



CONVITE Nº 32/2011

DATA E HORÁRIO PARA RECEBIMENTO E ABERTURA DOS ENVELOPES

Dia 21 / 11 / 2011 às 15 horas

01. DISPOSIÇÕES INICIAIS

- 1.1 O Senac – **Departamento Nacional** torna público que, na Seção de Material, localizada na Av. Ayrton Senna, 5.555, bloco B, sala 101 – Barra da Tijuca – Rio de Janeiro – RJ – CEP 22.775-004, serão abertos os envelopes contendo os Documentos para Habilitação e as *Propostas Comerciais* para o objeto desta licitação, conforme especificações constantes do(s) **anexo(s) I** na presença facultativa dos representantes **credenciados** das empresas interessadas, **na forma do modelo anexo II**.
- 1.2 Quando, por motivo de suspensão do expediente no **Senac - Departamento Nacional**, não se realizar o ato do recebimento e abertura dos envelopes que contêm os documentos e as propostas relativas à presente licitação, fica acordado que a realização do mesmo ocorrerá, no horário já estabelecido, no primeiro dia útil posterior à data fixada neste *Convite*.
- 1.3 A presente licitação na modalidade *Convite*, do tipo menor preço, será regida unicamente pela Resolução *Senac 845/2006, publicada na Seção 3, páginas 1001 a 103 do D.O.U. de 23/02/2006*, autorizada no(s) Pedido(s) de Compra 7028.
- 1.4 O Senac é uma instituição de direito privado, nos termos da Lei Civil, cabendo sua organização e direção à Confederação Nacional do Comércio de Bens, Serviços e Turismo.
- 1.5 Somente poderão participar do presente *Convite* as empresas habilitadas no objeto desta licitação, não sendo aceitas propostas enviadas por e-mail ou fac-símile.
- 1.6 Não poderão participar da presente licitação, dirigente ou funcionário do Senac - Departamento Nacional, empresas reunidas em consórcio, cooperativas e ainda empresas que não possuam sede ou filial na Cidade do Rio de Janeiro.
- 1.7 O objeto da presente licitação é a **Contratação de Solução de Segurança de Acesso à Internet**, conforme condições constantes do Anexo I deste Edital.
- 1.8 Fazem parte integrante deste Convite os seguintes anexos.
Anexo I – Condições para prestação do serviço.
Anexo II – Modelo de Credenciamento e Modelo de Aceitação das Condições.
Anexo III – Modelo de Contrato de Prestação dos Serviços.





02. DO ENVELOPE CONTENDO DOCUMENTOS PARA A HABILITAÇÃO (Envelope “A”)

- 2.1 As empresas licitantes deverão encaminhar os documentos de *Habilitação* abaixo relacionados, obrigatoriamente em envelope fechado no qual, externamente, deverá ser informado o nome da empresa licitante, o número e a data da presente licitação:
 - 2.1.1 Declaração, em papel timbrado da empresa licitante, de que recebeu e examinou, cuidadosamente, os **Documentos do Convite** e de ter integralmente compreendido e aceito as condições estabelecidas, **na forma do modelo constante do Anexo II**.
 - 2.1.2 Ato constitutivo, estatuto ou contrato social em vigor com as últimas alterações, devidamente registrado no órgão competente, em se tratando de sociedades comerciais, e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores.
 - 2.1.3 Cópia da carteira de identidade do representante legal da licitante.
 - 2.1.4 Prova de inscrição no Cadastro Nacional de Pessoas Jurídica (CNPJ).
 - 2.1.5 Prova de inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual.
 - 2.1.6 Prova de regularidade para com a fazenda federal, estadual e municipal do domicílio ou sede do licitante, na forma da lei.
 - 2.1.7 Prova de regularidade relativa à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço, no cumprimento dos encargos instituídos por lei.
 - 2.1.8 Apresentar, no mínimo, 1 (um) Atestado de Capacidade Técnica, emitido por empresa pública ou privada, em papel timbrado da empresa emitente, com data de emissão **não superior** a 180 (cento e oitenta) dias da data para recebimento e abertura dos envelopes de que trata esta **Licitação**, comprovando execução de serviço compatível com o objeto da licitação. O documento deverá conter o nome legível, endereço e telefone do emitente para que, a critério da Comissão Especial de Licitação, seja consultado
 - 2.1.9 Carta do fabricante dos equipamentos ofertados junto com o serviço, informando que a proponente é um parceiro autorizado;
- 2.2 Os documentos relacionados nos itens 2.1.2 ao 2.1.9 deverão ser apresentados em fotocópias legíveis e estarem devidamente atualizados e dentro dos respectivos prazos de validade, não sendo aceitos quaisquer tipo de protocolo ou guias de pagamento. À critério da Comissão, poderá ser solicitada a apresentação dos documentos originais.

03. DO ENVELOPE CONTENDO A PROPOSTA COMERCIAL (Envelope “B”)

- 3.1 A Proposta deverá, obrigatoriamente, ser apresentada em envelope lacrado, no qual, externamente deverá ser informado o nome da empresa licitante, o número e a data da presente licitação e, ainda, conter as informações e documentos abaixo relacionados:



- 3.1.1 Preço global para a execução dos serviços relacionados no **Anexo I**, incluindo, obrigatoriamente, todos os custos relativos a tributos, frete e demais despesas diretas e indiretas. Eventuais despesas com transporte e hospedagem que se façam necessárias para a execução dos serviços serão de responsabilidade da empresa contratada, sem quaisquer ônus para o Senac – Departamento Nacional.
- 3.1.2 Descrição clara e completa dos serviços a serem executados e sua forma de execução.
- 3.1.3 Prazo de validade das propostas de, no mínimo, 60 (sessenta) dias, a contar da data de abertura das mesmas.
- 3.1.4 Indicação do nome do banco, número da conta corrente e agência onde, caso a empresa seja declarada vencedora, será feito o crédito referente ao objeto desta licitação.

04. JULGAMENTO DAS PROPOSTAS

- 4.1 Será facultado à Comissão de Licitação, inverter o procedimento, abrindo primeiramente as propostas, classificando os proponentes, e só então abrindo o envelope de habilitação do licitante classificado em primeiro lugar
- 4.2 O julgamento das propostas será realizado pela Comissão Permanente de Licitação que, após a decisão, comunicará o resultado, por escrito, aos licitantes habilitados.
- 4.3 Será considerado vencedor o licitante que oferecer a proposta que atenda às exigências do presente Convite e que seja de **menor preço**.
- 4.4 Serão desclassificadas as Propostas que não atenderem a todas as exigências constantes deste Edital e seus Anexos.
- 4.5 Os recursos contra as decisões da Comissão Permanente de Licitação deverão ser encaminhados, através de correspondência em papel timbrado da empresa, à Diretoria de Administração e Recursos Humanos do **Senac – Departamento Nacional**, localizada na Avenida Ayrton Senna, 5555, Barra, Rio de Janeiro – RJ ou pelo fax (021) 2136.5689, no prazo de **2 (dois) dias úteis** após a comunicação do resultado da Habilitação ou do julgamento das Propostas.

05. DO CONTRATO

- 5.1 O proponente vencedor firmará com o **Senac - Departamento Nacional** contrato de prestação de serviços, pelo qual se obrigará a prestar os serviços objeto desta licitação, nas condições constantes do presente *Convite* e da proposta da empresa contratada.
- 5.2 O prazo para formalização do contrato será de até **05 (cinco) dias úteis**, a contar da data de homologação do resultado da licitação.

06. DO PAGAMENTO E REAJUSTE DE PREÇOS

- 6.1 O pagamento à empresa vencedora da presente licitação será efetuado pelo Senac - Departamento Nacional dentro de 15 dias após a entrega da Nota Fiscal Fatura, desde que os serviços tenham sido aceitos pelos técnicos do Senac - Departamento Nacional.
- 6.2 Os preços apresentados para a presente licitação serão fixos e irrevogáveis.



07. SUBCONTRATAÇÃO

O Senac - Departamento Nacional não aceitará, em nenhuma hipótese, subcontratação para prestação do objeto desta licitação.

08. DAS SANÇÕES EM CASO DE INADIMPLEMENTO

- 8.1 O inadimplemento, total ou parcial, por parte da empresa contratada, em relação às condições contratuais, acarretará as sanções abaixo:
 - 8.1.1 Perda do direito à contratação;
 - 8.1.2 Multa Administrativa, não excedente, em seu total, ao equivalente a 5 % (cinco por cento) do valor global do Contrato;
 - 8.1.3 Suspensão do direito de participação em licitação promovida pelo Senac - Departamento Nacional, por período de até 02 (dois) anos;
- 8.2 A critério do Senac - Departamento Nacional, as sanções poderão ser cumulativas.

9. ESCLARECIMENTOS DE DÚVIDAS

- 9.1 Até as 10 (dez) horas do dia 17/11/11, no endereço constante do item 1.1, através de correspondência dirigida à Comissão de Licitação, em papel timbrado da empresa licitante ou pelo fax (0XX21) 2136.5532/5689.

10. DAS DISPOSIÇÕES FINAIS

- 10.1 Os licitantes deverão examinar cuidadosamente os termos e condições do presente *Convite*, para que tenham ciência de todos os detalhes que possam afetar de algum modo o fornecimento objeto desta licitação.
- 10.2 Os envelopes contendo os **Documentos de Habilitação** e as **Propostas** poderão ser entregues antes da data de abertura, no endereço informado no item 1.1.
- 10.3 A Comissão Especial de Licitação poderá, a qualquer tempo, caso julgue necessário, realizar diligência para comprovar a veracidade das informações prestadas, o cumprimento das condições estabelecidas ou mesmo de idoneidade do **Licitante**, bem como promover retificação ou ratificação de documento já apresentado, a fim de corrigir falhas meramente formais, sendo vedada a inclusão de documento exigido que não tenha sido apresentado à época própria.
- 10.4 O Senac - Departamento Nacional se reserva o direito de adiar, cancelar, revogar, anular ou tornar sem efeito, no todo ou em parte a presente licitação
- 10.5 Em caso de desistência do licitante vencedor ou quando este não assinar o contrato, o licitante classificado em 2º (segundo) lugar poderá ser convocado, a critério do Departamento Nacional do Senac, para prestação dos serviços, objeto do presente contrato, no preço proposto pelo licitante vencedor, procedendo-se da mesma forma em relação aos demais licitantes remanescentes, por ordem de classificação, convocados pelo mesmo motivo constante neste item.



- 10.6 No caso de convocação de licitante classificado a partir do 2º (segundo) lugar, obedecida à ordem seqüencial e após o aceite do valor ofertado pelo 1º (primeiro) classificado, deverá o mesmo assinar o contrato, nos termos previstos neste Edital.
- 10.7 Todas as alterações no edital serão publicadas/divulgadas em nosso site de licitações: www.senac.br/licitacao.
- 10.8 Fica eleito o Foro Regional da Barra da Tijuca da Comarca do Rio de Janeiro/RJ, para dirimir quaisquer dúvidas referentes ao presente Edital.

Rio de Janeiro, 13 de outubro de 2011.

COMISSÃO PERMANENTE DE LICITAÇÃO

ANEXO I – CONVITE 32/2011

Condições para Prestação dos Serviços

1. PROPÓSITO

Contratação por 12 (doze meses), podendo ser renovável por iguais períodos até o máximo de 60 meses do serviço de segurança abrangendo mão de obra técnica, aluguel de hardware e software através de *appliance* para controle de acesso da rede, a internet e outros seguimentos de rede combinando com uma defesa proativa com funcionalidades de proteção acrescidas do direito à atualização de versões, suporte, conforme descrito neste Anexo.

2. JUSTIFICATIVA

Os problemas decorrentes da conexão de estações de trabalho de uma rede corporativa à Internet são, entre outros:

- Disseminação de vírus, *trojans* e *malware*;
- Acesso a informações privilegiadas (*phishing*);
- Propagação de códigos maliciosos para outros sistemas;
- Sobrecarga de estações de trabalho, servidores e canais de comunicação;
- Improdutividade dos colaboradores;
- Elevação dos custos de TI necessários para resolver os problemas gerados e manter os sistemas disponíveis;
- Comprometimento da imagem da instituição por acessos involuntários a sítios que veiculem informações ilegais ou imorais;
- Vazamento de informações sigilosas

Para minimizar os problemas elencados, o mercado oferece soluções de controle e proteção de acesso à Internet que, entre outros recursos, podem oferecer:

- Controle de acesso, através de regras e políticas, bem como o registro de sítios e páginas visitadas;
- Filtragem do conteúdo que pode ser acessado, a fim de impedir o tráfego de informações com sítios de conteúdo impróprio ou não relacionados, prioritariamente, a execução do serviço;
- Proteção do ambiente de TI contra vírus e códigos maliciosos contidos nas páginas visitadas e arquivos baixados;
- Filtro de palavras chaves ou arquivos para impedir o vazamento de informações;
- Controle da banda do link Internet, fazendo com que os serviços principais sejam priorizados;
- Redução do consumo do link Internet através das filtrações supracitadas;
- Redução dos links internos (interligação entre filiais) com os recursos de otimização de rede;
- Controle total e visibilidade sobre o tráfego de internet;
- Balanceamento de múltiplos links de dados;
- Aumento da disponibilidade dos negócios com o recurso de alta disponibilidade;
- Gerenciamento unificado de todas as soluções de segurança de borda.

3. OBJETO

Aluguel de solução dedicada de hardware e software, obrigatoriamente do mesmo fabricante composta por dois *appliances* (*conjunto de hardware e software*) conforme abaixo:



- Appliance para controle de acesso de rede, a internet e outros seguimentos de rede combinando com uma defesa proativa com funcionalidades de proteção em vários níveis e com mecanismos de alta velocidade na classificação de tráfego e inspeção de pacotes em tempo real, tanto de arquivos quanto a tráfego com base em conteúdo, independentemente da porta e do protocolo em uso. Produto sugerido: **Fortigate 200B + Módulo de Cache (ou similar)**.
- Appliance para disponibilização de relatórios gráficos com dados personalizáveis, permitindo filtros de registros vindos a partir do dispositivo de Appliance de Controle de Acesso de Rede e outros dispositivos compatíveis com o syslog, contemplando informações como tráfego, eventos, vírus, ataques, conteúdo Web, e-mails e ser capaz de permitir a criação de outros registros além dos citados. O mesmo deverá possuir gráficos personalizáveis, interface WEB e Administração baseada em perfis e capacidade de armazenamento de 1 TB. Produto sugerido: **FortiAnalyzer 100C (ou similar)**.

4. REQUISITOS

A solução de *appliances*, definido no OBJETO deste Convite, deve atender aos seguintes requisitos e funcionalidades, organizados por categorias, como segue:

- Firewall;
- VPN IPSec (Client-to-site e Site-to-site);
- VPN SSL;
- Detecção e Prevenção de Intrusos (IPS);
- Anti-X e/ou Anti-Malware e/ou Anti-Grayware;
- Funcionalidade de Traffic Shapping e/ou Qualidade de Serviço (QoS);
- Funcionalidade de Filtro de Conteúdo Web (URL Filtering);
- Antivírus;
- AntiSpam;
- Otimização de Wan;
- Controle de Aplicação;
- Prevenção contra perda/roubo/vazamento de informação (DLP);
- Funcionalidade de Controle da Rede sem fio.

Detalhamento Técnico de cada funcionalidade:

Item	Descrição
1.1.	Firewall baseado em <i>appliance</i> . Para maior segurança, não serão aceito equipamentos de propósito genérico (PCs ou servidores) sobre os quais podem instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN solaris, Apple OS-X o GNU/Linux.
1.2.	Possuir capacidade de processamento de pacotes e interfaces de acordo com a performance dos equipamentos desta especificação.
1.3.	Possuir controle de acesso à internet por endereço IP de origem e destino
1.4.	Possuir controle de acesso à internet por sub-rede
1.5.	Suporte a tags de VLAN (802.1q)
1.6.	Para equipamentos com desempenho maior que 1 Gbps de Firewall, o mesmo deverá suportar agregação de <i>links</i> , segundo padrão IEEE 802.3ad

1.7.	Possuir ferramenta de diagnóstico do tipo <i>tcpdump</i>
1.8.	Possuir integração com Servidores de Autenticação RADIUS, LDAP e Microsoft Active Directory.
1.9.	Possuir métodos de autenticação de usuários para os protocolos TCP (HTTP, HTTPS, FTP e Telnet).
1.10.	Possuir a funcionalidade de tradução de endereços estáticos – NAT (<i>Network Address Translation</i>), um para um, N-para-um e vários para vários.
1.11.	Permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana
1.12.	Permitir controle de acesso à internet por domínio, exemplo: gov.br, org.br, edu.br
1.13.	Possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT.
1.14.	Suporte a roteamento dinâmico RIP V1, V2, OSPF e BGP
1.15.	Possuir funcionalidades de DHCP Cliente, Servidor e Relay.
1.16.	Suportar aplicações multimídia como: H.323, SIP.
1.17.	Tecnologia de firewall do tipo Stateful
1.18.	Possuir possibilidade de alta disponibilidade (HA), trabalhando no esquema de redundância do tipo ativo-passivo e também ativo-ativo com divisão de carga, com todas as licenças de software habilitadas para tal.
1.19.	Deve permitir o funcionamento em modo transparente tipo “bridge”
1.20.	Permitir a criação de pelo menos 225 VLANS no padrão IEEE 802.1q
1.21.	Possuir conexão entre estação de gerencia e appliance criptografada tanto em interface gráfica quanto em CLI (linha de comando)
1.22.	Permitir filtro de pacotes sem controle de estado “stateless” para verificação em camada 2.
1.23.	Permitir forwarding de camada 2 para protocolos não IP.
1.24.	Suportar forwarding de multicast.
1.25.	Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP, UDP, ICMP e IP
1.26.	Permitir o agrupamento de serviços
1.27.	Permitir o filtro de pacotes sem a utilização de NAT
1.28.	Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas.
1.29.	Possuir mecanismo de anti-spoofing
1.30.	Permitir criação de regras definidas pelo usuário
1.31.	Permitir o serviço de autenticação para HTTP e FTP
1.32.	Deve permitir IP/MAC <i>binding</i> , permitindo que cada endereço IP possa ser associado a um endereço MAC gerando maior controle dos endereços internos e impedindo o IP <i>spoofing</i>
1.33.	O dispositivo deverá ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas, suportando ao menos: Yahoo! Messenger, MSN Messenger, ICQ, AOL Messenger, BitTorrent, eDonkey, GNUTella, KaZaa, Skype e WinNY.
1.34.	Permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (<i>inbound/outbound</i>) através da classificação dos pacotes (<i>Shaping</i>), criação de filas de prioridade, gerência de congestionamento e QoS.
1.35.	Permitir modificação de valores DSCP para o <i>DiffServ</i>

1.36.	Limitar individualmente a banda utilizada por programas de compartilhamento de arquivos do tipo peer-to-peer
1.37.	Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados
1.38.	Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP
1.39.	Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP
1.40.	Deverá controlar (limitar ou expandir) individualmente a banda utilizada por sub-rede de origem e destino
1.41.	Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino
1.42.	Funcionalidade de Antivírus
1.42.1.	Possuir funções de Antivírus, Anti-spyware
1.42.2.	Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, SMTP, IMAP, POP3 e FTP
1.42.3.	Possuir verificação de vírus para aplicativos de mensagens instantâneas (AIM, MSN, Yahoo Messenger, ICQ)
1.42.4.	Permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.)
1.42.5.	Permitir o bloqueio de download de arquivos por extensão, nome do arquivo e tipo de arquivo.
1.42.6.	Permitir o bloqueio de download de arquivos por tamanho
1.43.	Funcionalidade de Anti-spam
1.43.1.	Possuir verificação de a funcionalidade de anti-spam a verificação do cabeçalho SMTP do tipo <i>MIME</i>
1.43.2.	Possuir filtragem de e-mail por palavras chaves
1.43.3.	Permitir adicionar rótulo ao assunto da mensagem quando classificado como <i>SPAM</i>
1.43.4.	Possuir para a funcionalidade de Anti-Spam o recurso de RBL
1.43.5.	Permitir a checagem de reputação da URL no corpo mensagem de correio eletrônico
1.44.	Funcionalidade de Filtro de conteúdo Web
1.44.1.	Possuir solução de filtro de conteúdo web integrado a solução de segurança
1.44.2.	Possuir pelo menos 60 categorias para classificação de sites web
1.44.3.	Possuir base mínima contendo, 40 milhões de <i>sites</i> internet web já registrados e classificados
1.44.4.	Possuir a funcionalidade de cota de tempo de utilização por categoria
1.44.5.	Possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites web como: Proxy Anônimo; Webmail; Instituições de Saúde; Notícias; Phishing; Hackers; Pornografia; Racismo; Websites Pessoais; Compras;
1.44.6.	Permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários
1.44.7.	Permitir a criação de pelo menos 5 (cinco) categorias personalizadas
1.44.8.	Permitir a re-classificação de <i>sites</i> web, tanto por URL quanto por endereço IP
1.44.9.	Prover termo de Responsabilidade on-line para aceite pelo usuário, a ser apresentado toda vez que houver tentativa de acesso a determinado serviço permitido ou bloqueado
1.44.10.	Integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados
1.44.11.	Prover funcionalidade de identificação transparente de usuários cadastrados no

	Microsoft Active Directory
1.44.12.	Exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança da empresa
1.44.13.	Permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em <i>applets</i> Java, <i>cookies</i> , activeX através de: base de URL própria atualizável.
1.44.14.	Permitir o bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual
1.44.15.	Permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra
1.44.16.	Deverá permitir o bloqueio de URLs inválidas cujo o campo CN do certificado SSL não contém um domínio válido
1.44.17.	Filtro de conteúdo baseado em categorias em tempo real
1.44.18.	Garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo web
1.44.19.	Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP
1.44.20.	Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem
1.44.21.	Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem
1.44.22.	Deverá ser capaz de categorizar a página web tanto pela sua URL como pelo seu endereço IP
1.44.23.	Deverá permitir o bloqueio de redirecionamento HTTP
1.44.24.	Deverá permitir o bloqueio de páginas web por Classificação como páginas que facilitam a busca de Audio, Video e URLs originadas de Spam
1.44.25.	Deverá permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra
1.45.	Possuir capacidade de desempenho de acordo com a performance dos equipamentos desta especificação.
1.46.	Capacidade de detecção de mais de 200 ataques.
1.47.	O Sistema de detecção e proteção de intrusão deverá estar orientado à proteção de redes.
1.48.	Possuir tecnologia de detecção baseada em assinatura
1.49.	O sistema de detecção e proteção de intrusão deverá possuir integração à plataforma de segurança.
1.50.	Possuir capacidade de remontagem de pacotes para identificação de ataques
1.51.	Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server para que seja usado para proteção específica de Servidores Web;
1.52.	Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;
1.53.	Mecanismos de detecção/proteção de ataques:
1.53.1.	Reconhecimento de padrões
1.53.2.	Análise de protocolos
1.53.3.	Detecção de anomalias
1.53.4.	Detecção de ataques de RPC (Remote procedure call)
1.53.5.	Proteção contra ataques de Windows ou NetBios
1.53.6.	Proteção contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet

	Message Access Protocol, Sendmail ou POP (Post Office Protocol)
1.53.7.	Proteção contra ataques DNS (Domain Name System)
1.53.8.	Proteção contra ataques a FTP, SSH , Telnet e rlogin
1.53.9.	Proteção contra ataques de ICMP (Internet Control Message Protocol).
1.54.	Métodos de notificação:
1.54.1.	Alarmes na console de administração.
1.54.2.	Alertas via correio eletrônico.
1.55.	Monitoração do comportamento do appliance mediante SNMP, o dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede.
1.56.	Capacidade de resposta/logs ativa a ataques
1.56.1.	Terminação de sessões via TCP resets.
1.56.2.	Armazenamento de logs de sessões
1.57.	Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos
1.58.	O Sistema de detecção de Intrusos deverá mitigar os efeitos dos ataques de negação de serviços.
1.59.	Deverá permitir a criação de assinaturas personalizadas.
1.60.	Possuir filtros de ataques por anomalias
1.61.	Permitir filtros de anomalias de tráfego estatístico de: <i>flooding</i> , <i>scan</i> , <i>source</i> e <i>destination session limit</i>
1.62.	Permitir filtros de anomalias de protocolos
1.63.	Suportar reconhecimento de ataques de DoS, <i>reconnaissance</i> , <i>exploits</i> e <i>evasion</i>
1.64.	Suportar verificação de ataque nas camada de aplicação
1.65.	Possuir as seguintes estratégias de bloqueio: <i>pass</i> , <i>drop</i> , <i>reset</i> ,
1.66.	Possuir capacidade de desempenho de acordo com a tabela de performance dos equipamentos no final desta especificação (item 11).
1.67.	Possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES.
1.68.	Suporte a certificados PKI X.509 para construção de VPNs
1.69.	Possuir suporte a VPNs IPSec site-to-site, VPNs IPSec client-to-site.
1.70.	Possuir suporte a VPN SSL.
1.71.	Possuir capacidade de realizar SSL VPNs utilizando certificados digitais
1.72.	A VPN SSL deve possibilitar o acesso a toda infra-estrutura da empresa de acordo com a política de segurança, através de um plug-in ActiveX e/ou Java.
1.73.	A VPN SSL deverá suportar cliente para plataforma Windows, Linux e Mac OS X
1.74.	Deve permitir a arquitetura de <i>vpn hub and spoke</i>
1.75.	Suporte a VPN do tipo PPTP, L2TP
1.76.	Suporte a inclusão em autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol) e mediante arquivos.
1.77.	Deverá reconhecer no mínimo 700 aplicações;
1.78.	Deverá possuir pelo menos 10 categorias para classificação de aplicações;
1.79.	Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações como: P2P; Instant Messaging; Web; Transferência de arquivos; VOIP; Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;
1.80.	Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
1.81.	Deverá prover funcionalidade de identificação transparente de usuários cadastrados no

	Microsoft Active Directory;
1.82.	Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;
1.83.	Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;
1.84.	Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
1.85.	Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem e destino;
1.86.	Deverá permitir a inspeção/bloqueio de códigos maliciosos para no mínimo as seguintes categorias: Instant Messaging; Transferência de arquivos
1.87.	Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações
1.88.	Deverá implementar, no mínimo, as seguintes técnicas de otimização: Otimização de protocolos; Byte caching; Web caching.
1.89.	Deverá ter a possibilidade de otimizar no mínimo os seguintes protocolos: CIFS;FTP;HTTP;MAPI.
1.90.	Deverá criptografar a comunicação entre os <i>appliances</i> envolvidos na otimização do tráfego através de protocolos IPSEC ou SSH
1.91.	Deverá implementar alta disponibilidade no mínimo ativo-passivo
1.92.	Deverá possuir Cache de páginas web (HTTP)
1.93.	Deverá ser capaz de gerenciar e configurar Access Points de maneira remota automaticamente.
1.94.	Deverá ser capaz de implementar pelo menos 12 SSIDs diferentes.
1.95.	Deve ser capaz de detectar a presença de Rogue APs
1.96.	Deve ser capaz de mostrar status e informações gerais sobre cada AP (Número de Clientes, Potência de Sinal)
1.97.	Interface
1.97.1.	Interface gráfica de usuário (GUI) via HTTPS para fazer administração das políticas de segurança e que forme parte da arquitetura nativa da solução, por segurança, ou ainda, a solução pode ter interface proprietária, desde que a mesma seja fornecida com todos os componentes de hardware e software necessários e em alta-disponibilidade;
1.98.	Interface baseada em linha de comando para administração da solução.
1.99.	Comunicação cifrada e autenticada com usuário e senha, tanto como para a interface gráfica de usuário como a console de administração de linha de comandos (SSH)
1.100.	Possuir comunicação entre os componentes de forma criptografada
1.101.	Interface baseada em linha de comando para administração da solução.
1.102.	Possuir perfis administrativos com capacidade de criar ao menos 2 (dois) perfis para administração e monitoração do Firewall.
1.103.	Permitir a monitoração de CPU e memória
1.104.	Suportar SNMP versão 2
1.105.	Suportar log remoto no formato syslog
1.106.	Possuir notificação via e-mail
1.107.	Quanto ao armazenamento de dados de segurança
1.107.1.	Deve ser capaz de receber logs de pelo menos 100 dispositivos
1.107.2.	Possuir a visualização de <i>log</i> em tempo real de tráfegos de rede
1.107.3.	Permitir a visualização de logs de histórico dos acessos de tráfegos de rede

1.107.4.	Permitir a visualização dos eventos de auditoria
1.107.5.	A solução deve possuir plataforma de <i>log</i> especializada de segurança, com no mínimo 1TB de armazenamento.
1.107.6.	Permitir realização de backup e restauração dos dados
1.107.7.	Permitir o envio dos <i>logs</i> a outro centralizador de <i>log</i> externo à solução
1.107.8.	Atuar como um NAS (<i>Network Attached Storage</i>)
1.108.	Quanto aos relatórios
1.108.1.	Possuir pelo menos 20 tipos de relatórios pré-definidos na solução
1.108.2.	Permitir geração de relatórios agendados ou sob-demanda nos formatos HTML e PDF
1.108.3.	Permitir o envio dos relatórios, conforme item anterior, através de e-mail para usuários pré-definidos
1.108.4.	Disponibilizar relatórios através de FTP
1.108.5.	Possuir relatórios de acessos autorizados demonstrando a quantidade de acessos autorizados, bem como a quantidade de bytes trafegados, sendo possível sua visualização detalhada por, IP de origem, URL acessada
1.108.6.	Possuir relatório de utilização da internet por protocolo
1.108.7.	Possuir relatório dos 10 (dez) <i>sites</i> web mais acessados
1.108.8.	Possuir relatório das 10 (dez) categorias de <i>sites</i> web mais acessados
1.108.9.	Possuir relatório dos 10 (dez) usuários mais ativos
1.108.10.	Permitir customização dos relatórios, incluindo logotipo do Órgão
1.108.11.	Possuir relatórios pré-configurados para os seguintes tipos: Máquinas mais acessadas; Serviços mais utilizados; Usuários que mais utilizaram serviços, URLs mais visualizadas, Categorias Web mais acessadas; Maiores emissores e receptores de e-mail;
1.109.	Certificação ICSA para o Firewall
1.110.	Certificação ICSA IPSEC (VPN IPsec)
1.111.	Certificação ICSA para Sistema de Detecção de Intrusão
1.112.	Certificação Common Criteria como EAL4+
1.113.	Possuir Fonte de alimentação com chaveamento automático 110/220 V – 50-60Hz. A fonte fornecida deve suportar sozinha a operação da unidade com todos os módulos de interface ativos. Para o appliance do tipo 3 será necessário que o mesmo possua fontes de alimentação DC
1.114.	Permitir número ilimitado de estações de rede, usuários e túneis VPN
1.115.	Incluir licença para a funcionalidade de VPN SSL
1.116.	Incluir licença para atualização de vacina de antivírus/anti-spyware
1.117.	Incluir licença de atualização para filtro de conteúdo web
1.118.	Fornecer documentação técnica, bem como manual de uso, em inglês ou português do Brasil



Considerando os requisitos listados acima, o dimensionamento deverá atender os seguintes perfis de equipamentos:

4.1 Perfil I

Especificações Técnicas - Appliance	
Total de Interfaces RJ45	16
10/100/1000 RJ45 com possibilidade de ser uma interface acelerada com processador próprio	4
Interfaces 10/100/1000	4
Interfaces 10/100 que seja possível utilizar como Switch	8
Interface USB	3
RJ45 Serial Console	1
Performance do Sistema	
Throughput de Firewall (512/1518 byte, pacotes UDP)	5Gbps
Throughput de Firewall (64 byte, pacotes UDP)	4Gbps
Throughput IPSec VPN	2.5Gbps
Throughput IPS - Intrusion Prevention System	500Mbps
Gateway-to-Gateway IPSec VPN Tunnels	2.000
Throughput SSL-VPN	110Mbps
Throughput de Antivirus	95Mbps
Sessões Concorrentes	500.000
Novas Conexões por segundo	15.000
Usuários concorrentes SSL-VPN (Máximo recomendado)	200
Políticas (máximo)	6.000
Domínios Virtuais	10
Usuários Ilimitados	Sim
Dimensões	
Altura	4,55 cm
Largura	43,20 cm
Comprimento	29,35 cm
Peso	4,45 Kg

4.2 Perfil de Relatórios Unificados:

A solução deverá possuir uma solução de relatórios unificados totalmente integrado ao AD – Active Direct da Microsoft

A solução de relatórios deverá disponibilizar relatórios gráficos com dados personalizáveis, permitindo filtros de registros vindos a partir do dispositivo de Appliance de Controle de Acesso de Rede e outros dispositivos compatíveis com o syslog, contemplando informações como tráfego, eventos, vírus, ataques, conteúdo Web, e-mails e ser capaz de permitir a criação de outros registros além dos citados. O mesmo deverá possuir gráficos



personalizáveis, interface WEB e Administração baseada em perfis e seguindo os seguintes requisitos conforme abaixo:

Interface 10/100/1000 Ethernet	2
Interface 10/100 Ethernet	1
Capacidade de armazenamento	1TB
Número de equipamentos suportados	100
Número de agentes do fabricante da Solução suportados	100
Quarentena Centralizada	Sim
Taxa de recebimento de Arquivo	Mais de 700 Kbps
Desempenho de Logs (Logs / Seg)	Mais de 180

5 INSTALAÇÃO TÉCNICA

Escopo da Instalação On-site:

Serviço	Total de Horas
Instalação <ul style="list-style-type: none">• Atualização de versão do equipamento (Firmware)• Configuração das Interfaces de Rede• Configuração das rotas de rede• Configuração de monitoramento SNMP• Ajuste do horário• Ativação do sincronismo de logs com o Analyzer	1
Filtro WEB <ul style="list-style-type: none">• Criação das Regras de Filtro de conteúdo WEB• Instalação do aplicativo de sincronismo de contas com o AD (Microsoft Active Directory)• Definição do Perfil de antivírus• Definição do Perfil de Controle de Aplicação• Definição do bloqueio de arquivos por extensão	4
Operação Assistida (Acompanhamento pós-migração)	5
Documentação	5
Total de horas técnicas:	15

Obs.: A solução que atenderá a cada um dos perfis descritos poderá ser composta de um ou mais *appliances* e **não deverá considerar o requisito de redundância**, somente o volume de tráfego e carga de processamento esperados.

6 ADMINISTRAÇÃO E MANUTENÇÃO

- Oferecer futuramente suporte a agregação de várias unidades, tanto para gerenciamento unificado quanto para escalabilidade, possibilitando o compartilhamento ou distribuição automática de configurações e políticas, mesmo se os *appliances* estiverem geograficamente dispersos e instalados em redes distintas;
- Suportar a ampliação de sua capacidade, com a adição de novos *appliances*;
- Possuir interface de administração web com suporte aos idiomas Português Brasileiro e Inglês, e com acesso através dos protocolos HTTP e HTTPS;
- Suportar monitoramento SNMP;
- Possibilitar atualização periódica das definições de categoria, de vírus e de spyware, de forma automatizada, sem a interferência do administrador;
- Permitir a customização das mensagens de bloqueio para spyware, vírus, FTP e conteúdo;
- Permitir o backup da configuração do appliance para que o sistema possa ser restaurado ou substituído em caso de falha e suportar a configuração em alta disponibilidade.

7 DESCRIÇÃO DOS SERVIÇOS

SERVIÇOS DE SUPORTE

- ✓ Regime de atendimento de 8x5 (oito horas por dia X cinco dias por semana) com SLA de atendimento de 4 horas úteis;
- ✓ Abertura de chamados através de telefone ou e-mail;
- ✓ Suporte local de até 04 horas mensais;
- ✓ Suporte telefônico e remoto para dúvidas técnicas;
- ✓ Recomendações de segurança baseada nas funcionalidades do equipamento e no atual ambiente de rede;
- ✓ Instalação e restauração do backup no caso da necessidade de substituição do equipamento;
- ✓ Substituição do equipamento em caso de falhas com SLA de até 6 horas úteis;

SERVIÇOS DE SUPORTE COM MONITORAMENTO

- ✓ Monitoramento com ações técnicas necessárias para manter a saúde dos equipamentos fornecidos;
- ✓ Monitoramento de disponibilidade e desempenho dos equipamentos fornecidos no cenário atual;
- ✓ Monitoramento e análise dos logs dos equipamentos fornecidos;
- ✓ Monitoramento das políticas de seguranças adotadas;
- ✓ Backup semanal dos equipamentos fornecidos;
- ✓ Acompanhamento das rotas de rede em relação aos UTMs;
- ✓ Relatório mensal sobre a saúde dos equipamentos fornecidos;
- ✓ Controle do período de vigência das licenças;



8 PRAZO DE ENTREGA

A Contratada deverá disponibilizar, em até 2 (dois) dias corridos após assinatura do Contrato, os serviços e *appliances* contratados;

As novas versões de *firmware* dos produtos contratados deverão ser disponibilizadas em até 30 (trinta) dias corridos, a partir do lançamento oficial da nova versão;

9 RECEBIMENTO DO OBJETO

Os serviços com seus respectivos equipamentos, objeto da contratação serão recebidos e aceitos por representante do SENAC no Brasil que emitirá o Termo ou E-mail de Aceite, após todos os testes que comprovem os serviços contratados tais como as funcionalidades, a performance do equipamento e a qualidade técnica da proponente em conformidade com as características dos produtos disponibilizados contra as especificações técnicas solicitadas. A entrega deverá ser feita na sede do Senac - Departamento Nacional, situado na Avenida Ayrton Senna, 5555 – Rio de Janeiro.

O SENAC terá o prazo de 2 (dois) dias corridos, após recebimento do objeto, para efetuar os testes e verificações mencionadas no parágrafo anterior.

10 Valor:

Item	Descrição	Período Mínimo	Valor Mensal	Valor Anual
1	(descrever o item ofertado aqui)	12 meses	R\$	R\$



ANEXO II – CONVITE 32/2011

MODELO DE CREDENCIAMENTO

Em atendimento ao disposto no item **1.1** do Convite em referência, credenciamos o Sr., portador da Carteira de Identidade nº e do CIC nº, para que represente nossa empresa nesta licitação, com poderes plenos para prestar esclarecimentos, assinar Atas, interpor recursos ou renunciar ao direito de interpô-los e praticar tudo mais que seja necessário à participação de nossa empresa na licitação.

Rio de Janeiro, de de 2011.

nome e assinatura do responsável pela empresa

MODELO DE DECLARAÇÃO DE ACEITAÇÃO

Declaramos, em atendimento ao disposto no item **2.1.1** do Convite em referência, que recebemos e examinamos, cuidadosamente, os Documentos da licitação e, integralmente compreendemos e aceitamos as condições estabelecidas no mesmo.

Rio de Janeiro, de de 2011.

nome e assinatura do responsável pela empresa

OBSERVAÇÃO:

Estes documentos deverão ser preenchidos em papel timbrado da empresa licitante e estarem devidamente assinados por seu representante legal.



ANEXO III – CONVITE 32/2011

Modelo de Contrato de Prestação de Serviços

CONTRATANTE : Serviço Nacional de Aprendizagem Comercial - **Senac** - Administração Nacional
ENDEREÇO : Av. Ayrton Senna, 5.555 TEL.: (21) 2136-5799
BAIRRO : Barra da Tijuca CEP : 22775-004
CIDADE : Rio de Janeiro ESTADO: RJ
CNPJ : 33.469.172/0001-68 INSC. MUNICIPAL: 78.049.006

Representado por sua Diretora de Administração e Recursos Humanos, Vera Lúcia Espírito, que também assina com Vera Espírito.

CONTRATADA :
ENDEREÇO :
TEL. : Fac-símile:
BAIRRO : CEP :
CIDADE : ESTADO:
CNPJ : INSC. MUNICIPAL:

Representada por seu sócio-diretor,.

As partes acima decidem firmar entre si o presente Contrato, segundo os termos e as condições seguintes.

CLÁUSULA PRIMEIRA – OBJETO:

1.1 Constitui objeto do presente contrato a prestação pela Contratada dos serviços de Solução de Segurança de Acesso à Internet, conforme especificações contidas no Convite 32/2011 de 13/10/2011 e Proposta Comercial da Contratada de _____, que ficam fazendo parte integrante do presente **Contrato**.

CLÁUSULA SEGUNDA – VIGÊNCIA E RENOVAÇÃO

2.1 O presente Contrato entra em vigor a partir de sua assinatura e vigorará por 12 (doze) meses, podendo ser renovado por iguais períodos, através de Termo Aditivo, até o máximo de 60 meses, caso seja do interesse de ambas as partes. Neste caso, as partes deverão se pronunciar, através de correspondência, com antecedência de trinta dias do término contratual



CLÁUSULA TERCEIRA – PREÇO, CONDIÇÕES DE PAGAMENTO E REAJUSTE

- 3.1 A **Contratante** pagará a **Contratada** o valor **mensal de R\$ XXXX (valor por extenso)**, perfazendo o valor **anual de R\$ XXX (valor por extenso)**. O pagamento será efetuado até o 15º dia do mês subsequente ao da realização do serviço, através de crédito em conta corrente no Banco que a Contratada indicar na Nota Fiscal Fatura
- 3.2 O faturamento e a cobrança deverão ser efetuados para o endereço constante no caput deste contrato.
- 3.3 O preço descrito no item 3.1 será fixo e irrevogável até o término do serviço. Havendo renovação contratual para mais um período, as partes negociarão, livremente, novo preço para a prestação dos serviços.
- 3.4 A Contratante informa a todos os usuários de Nota Fiscal Eletrônica, ao emitirem-na para o Senac Departamento Nacional deverão enviar o arquivo XML para o e-mail abaixo: recepcao-fe-scc@senac.br

CLÁUSULA QUARTA – OBRIGAÇÕES DA CONTRATANTE:

- 4.1 Informar à Contratada e seus prepostos, tempestivamente, todas as informações necessárias execução dos serviços contratados;
- 4.2 Fiscalizar o cumprimento das obrigações contratuais;
- 4.3 Documentar as ocorrências havidas;
- 4.4 Facultar acesso, aos técnicos da Contratada, às instalações nas quais esteja prevista o licenciamento dos softwares ordenados;
- 4.5 Prestar as informações e os esclarecimentos que venham a ser solicitados pela Contratada;
- 4.6 Efetuar os pagamentos relativos à prestação dos serviços, nas condições previstas na Cláusula Terceira deste Contrato;

CLÁUSULA QUINTA – OBRIGAÇÕES DA CONTRATADA:

- 5.1 Executar com exatidão a entrega do objeto contratado, sob pena de responsabilidade;
- 5.2 Responsabilizar-se por todos os encargos de natureza trabalhista, social, previdenciária e/ou fiscal, relativos aos prepostos designados para realizar os serviços, objetos deste Contrato, assumindo, em consequência, a condição de única empregadora;
- 5.3 Manter, por seus funcionários, sigilo quanto aos trabalhos executados e elementos utilizados;
- 5.4 Fornecer, sempre que houver atualização de versão ou da lista de produtos, a relação atualizada das alterações ocorridas nas novas versões dos produtos do fabricante do software;
- 5.5 Fornecer em até 6 horas úteis de SLA, equipamentos de Spare part no caso de falhas, fazendo todo o processo de substituição do equipamento parado;



- 5.6 Disponibilizar, em até 2 (dois) dias corridos, após a assinatura do Contrato, os serviços e *appliances* contratados;
- 5.7 Disponibilizar as novas versões de *firmware* dos produtos contratados em até 30 (trinta) dias corridos, a partir do lançamento oficial da nova versão.

CLÁUSULA SEXTA – ALTERAÇÕES:

- 6.1 Qualquer alteração no presente Contrato será considerada como extensão ao pacto e poderá ser realizada através de correspondência entre as partes, com antecedência mínima de trinta dias, resultando em **Termo Aditivo**, o qual passará a fazer parte integrante do instrumento contratual, para todos os fins e efeitos de direito.

CLÁUSULA SÉTIMA – REAJUSTE:

- 7.1 O valor do presente Contrato será fixo e irrevogável durante sua vigência e somente poderá ser reajustado em caso de renovação, momento em que haverá livre negociação entre as partes.

CLÁUSULA OITAVA – SANÇÕES POR INADIMPLEMENTO:

- 8.1 O descumprimento, pela **Contratada**, de quaisquer das obrigações decorrentes deste Contrato implicará em mora de pleno direito, sujeitando-a, se não tomar as providências necessárias em até quinze dias após comunicação expressa da **Contratante**, a:
 - 8.1.1 Advertência;
 - 8.1.2 Pagamento de multa de cinco por cento sobre o valor mensal do Contrato;
 - 8.1.3 Rescisão do Contrato;
 - 8.1.4 Suspensão do direito de participação nas licitações promovidas pela Contratante, por período de até dois anos.

Parágrafo Único: A critério da **Contratante**, as sanções poderão ser cumulativas.

CLÁUSULA NONA – RESCISÃO:

- 9.1 O presente Contrato poderá ser rescindido:
 - 9.1.1 A qualquer tempo, por quaisquer das partes, mediante comunicação por escrito, com antecedência mínima de trinta dias da data em que se pretender rescindi-lo, momento em que deverão ser observadas as obrigações contraídas no período.
 - 9.1.2 Por descumprimento de quaisquer das cláusulas, independente de ações legais.
 - 9.1.3 Em caso de falência, concordata, dissolução ou liquidação societária e, também, em caso de insolvência.



CLÁUSULA DÉCIMA – LIMITAÇÕES DE RESPONSABILIDADE:

10.1 O direito da **Contratante** à indenização por danos a ela causados, por culpa ou negligência da **Contratada**, será limitado ao valor deste Contrato.

Parágrafo Único – Qualquer ação contra a **Contratada**, por parte da **Contratante**, para recebimento da indenização, poderá ser feita em até oito meses após a ocorrência do evento gerador da indenização.

CLÁUSULA DÉCIMA PRIMEIRA – NOVACÃO:

11.1 A não-utilização, pela **Contratante**, de qualquer direito a ele assegurado neste Contrato ou na Lei em geral, ou a não-aplicação de quaisquer das sanções nele previstas, não importará em novações quanto a seus termos, não devendo, portanto, ser interpretada como renúncia ou desistência de aplicação ou de ações futuras.

CLÁUSULA DÉCIMA SEGUNDA – DISPOSIÇÕES FINAIS:

12.1 Todas as comunicações feitas pela **Contratante**, relativas ao presente Contrato, serão consideradas como regularmente feitas, se entregues ou enviadas por carta protocolizada, telegrama, *e-mail* ou *fac-símile* para o endereço da **Contratada**.

12.3 Qualquer mudança de endereço da **Contratada** deverá ser imediatamente comunicada à **Contratante**.

12.4 Os prazos estipulados neste Contrato, para cumprimento das obrigações contratuais, vencem independentes de interpelação judicial ou extrajudicial.

CLÁUSULA DÉCIMA TERCEIRA – FORO:

13.1 As partes elegem o Foro Regional da Barra da Tijuca da Comarca do Rio de Janeiro/RJ com renúncia a qualquer outro, por mais privilegiado que seja, para dirimir as questões que, porventura, surgirem na execução do presente contrato.

Por estarem justas e de comum acordo, as partes assinam o presente Contrato em duas vias, de igual teor, e para um só efeito, na presença das testemunhas abaixo assinadas

Rio de Janeiro,

Contratada

Contratante