Manuel, 25, Centro, Rio de Janeiro além da Biblioteca, situada na Rua Dom Manuel, 37, 1º andar.

2.2 Do Ambiente Tecnológico da EMERJ

- 2.2.1 O ambiente de tecnológico da CONTRATANTE, no que diz respeito à rede Wi-Fi, compreende os seguintes itens:
- 2.2.1.1 29 (vinte e nove) Access Points do fabricante Ruckus – modelo 7341;
 - 2.2.1.2 01 (um) Switch Controller Ruckus modelo ZoneDirector 3000;
 - 2.2.1.3 01 (um) Switch Cisco modelo catalyst 2960-S.
- 2.2.2 Poderão ser agendadas visitas técnicas ao ambiente da CONTRATANTE a fim de sanar qualquer dúvida, pelo telefone (21) 3133-1880.

2.3 Bem/Serviço

- 2.3.1 Para fins desta contratação deverão ser fornecidos pela CONTRATADA os seguintes serviços:

2.3.1.1 Lote 1:

- 2.3.1.1.1 01 (um) Serviço de conexão com a internet de 30 Mbps full duplex;
- 2.3.1.1.2 01 (um) serviço de gerenciamento da rede Wireless.
- 2.3.1.1.3 01 (um) serviço de segurança de acesso à internet UTM.

2.3.1.2 Lote 2:

- 2.3.1.2.1 01 (um) serviço de Suporte Técnico e Garantia dos Equipamentos da Contratante.

Valor Estimado

Lote 1		
Serviço	Valor Mensal	Valor total (24 meses)
Serviço de conexão com a internet de 30 Mbps full duplex	R\$ 6.280,00	R\$ 150.720,00
Serviço de gerenciamento da rede Wireless	R\$ 5.735,00	R\$ 137.640,00
Serviço de segurança de acesso à internet UTM	R\$ 5.141,00	R\$ 123.384,00
Total	R\$ 17.156,59	R\$ 411.744,00

Lote 2		
Serviço	Valor Mensal	Valor total (24 meses)
Suporte Técnico e Garantia para os equipamentos da Contratante	R\$ 5.760,50	R\$ 138.254,08
Total	R\$ 5.760,50	R\$ 138.254,08

O valor total estimado para a presente contratação é de R\$ 549.998,08 (quinhentos e quarenta e nove mil, novecentos e noventa e oito reais e oito centavos).

3 ESPECIFICAÇÃO TÉCNICA DOS SERVIÇOS

3.1 Especificações globais da solução

- 3.1.1 Todos os equipamentos e circuitos de comunicação de dados deverão ser fornecidos em regime de comodato pela CONTRATADA, que também será responsável pela sua manutenção, reparo e/ou troca, garantindo, assim, o perfeito funcionamento do sistema;
- 3.1.2 Os serviços que compõe o objeto deste termo de referência deverão ser implantados em até 90 (noventa) dias corridos a partir do memorando de início da contratação.
- 3.1.3 A implantação da solução de UTM deverá ocorrer em no máximo 15 dias após a instalação da internet;
- 3.1.4 O prazo de contrato será de 24 (vinte e quatro) meses a partir da assinatura do memorando de início da contratação;
- 3.1.5 Em até 48 (quarenta e oito) horas após a assinatura do contrato, a CONTRATADA deverá apresentar projeto executivo detalhado, o qual deverá conter o cronograma pormenorizado de implantação e ativação dos sistemas bem como os detalhes de configuração da solução para que seja apreciado e aprovado pela CONTRATANTE;
 - 3.1.5.1 O Projeto Executivo deverá conter detalhes sobre o método de autenticação proposto pela CONTRATADA.
- 3.1.6 Caso o projeto não seja aprovado, a CONTRATADA terá 5 dias úteis para apresentar novo projeto de acordo com as orientações da CONTRATANTE;
- 3.1.7 O prazo de que trata o item anterior poderá ser dilatado a critério da CONTRATANTE;
- 3.1.8 Todos os equipamentos de comunicação de dados, com exceção dos que já pertencem à CONTRATANTE, deverão ser fornecidos, em regime de comodato, pela CONTRATADA, que também será responsável pela manutenção dos mesmos, garantindo, assim, o perfeito funcionamento do sistema;
- 3.1.9 O item acima inclui, também, os equipamentos relativos a solução de UTM;
- 3.1.10 O Índice de Disponibilidade Mensal (IDM) dos serviços de que trata os itens 2.3.1.1.1, 2.3.1.1.2 e 2.3.1.1.3 deverá ser de 99,9%, excluídas as paradas para realização de intervenções programadas, hipóteses

decorrentes de caso fortuito e/ou força maior ou ainda qualquer outro evento fora do controle da empresa, como atos de vandalismo e/ou furto;

- 3.1.11 O Suporte técnico e a garantia de que trata o item 2.3.1.2.1 deverá ser prestado dentro de 24 (vinte e quatro horas) a partir da abertura do chamado;
- 3.1.12 A solução apresentada para o Lote 1 deverá fornecer completa segurança para o ambiente da CONTRATANTE, garantindo o controle total do tráfego de informações na rede.
- 3.1.13 A prestação do serviço deverá permitir, já no final da sua instalação, a conexão simultânea de no mínimo 1000 (um mil) usuários.
- 3.1.14 Os serviços constantes dos itens 2.3.1.1.2 e 2.3.1.1.3 deverão contemplar treinamento para 03 (três) profissionais da DETEC, órgão Fiscal do Contrato.
- 3.1.15 A prestação do serviço contemplará a operação de suporte e gerenciamento pró-ativo 24x7 de toda a rede wi-fi da CONTRATANTE, já implantada, com equipamentos de sua propriedade.
- 3.1.16 A CONTRATADA deverá arcar com todas as despesas referentes ao transporte vertical e horizontal, bem como carga e descarga, de todos os bens que compõem o objeto desta contratação, necessária à implantação dos seus serviços componentes;
- 3.1.17 As CONTRATADAS deverão colocar à disposição da CONTRATANTE uma Central de Atendimento Especializado, com número telefônico único não tarifado (0800), para registros dos chamados, operando, no caso do Lote 1, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, todos os dias do ano e, no caso do Lote 2, mínimo de 8 (oito) horas por dia, 5 dias por semana;
- 3.1.18 As Centrais de Atendimento Especializado deverão manter um sistema de registro, acompanhamento dos chamados, esclarecimentos de dúvidas, compreendendo desde o registro até a resolução do fato motivador do chamado e permitindo inclusive o acesso a essas informações pelo Órgão Fiscal;
 - 3.1.18.1 Caso uma única licitante seja a arrematante dos dois lotes, a Central de Atendimento poderá ser a mesma.
- 3.1.19 Para fins de gestão, a(s) prestadora(s) de serviço deverá(ão) disponibilizar à CONTRATANTE os seguintes relatórios:
 - 3.1.19.1 Chamados ou conjunto de chamados abertos dentro e fora do prazo, fechados e encerrados dentro e fora do prazo, e de reincidência de problemas;
 - 3.1.19.2 Relatórios de disponibilidade, tráfego disponibilizados mensalmente (apenas para o Lote 1);
 - 3.1.19.3 Relatórios de utilização e performance (apenas para o Lote 1);
- 3.1.20 Todos os relatórios de que tratam o item anterior deverão ser disponibilizados de forma online, com estatísticas diárias, semanais e mensais.
- 3.1.21 O atendimento a solicitações de Órgão Fiscal deverá ser realizado pela(s) equipe(s) técnica(s) da(s) CONTRATADA(S) no prazo de até 4 (quatro) horas, em casos de interrupções totais do serviço e em até 24 (vinte e quatro) horas, em caso de interrupções parciais ou variações na qualidade da prestação do serviço.
- 3.1.22 A(s) CONTRATADA(S) deverá(ão) solicitar ao Órgão Fiscal interrupções programadas para a realização de manutenções preventivas e/ou corretivas, por escrito, com no mínimo 48 (quarenta e oito) horas de antecedência.
- 3.1.23 Qualquer manutenção e/ou intervenção, mesmo não implicando inoperância dos serviços ou alteração nas suas características, deverá ser agendada e acordada previamente com o órgão fiscal;
- 3.1.24 As interrupções preventivas devem ser realizadas, em regra, no horário que não comprometa as atividades da CONTRATANTE;
- 3.1.25 Em caso de falha e/ou inoperância de qualquer sistema, enlace e/ou equipamento de sua propriedade que impacte na prestação dos serviços, a CONTRATADA deverá abrir uma ocorrência técnica independente de solicitação do órgão fiscal, após a constatação do problema e dar ciência ao mesmo;
- 3.1.26 Uma vez verificada falha na prestação do serviço por responsabilidade da CONTRATADA, será concedido um desconto correspondente ao número de horas ou fração superior a trinta minutos de serviço interrompido ou degradado;
- 3.1.27 Para efeito do aludido desconto, será considerado o lapso temporal entre a abertura do chamado técnico de indisponibilidade do serviço e/ou circuito até a sua total recuperação.

3.2 Especificações do serviço de Internet (Lote 1)

- 3.2.1 O serviço de internet deverá permitir a conexão dedicada à internet com a velocidade mínima de 30 Mbps.

- 3.2.2 O circuito a ser contratado deverá ser implementado através de enlace dedicado ponto a ponto ou metro ethernet, e meio físico por fibra ótica ou rádio frequência oferecida pela operadora, interligando a rede Wi-Fi da EMERJ à internet pública.
- 3.2.3 Caso a escolha da implementação de que trata o item anterior seja feita por radiofrequência, dever-se-á levar em conta que o prédio que abriga a Escola da Magistratura do Estado do Rio de Janeiro, é tombado pelo patrimônio Histórico, logo deverão ser tomadas todas as precauções possíveis para que as antenas não fiquem aparentes.
- 3.2.4 O serviço de internet deverá ser prestado de forma ininterrupta, 24 (vinte e quatro) horas por dia, 7(sete) dias por semana.
- 3.2.5 O serviço de acesso à internet fornecido pela CONTRATADA deverá possuir backbone com rotas diferenciadas.
- 3.2.6 A EMERJ poderá a qualquer momento solicitar diligências de caráter técnico visando comprovar as características do item acima;
- 3.2.7 Sempre que for verificada a falha, a empresa deverá prover a dupla abordagem física no prazo máximo de 15 (quinze) dias, sem prejuízo das penalidades cabíveis.
- 3.2.8 A taxa máxima de transmissão (upload) deverá ser igual à taxa máxima de recepção (download), com 100% de banda garantida.
- 3.2.9 Todos os equipamentos e o circuito de comunicação de dados serão fornecidos pela CONTRATADA, em regime de comodato, nas suas condições de fabricação, operação, manutenção, configuração, funcionamento, alimentação e instalação, deverão obedecer rigorosamente às normas e recomendações em vigor elaboradas pelos Órgãos oficiais competentes:
 - 3.2.9.1 ABNT (Associação Brasileira de Normas Técnicas) e ANATEL (Agência Nacional de Telecomunicações);
 - 3.2.9.2 Entidades internacionais de padronização – ITU-T (International Telecommunication Union), ISO (International Standardization Organization), IEEE (Institute of Electrical and Electronics Engineers), EIA/TIA (Electronic Industry Alliance and Telecommunication Industry Association).

Roteador de Internet

- 3.2.10 O roteador de internet deverá ser dimensionado de forma a garantir o desempenho e os níveis de serviço requeridos para o tráfego do serviço contratado, com utilização máxima de CPU a 75% de sua capacidade;
- 3.2.11 O roteador deverá suportar o padrão IEEE 802.1p/IEEE 802.1d, permitindo assim a configuração de parâmetros de qualidade de serviço (QoS);
- 3.2.12 O roteador instalado deverá suportar gerência SNMP, versões 1, 2 e 3, e suportar a especificação MIB-II, implementados em conformidade com as RFCs 1157, 1213 e 2570;
- 3.2.13 Sempre que houver lançamento de uma nova versão de sistema operacional e/ou “firmware” que faça correção de segurança e atualização de serviços, poderá ser solicitada pelo TJERJ, à CONTRATADA, a atualização do sistema operacional e/ou “firmware” do roteador instalado. Nesse caso, a CONTRATADA terá 7 (sete) dias corridos para realizar as atualizações solicitadas, sem nenhum ônus para o EMERJ;
- 3.2.14 A CONTRATADA deverá fornecer a EMERJ as senhas de acesso, via porta de console, para o roteador instalado com privilégio de leitura para toda a configuração do equipamento, a fim de que possa ser verificado se está de acordo com os termos do contrato, a qualquer tempo. Também deverá ser fornecido acesso somente de leitura às variáveis SNMP (comunidade de leitura ou usuário/senha). Opcionalmente, a pedido do EMERJ, a CONTRATADA poderá configurar o roteador para gerar logs (Syslog RFC 3164) ou traps SNMP para um ou mais endereços IP;
- 3.2.15 Os roteadores instalados na EMERJ deverão estar configurados para permitir acesso remoto através de SSH v2, ficando por conta da CONTRATADA o fornecimento de todos os recursos necessários à configuração remota, sempre sem nenhum ônus para a EMERJ;
- 3.2.16 O roteador instalado deverá possuir internamente, sem adição de placas ou módulos adicionais, o Hardware necessário para a aceleração de criptografia dos protocolos IPSEC e SSL (Secure Sockets Layer);
- 3.2.17 O roteador instalado deverá possuir no mínimo 03 (três) slots livres para adição de módulos para interfaces WAN, e 04 (quatro) slots para módulos de serviço;
- 3.2.18 O roteador instalado deverá possuir no mínimo 01 (um) GB de memória DRAM instalada, e no mínimo 256 (duzentos e cinquenta e seis) MB de memória FLASH;
- 3.2.19 O roteador instalado deverá possuir no mínimo 02 (duas) interfaces USB do tipo A;
- 3.2.20 O roteador instalado deverá possuir uma interface RS-232 para acesso console, de até 115.200 kbps, o cabo necessário para o acesso ao roteador deve ser fornecido;

- 3.2.21 O roteador instalado deverá possuir uma interface USB Tipo B, para os fins de acesso a console do equipamento, o cabo necessário à interligação do roteador deve ser fornecido;
- 3.2.22 O roteador deverá ser fornecido com Fontes (Power Supply) redundantes, que operem na faixa de 100 a 240 VAC, e que forneçam no mínimo a potência de 420 W (watts) para os equipamentos;
- 3.2.23 Para efeito de referência devem ser considerados os seguintes serviços concorrentes para o roteador: NAT, QoS, Access Control Lists (ACLs);
- 3.2.24 O roteador deverá suportar os protocolos de roteamento RIPv2 (RFC 2453) e OSPF v2 (RFC 2328) e BGP (RFCs 4271 e 1771).

3.3 Especificações do serviço de Gerenciamento da Rede Wi-Fi (Lote 1)

- 3.3.1 A CONTRATADA deverá gerenciar a solução de Wi-Fi Instalada nas dependências da EMERJ;
- 3.3.2 Deverá ser fornecida uma forma de comunicação sem ônus adicional para a EMERJ;
- 3.3.3 A CONTRATADA deverá prover ferramenta de gerenciamento via WEB, para monitoramento do funcionamento do ambiente, que informe o seu status operacional e de desempenho, a qual deverá ter visão compartilhada com a equipe do Serviço de Monitoramento do CONTRATANTE;
- 3.3.4 A ferramenta de gerenciamento deverá fornecer relatórios que permitam ao CONTRATANTE o acompanhamento dos níveis do serviço fornecido, contendo, pelo menos, as seguintes informações: Índice de disponibilidade, global e por localidade de instalação; Consumo de banda global e por localidade de instalação, Número de acessos mensal global e por localidade de instalação, Natureza de conteúdo acesso Global e por localidade de instalação;
- 3.3.5 Deverá ser garantida ao usuário experiência em nível de Banda Larga residencial, a fim de que estes possam consultar páginas Web dinâmicas e estáticas, assistir vídeos, enviar e receber e-mails e fazer download e upload de arquivos;
- 3.3.6 Deverão haver reuniões ENTRE o Gestor, o Fiscal do Contrato e o Preposto da CONTRATADA para avaliação do serviço prestado no período e verificação do atendimento aos requisitos contratuais estabelecidos, com periodicidade a ser definida pelo Gestor do Contrato;
- 3.3.7 O tempo de disponibilidade do serviço deverá ser de 99,9% do tempo, tendo como referência o período de minutos mensais;
- 3.3.8 Os índices de serviço deverão ser informados através de relatórios mensais emitidos pela CONTRATADA e encaminhados ao Gestor e Fiscal Técnico do Contrato.
- 3.3.9 O prazo máximo de resolução de interrupção do serviço ou de degradação de seu desempenho é de 4 (quatro) horas, iniciando-se com a abertura do chamado pela CONTRATADA, ou alarme de ferramenta de gerenciamento identificado pela mesma ou pela CONTRATANTE, compreendendo o atendimento e resolução do problema;
- 3.3.10 A solução fornecida e gerenciada pela CONTRATADA deverá ser configurada segundo as orientações da CONTRATANTE.

3.4 Do suporte técnico e garantia dos equipamentos da CONTRATANTE (Lote 2).

- 3.4.1 A CONTRATADA deverá fornecer suporte técnico e garantia total aos equipamentos da CONTRATANTE descrito nos itens 2.2.1.1, 2.2.1.2 e 2.2.1.3 durante toda a vigência do contrato;
- 3.4.2 O Suporte técnico e a garantia de que trata o item 2.3.1.2.1 deverá ser prestado dentro de 24 (vinte e quatro horas) a partir da abertura do chamado;
- 3.4.3 Em caso de defeito nos equipamentos descritos no item acima, deverão ser substituídos por equipamentos de igual modelo ou superiores, compatíveis com a solução, até que sejam feitos os reparos sem ônus adicional para a EMERJ.
- 3.4.4 O reparo do(s) equipamento(s) avariado(s) deverá(ão) ser de responsabilidade da CONTRATADA;
- 3.4.5 Caso não haja possibilidade de conserto, a CONTRATADA deverá prover a troca, em caráter permanente, do(s) equipamento(s) avariado(s) por equipamento(s) idêntico(s) ou superior(es) e, compatíveis com a solução sem ônus para a EMERJ;
- 3.4.6 Segue abaixo a lista de equipamentos pertencentes à CONTRATANTE:

Switch		
Part Number	S/N	Fabricante
WS-C2960S-48FPS-L	FOC1616X3LJ	CISCO

Controlador Wireless		
Part Number	S/N	Fabricante
909-3050-ZD00	351108000120	Ruckus Wireless

Access Points		
Part Number	S/N	Fabricante
901-7341-ZD00	331104004455	Ruckus Wireless
901-7341-ZD00	331104005241	Ruckus Wireless
901-7341-ZD00	341104000015	Ruckus Wireless
901-7341-ZD00	521104009336	Ruckus Wireless
901-7341-ZD00	331104005246	Ruckus Wireless
901-7341-ZD00	341104000016	Ruckus Wireless
901-7341-ZD00	521104009328	Ruckus Wireless
901-7341-ZD00	521104009319	Ruckus Wireless
901-7341-ZD00	331104005181	Ruckus Wireless
901-7341-ZD00	521104009331	Ruckus Wireless
901-7341-ZD00	331104005248	Ruckus Wireless
901-7341-ZD00	331104005244	Ruckus Wireless
901-7341-ZD00	521104009329	Ruckus Wireless
901-7341-ZD00	521104009180	Ruckus Wireless
901-7341-ZD00	521104009260	Ruckus Wireless
901-7341-ZD00	521104009327	Ruckus Wireless
901-7341-ZD00	331104005051	Ruckus Wireless
901-7341-ZD00	521104009338	Ruckus Wireless
901-7341-ZD00	521104009324	Ruckus Wireless
901-7341-ZD00	521104009342	Ruckus Wireless
901-7341-ZD00	521104009207	Ruckus Wireless
901-7341-ZD00	521104008305	Ruckus Wireless
901-7341-ZD00	521104009341	Ruckus Wireless
901-7341-ZD00	521104009203	Ruckus Wireless
901-7341-ZD00	521104009335	Ruckus Wireless
901-7341-ZD00	521104009330	Ruckus Wireless
901-7341-ZD00	521104009325	Ruckus Wireless
901-7341-ZD00	521104009198	Ruckus Wireless
901-7341-ZD00	521104009194	Ruckus Wireless

3.5 Especificações da Solução de Firewall UTM (Lote 1).

- 3.5.1 A solução deverá ser fornecida em Appliance de Firewall stateful packet inspection com capacidade de deep packet inspections para a filtragem de tráfego IP.
- 3.5.2 A solução de que trata em item anterior deverá vir embarcada em appliance compatível com rack 19", não sendo aceitas soluções baseadas em PC de uso geral ou soluções que contenham componentes do tipo acionadores de discos rígidos ou flexíveis;
- 3.5.3 A solução deverá possuir nativamente recursos de filtro de conteúdo e de inspeção, de antivírus e antispware de gateway e IPS, a fim de detectar e prevenir a ocorrência de spyware, vírus, trojans e worms, intrusões, vulnerabilidades de protocolos, sistemas operacionais e aplicativos servidores, nos protocolos SMTP, POP3, IMAP, HTTP e FTP, através de assinaturas, em tempo real, com quantidade de downloads simultâneos em número igual ao de conexões suportadas pelo equipamento;
- 3.5.4 A solução deve atualizar automaticamente as assinaturas de vírus e spyware e IPS sem a necessidade de intervenção humana;
- 3.5.5 A solução deve fornecer suporte a VPN IPsec, incluindo criptografia DES-56 bits, 3DES-168 bits, AES-128 e AES-256, com capacidade de implementar topologias site-to-site e cliente-to-site;
- 3.5.6 A solução deve possuir recursos capazes de detectar e evitar automaticamente IP source spoofing, IP source routing, túnel IPsec e ataques tipo DOS (denial-of-service) e DDOS (distributed denial-of-service) como Ping of Death;
- 3.5.7 A solução deve implementar recursos de NAT (network address translation) tipo one-to-one, one-to-many, many-to-one, e tradução simultânea de endereço IP, porta TCP de conexão (NATP), e NAT transversal em VPN IPsec;
- 3.5.8 Deve possuir servidor de DHCP (dynamic host configuration protocol) interno com capacidade de alocação de endereçamento IP para as estações conectadas às interfaces do firewall e em VPN e detecção de duplicação de endereços;

- 3.5.9 A solução deve possibilitar a aplicação de regras de firewall e IPS por IP e grupo de usuários permitindo a definição de regras para determinado horário ou período (dia da semana e hora) com matriz de horários que possibilite o bloqueio de serviços em horários específicos, tendo o início e fim das conexões vinculadas a essa matriz de horários;
- 3.5.10 Deve permitir a utilização de regras de antivírus, antispware, IDS e IPS e filtro de conteúdo por segmentos de rede. Todos os serviços devem ser suportados no mesmo segmento de rede ou VLAN;
- 3.5.11 Deve ser capaz, já no momento da implantação, de inspecionar e bloquear em tempo real aplicativos e transferências de arquivos de software p2p (peer-to-peer);
- 3.5.12 A solução deve ser capaz de detectar e bloquear, no mínimo, 2000 (duas mil) assinaturas de malware;
- 3.5.13 Deve possuir mecanismo que limite o número máximo de conexões simultâneas de uma mesma origem;
- 3.5.14 Deve possuir validação completa da sintaxe de toda sinalização de VoIP e pacotes de streams de mídia (para assegurar que pacotes mal-formados não possam passar pelo *firewall* e afetar adversamente o destinatário da comunicação);
- 3.5.15 Deve Suportar endereçamento na interface de *WAN* por *PPPOE* (*Point-to-point Protocol Over Ethernet*), IP estático e dinâmico, por *DHCP* e *PPTP* (*point-to-point tunneling protocol*) ou, no caso deste último, outro protocolo reconhecidamente mais seguro;
- 3.5.16 Permitir alta disponibilidade das interfaces *WAN* nas modalidades ativo-ativo (balanceamento) e ativo-passivo (redundância);
- 3.5.17 Deve, possuir capacidade de definição de múltiplas regiões de segurança no *firewall*, com objetos e regras de acesso distintas;
- 3.5.18 Deve permitir a definição de objetos como grupo de usuários, redes ou serviços de modo que, quando a política de segurança mudar, o administrador possa modificar o objeto pré-definido e propagar as mudanças instantaneamente sem necessidade de redefinir as regras;
- 3.5.19 Deve permitir a restrição de arquivos por sua extensão e bloqueio de anexos através de protocolos *SMTP* e *POP3* baseado em seus nomes;
- 3.5.20 Deve possuir gerenciamento de banda de entrada e saída, e classes de serviço por *DSCP* (*differentiated services code points*);
- 3.5.21 Possuir recurso de balanceamento de links *WAN*, sendo possível definir um valor que represente a quantidade de link disponível;
- 3.5.22 A solução deve possuir mecanismo que possibilite o funcionamento transparente dos protocolos *FTP*, *SIP*, *RTSP* e *H.323*, mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para acessos de dentro para fora quanto de fora para dentro;
- 3.5.23 Possuir suporte ao protocolo *SNMP*, através de *MIBs*;

Autenticação

- 3.5.24 A solução deve prover autenticação de usuários para os serviços *TELNET*, *FTP* e *HTTP*;
- 3.5.25 Deve permitir a autenticação dos usuários utilizando servidores *LDAP*, *AD* e *RADIUS*;
- 3.5.26 Deve permitir o cadastro manual dos usuários e grupos diretamente no *firewall* por meio da interface de gerência remota do equipamento;
- 3.5.27 Deve permitir a integração com qualquer autoridade certificadora emissora de certificados X.509 que siga o padrão de *PKI* descrito na *RFC 2459*, inclusive verificando os certificados expirados/revogados, emitidos periodicamente pelas autoridades certificadoras, os quais devem ser obtidos automaticamente pelo firewall;
- 3.5.28 Deve permitir aos usuários o uso de seu perfil independentemente do endereço IP da máquina que o usuário esteja utilizando;
- 3.5.29 A solução deve permitir a atribuição de perfil por faixa de endereço IP nos casos em que a autenticação não seja requerida;
- 3.5.30 A solução deve suportar padrão *IPSec*, de acordo com as *RFC 2401* a *2412*, de modo a estabelecer canais de criptografia com outros produtos que também suportem tal padrão;
- 3.5.31 Deve também suportar a criação de túneis seguros sobre IP (*IPSec tunnel*), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet;

Do controle de conteúdo da Web:

- 3.5.32 A solução deve permitir a classificação dinâmica de sites web, URLs e domínios;
- 3.5.33 Deve também permitir a reclassificação de sites;
- 3.5.34 Deve controlar conteúdo filtrado por categorias de sites com base de dados diariamente atualizada pelo fabricante;
- 3.5.35 A solução deverá filtrar no mínimo conteúdo sobre os assuntos listados abaixo:
 - 3.5.35.1 Violência;
 - 3.5.35.2 Pornografia;
 - 3.5.35.3 Armas;
 - 3.5.35.4 Drogas;
 - 3.5.35.5 Comportamento ilegal;
 - 3.5.35.6 Jogos;
 - 3.5.35.7 Conteúdo adulto;
 - 3.5.35.8 Entretenimento;
 - 3.5.35.9 Chat;
 - 3.5.35.10 Web Mail;
 - 3.5.35.11 Jogos de Azar;
 - 3.5.35.12 Navegação anônima;
 - 3.5.35.13 Newsgroups;
 - 3.5.35.14 Encontros pessoais;
 - 3.5.35.15 Streaming de músicas e vídeos.
- 3.5.36 Os assuntos de que tratam os itens 3.5.35.1 a 3.5.35.15 serão bloqueados e/ou permitidos a critério da EMERJ.
- 3.5.37 A solução deve permitir a associação de grupos de usuários a diferentes regras de filtragem de sites web, definindo quais categorias deverão ser bloqueadas ou permitidas para cada grupo de usuários, podendo ainda adicionar ou retirar acesso a domínios específicos da Internet;
- 3.5.38 Deve permitir a definição de quais zonas de segurança terão aplicadas as regras de filtragem de web;

Dos requisitos para administração

- 3.5.39 A solução deve permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o firewall, com no mínimo dois níveis de permissão: total e apenas leitura;
- 3.5.40 Deve permitir a visualização e o gerenciamento em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall, por serviços e endereços IP;
- 3.5.41 Deve possibilitar o controle do tráfego, pelos endereços de origem e destino;

Dos requisitos de LOG

- 3.5.42 A solução deve prover mecanismo de consulta às informações registradas integrado à interface de administração;
- 3.5.43 A solução deve possibilitar a análise dos seus registros (LOGs) por pelo menos um programa analisador de LOG disponível no mercado;
- 3.5.44 Deve possuir mecanismo que permita inspecionar o tráfego de rede em tempo real (sniffer) via interface gráfica, possibilitando exportar os dados visualizados para arquivo formato PCAP e permitindo a filtragem dos pacotes por protocolo, endereço IP de origem, endereço IP de destino, porta TCP de origem e porta TCP de destino;
- 3.5.45 Deve permitir a visualização do tráfego de rede em tempo real tanto nas interfaces de rede do firewall quando nos pontos internos do mesmo.

3.6 Das Sanções

3.6.1 Multa sob forma de desconto pelo não atingimento dos índices de disponibilidade dos Serviços descritos nos itens 2.3.1.1.1, 2.3.1.1.2 e 2.3.1.1.3.

3.6.1.1 O Cálculo da disponibilidade obedecerá a seguinte equação matemática:

$$IDM = \left(\frac{TTM - TTIEM}{TTM} \right) * 100$$

Onde:

- TTIEM: Tempo Total de Interrupção do serviço em minutos no Mês
- IDM(%): Disponibilidade Mensal Atingida
- TTM: Total de minutos do Mês de referência

3.6.1.2 A multa por não cumprimento do Índice de Disponibilidade Mensal (IDM) conforme o item 3.1.10 será aplicada segundo a tabela abaixo.

IDM		Multa
De	até	
99,80 %	99,89%	5 %
99,60 %	99,79%	10 %
99,50 %	99,59%	15 %
Abaixo de 99,39%		20 %

3.6.1.3 Os percentuais de multa estipulados no item anterior incidirão sobre todo o valor mensal do contrato caso haja impossibilidade de acesso à internet, seja qual for o problema que o ocasionou.

3.6.1.4 Caso a indisponibilidade de qualquer dos serviços não impeça a utilização da internet, a multa deverá ser cobrada em cima de 25% do valor mensal pago pela EMERJ por serviço indisponível.

3.6.2 Após o prazo estipulado no item 3.1.11 haverá o desconto de 1% em cima do valor mensal do contrato a cada dia de atraso no atendimento.

CHEFE DO SERVIÇO DE COMPRAS

DIRETOR (A) DO DEPARTAMENTO DE ADMINISTRAÇÃO

MATRÍCULA:

MATRÍCULA: