

ANEXO II É MINUTA DE CONTRATO

**TERMO DE CONTRATO Nº/..... QUE FAZEM
ENTRE SI A UNIÃO, POR INTERMÉDIO DO (A)
..... E A EMPRESA
.....**

A **AGÊNCIA NACIONAL DO CINEMA É ANCINE**, autarquia federal de natureza especial, instituída pela Medida Provisória n.º 2228-1, de 6 de setembro de 2001, com Escritório Central na cidade do Rio de Janeiro/RJ, na Avenida Graça Aranha, n.º 35 . Centro, inscrita no CNPJ/MF sob o n.º 04.884.574/0001-20, neste ato representada por seu Diretor-Presidente, **MANOEL RANGEL NETO**, nomeado pelo Decreto de 16/05/2013, publicado no Diário Oficial da União de 17/05/2013, inscrito no CPF/MF sob o n.º 136.524.478-40, Cédula de Identidade n.º 1.552.574, expedida pela SSP/GO, expedida pela SSP/DF, residente e domiciliado nesta cidade, doravante denominada **CONTRATANTE**, e o(a) inscrito (a) no CNPJ/MF sob o nº, sediado(a) na, em doravante designada **CONTRATADA**, neste ato representada pelo (a) Sr.(a), portador(a) da Carteira de Identidade n.º, expedida pela (o), e CPF n.º, tendo em vista o que consta no Processo n.º e em observância às disposições da Lei nº 8.666, de 21 de junho de 1993, da Lei nº 10.520, de 17 de julho de 2002 e na Lei nº 8.078, de 1990 - Código de Defesa do Consumidor, resolvem celebrar o presente Termo de Contrato, decorrente do Pregão nº/20....., mediante as cláusulas e condições a seguir enunciadas.

1. CLÁUSULA PRIMEIRA É OBJETO

1.1. O objeto do presente Termo de Contrato é a aquisição de **solução integrada de segurança de rede**, composta por dois equipamentos em cluster de alta disponibilidade, suporte técnico, licenciamento, instalação e configuração on-site, transferência de conhecimento, treinamento, operação assistida e manutenção preventiva, corretiva e evolutiva com atualizações de softwares e garantia, que serão prestados nas condições estabelecidas no Termo de Referência, Anexo I do Edital.

1.2. Este Termo de Contrato vincula-se ao Edital do Pregão, identificado no preâmbulo e à Proposta vencedora, independentemente de transcrição.

1.3. Discriminação do objeto:

AQUISIÇÃO DE SOLUÇÃO INTEGRADA DE SEGURANÇA			
ITEM	OBJETO	QUANTITATIVO	VALOR
I	Solução Integrada de Segurança de Rede, composta por dois equipamentos em cluster de alta disponibilidade, suporte técnico, licenciamento, instalação e configuração on-site, transferência de conhecimento, treinamento, operação assistida e manutenção preventiva, corretiva e evolutiva com atualizações de softwares e garantia.	01	

1.4. A solução deverá ter garantia de 36 (trinta e seis) meses, sob responsabilidade da CONTRATADA.

2. CLÁUSULA SEGUNDA É VIGÊNCIA

2.1. O prazo de vigência deste Termo de Contrato tem início na data de ____/____/____ e encerramento em ____/____/____, prorrogável na forma do art. 57, §1º, da Lei nº 8.666, de 1993.

3. CLÁUSULA TERCEIRA É PREÇO

3.1. O valor do presente Termo de Contrato é de R\$ (.....).

3.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução contratual, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

4. CLÁUSULA QUARTA É DOTAÇÃO ORÇAMENTÁRIA

4.1. As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria, prevista no orçamento da ANCINE, para o exercício de 2017, na classificação abaixo:

Gestão/Unidade: **203003/20203 É AGÊNCIA NACIONAL DO CINEMA É ANCINE**

Fonte: **0100000000**

Programa de Trabalho: **13.122.2107.2000.0001**

Elemento de Despesa: **4.4.90.52.35 É EQUIPAMENTOS DE PROCESSAMENTO DE DADOS**

PI: **7CNM0020001**

Nota de Empenho:

5. CLÁUSULA QUINTA É PAGAMENTO

5.1. O pagamento será efetuado pela **CONTRATANTE** no prazo de 05 (cinco) dias, contados da apresentação da Nota Fiscal/Fatura contendo o detalhamento dos serviços executados e os materiais empregados, através de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo **CONTRATADO**.

5.2. A apresentação da Nota Fiscal/Fatura deverá ocorrer no prazo de 05 (cinco) dias, contado da data final do período de adimplemento da parcela da contratação a que aquela se referir.

5.3. O pagamento somente será autorizado depois de efetuado o ~~at~~atesto+ pelo servidor competente, condicionado este ato à verificação da conformidade da Nota Fiscal/Fatura apresentada em relação aos serviços efetivamente prestados e aos materiais empregados.

5.4. Havendo erro na apresentação da Nota Fiscal/Fatura ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a **CONTRATADA** providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a **CONTRATANTE**.

5.5. Nos termos do artigo 36, § 6º, da Instrução Normativa SLTI/MPOG n.º 02, de 2008, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a **CONTRATADA**:

5.5.1. não produziu os resultados acordados;

5.5.2. deixou de executar as atividades contratadas, ou não as executou com a qualidade mínima exigida;

5.5.3. deixou de utilizar os materiais e recursos humanos exigidos para a execução do serviço, ou utilizou-os com qualidade ou quantidade inferior à demandada.

5.6. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

5.7. Antes de cada pagamento à **CONTRATADA**, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no Edital.

5.8. Constatando-se, junto ao SICAF, a situação de irregularidade da **CONTRATADA**, será providenciada sua advertência, por escrito, para que, no prazo de 5 (cinco) dias, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da **CONTRATANTE**.

5.9. Não havendo regularização ou sendo a defesa considerada improcedente, a **CONTRATANTE** deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da **CONTRATADA**, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

5.10. Persistindo a irregularidade, a **CONTRATANTE** deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à **CONTRATADA** a ampla defesa.

5.11. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a **CONTRATADA** não regularize sua situação junto ao SICAF.

5.12. Somente por motivo de economicidade, segurança nacional ou outro interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da **CONTRATANTE**, não será rescindido o Contrato em execução com a **CONTRATADA** inadimplente no SICAF.

5.13. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

5.13.1. A **CONTRATADA** regularmente optante pelo Simples Nacional não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

5.14. Nos casos de eventuais atrasos de pagamento, desde que a **CONTRATADA** não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela **CONTRATANTE**, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

$EM = I \times N \times VP$, sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,00016438, assim apurado:

$$I = (TX) \quad I = \frac{(6 / 100)}{\quad} \quad I = 0,00016438$$

TX = Percentual da taxa anual = 6%

6. CLÁUSULA SEXTA É REAJUSTE E ALTERAÇÕES

6.1. Os preços são fixos e irredutíveis.

7. CLÁUSULA SÉTIMA É GARANTIA DE EXECUÇÃO

7.1. A **CONTRATADA** prestará garantia no valor de R\$ (.....), na modalidade de fiança bancária, correspondente a 5% (cinco por cento) de seu valor total, no prazo de 10 (dez) dias da assinatura do contrato, observadas as condições previstas no Edital. As condições relativas à garantia prestada são as estabelecidas no Edital.

8. CLÁUSULA OITAVA - ENTREGA E RECEBIMENTO DO OBJETO

8.1. O prazo para entrega será de, no máximo, **60 (sessenta) dias** corridos após assinatura do Contrato.

8.2. Caso se veja impossibilitada de cumprir o prazo estipulado para a entrega de um dos itens do certame ou ainda de sua totalidade, a **CONTRATADA** deverá apresentar justificativas escritas e devidamente comprovadas, apoiando o pedido de prorrogação em ocorrência de fato superveniente, excepcional ou imprevisível, estranho à vontade das partes, que altere fundamentalmente as condições do Contrato.

9. CLÁUSULA NONA - FISCALIZAÇÃO

9.1. A fiscalização da execução do objeto será efetuada por Comissão/Representante designado pela **CONTRATANTE**, na forma estabelecida no Termo de Referência.

10. CLÁUSULA DÉCIMA É ESPECIFICAÇÕES TÉCNICAS

10.1. As especificações são mínimas e de atendimento obrigatório.

10.2. CARACTERÍSTICAS GERAIS

10.2.1. A solução deve ser fornecida em dispositivo de hardware físico dedicado, tipo *appliance*, com sistema operacional otimizado, do mesmo fabricante, para o uso como firewall multifunção;

10.2.2. Não serão aceitos 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 ou GNU/Linux;

10.2.3. A solução deve conter todos os acessórios necessários à instalação e operação, como, por exemplo, cabos, conectores, kits de fixação, fibras óticas (incluindo sua fusão, se necessário) e patch cords;

10.2.4. Deve possuir altura máxima de 2U para cada equipamento;

10.2.5. Deve possuir, no mínimo, no próprio equipamento, uma fonte de energia 100 VAC a 127 VAC e de 200 VAC a 240 VAC, a 60 Hz, sem uso de chave de seleção de voltagem (chaveamento automático), capaz de sustentar a configuração máxima;

10.2.6. Cada fonte de energia fornecida deve suportar sozinha a operação do hardware dedicado e de todos os módulos de interface ativos;

10.2.7. Deve possuir unidade de armazenamento interna com capacidade suficiente para armazenar todo o software e configuração;

10.2.8. Deve estar licenciado para permitir número ilimitado de estações de rede e usuários;

10.2.9. Deve incluir licença para todas as funcionalidades solicitadas pelo período de validade do Contrato;

10.2.10. A licença do gateway de segurança não deve estar vinculada a nenhum IP configurados em suas interfaces;

10.2.11. Deve permitir exportar o backup das configurações para posteriormente importar no equipamento;

10.2.12. Suportar NetFlow;

10.2.13. Deve permitir utilizar um administrador que seja autenticado em base LDAP ou RADIUS externa;

10.2.14. Pode ser entregue em equipamento único ou com composição de equipamentos e possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades;

10.2.15. Devem ser licenciados para operar em alta disponibilidade ativo-ativo e ativo-passivo;

10.2.16. Deve possuir interface de administração via web no próprio equipamento, permitindo configurá-lo diretamente por meio de um navegador web;

10.2.17. Deve permitir fazer o backup e restore das configurações.

10.3. REQUISITOS MÍNIMOS DE HARDWARE E DE DESEMPENHO

10.3.1. A solução deve suportar alta disponibilidade em modos ativo/passivo e ativo/ativo com sincronização de configuração e de estados das conexões

10.3.2. Possuir, no mínimo, 16 interfaces de 1Gb;

10.3.3. Possuir, no mínimo, 4 interfaces de 10Gb Fiber;

10.3.4. Possuir porta console;

10.3.5. Possuir, no mínimo, 1 porta USB;

10.3.6. Suportar, no mínimo, 900 interfaces de VLAN;

10.3.7. Suportar, no mínimo, 150.000 novas conexões por segundo;

10.3.8. Suportar, no mínimo, 7 milhões de conexões simultâneas;

10.3.9. Firewall Throughput de, no mínimo, 35 Gbps, baseado na RFC 2544;

10.3.10. UTM Throughput de, no mínimo, 7 Gbps;

10.3.11. Performance de VPN de, no mínimo, 9 Gbps;

10.3.12. Performance de IPS de, no mínimo, 10 Gbps;

10.3.13. Suportar, no mínimo 4.000 VPNs site-to-site (IPSec);

10.3.14. Suportar no mínimo 9.000 VPNs do tipo Client-to-Site (SSL-VPN), já licenciadas.

10.4. FUNCIONALIDADES DE FIREWALL

10.4.1. Certificação ICSA para Firewall;

10.4.2. Possuir controle de acesso à internet por endereço IP de origem e destino, subrede e vlan;

10.4.3. Permitir a criação de VLANS no padrão IEEE 802.1q;

10.4.4. Possuir integração com Servidores de Autenticação RADIUS, LDAP e Microsoft Active Directory;

10.4.5. Suportar single-sign-on para Active Directory sem a necessidade de agentes instalados nas máquinas clientes;

10.4.6. Suportar configuração off-line;

10.4.7. Suportar políticas por FQDNs;

10.4.8. Possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);

10.4.9. Possuir a funcionalidade de tradução de endereços estáticos . NAT (Network Address Translation), um para um, N-para-um, vários para um, PAT;;

10.4.10. Permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;

- 10.4.11.** Possuir a funcionalidade de fazer tradução de endereços dinâmicos utilizando o IP da própria interface;
- 10.4.12.** Suporte a roteamento estático e dinâmico RIP V1, V2, OSPF, ISIS e BGPv4;
- 10.4.13.** Possuir funcionalidades de DHCP Cliente, Servidor e Relay;
- 10.4.14.** Implementar DHCP Client e Servidor também em IPv6;
- 10.4.15.** Suportar aplicações multimídia como: H.323, SIP;
- 10.4.16.** Tecnologia de firewall do tipo Statefull;
- 10.4.17.** Possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo ativo-passivo ou Ativo-Ativo com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;
- 10.4.18.** Deve ser possível implementar múltiplas interfaces para o sincronismo do cluster, sem a necessidade de link aggregation ou configuração de interfaces redundantes;
- 10.4.19.** Deve permitir o funcionamento em modo transparente tipo ~~%bridge~~bridge+sem alterar o endereço MAC do tráfego;
- 10.4.20.** Deve suportar PBR - Policy Based Routing;
- 10.4.21.** Possuir conexão entre estação de gerencia e appliance criptografada tanto em interface gráfica quanto em CLI (linha de comando);
- 10.4.22.** Permitir forwarding de camada 2 para protocolos não IP;
- 10.4.23.** Suportar forwarding Multicast, inclusive em modo bridge;
- 10.4.24.** Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP, UDP, ICMP e IP;
- 10.4.25.** Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;
- 10.4.26.** Possuir mecanismo de anti-spoofing de endereços IP;
- 10.4.27.** Possuir a funcionalidade de balanceamento e contingência de links;
- 10.4.28.** Permitir que sejam criados testes (health checks) para identificação de falha de determinados links, que devem ser automaticamente removidos do roteamento no caso de falha;
- 10.4.29.** Permitir que o balanceamento entre os diversos links de saída seja feito por peso, sessões, IP de origem e/ou IP de destino;
- 10.4.30.** Deve suportar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;
- 10.4.31.** Permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS;
- 10.4.32.** Permitir a criação de regras baseada em usuário, grupo de usuários, endereço IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação;

10.4.33. Possuir serviço de DNS dinâmico incluído e licenciado que permita acesso por nome ao dispositivo, mesmo que ele possua IP dinâmico;

10.4.34. Possuir base de dados dinâmica e atualizada automaticamente, que contenha IPs de botnets conhecidas, permitindo o bloqueio de qualquer tráfego para tais endereços;

10.4.35. Permitir identificar graficamente, através de tabela ou mapa, quais os países que mais originaram ou receberam tráfego nos últimos minutos e horas;

10.4.36. Permitir identificar graficamente quais as políticas mais utilizadas e a quantidade de tráfego e sessões relacionadas a elas nos últimos minutos e horas;

10.4.37. Deve possuir mapa mundial indicando por cores quais países geram e recebem maior quantidade de tráfego, a quantidade de sessões e banda nos últimos minutos ou horas;

10.4.38. A solução de firewall deve possuir ferramenta para captura de pacote tcpdump ou similar;

10.4.39. Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QoS e regras DoS;

10.4.40. Deve permitir a definição de perfis de acesso à console de gerenciamento com permissões granulares: acesso de escrita, leitura, criação de usuários e alteração de configurações;

10.4.41. Gerar alertas automáticos via e-mail, SNMP V3;

10.4.42. Habilidade de realizar upgrade via interface de gerenciamento;

10.4.43. Suportar *rollback* para a última configuração salva e do sistema operacional para a última versão local;

10.4.44. Permitir que regras fiquem ativas em horários específicos;

10.4.45. A interface de gerenciamento deve exibir as seguintes informações em tempo real, atualizadas automática e continuamente:

10.4.46. Número de sessões simultâneas;

10.4.47. Status e fluxo das interfaces;

10.4.48. Uso de CPU.

10.4.49. Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário de alteração.

10.5. FUNCIONALIDADES DE RELATÓRIO, LOG E AUDITORIA

10.5.1. A solução deve incluir a funcionalidade de armazenamento de logs e geração de relatórios do mesmo fabricante do Firewall;

10.5.2. A funcionalidade poderá se dar por meio de um equipamento físico, do tipo appliance, ou por meio de Virtual Appliance; desde que compatível com sistema de virtualização VMware ESX/ESXi 6.0 ou superior, atendendo os seguintes requisitos:

10.5.3. Deve possuir interface em inglês ou português;

- 10.5.4.** Prover uma visualização sumarizada de todas as ameaças analisadas pelo firewall;
- 10.5.5.** Deve ser possível incluir múltiplas entradas nos critérios de pesquisa dos logs;
- 10.5.6.** Ela deve suportar mais de 90 tipos pré-definidos de relatórios sem custo adicional;
- 10.5.7.** Ela deve permitir configurar alertas quando estiver próxima de sua capacidade máxima, previamente definida, para a base de logs;
- 10.5.8.** Deve conseguir gerar relatórios em formato PDF e CSV para detalhamento;
- 10.5.9.** Deve possuir relatórios de *compliance* para HIPAA e PCI;
- 10.5.10.** Deve permitir a automatização da criação e envio de relatórios via e-mail;
- 10.5.11.** Deve possuir acesso baseado em função, permitindo usuários apenas visualizar relatórios e equipamentos liberados de acordo com suas funções;
- 10.5.12.** Deve possuir um relatório executivo com um sumário de informações relevantes ao tráfego passante da rede;
- 10.5.13.** O sistema deve suportar o envio automático e manual de qualquer relatório pré-definido;
- 10.5.14.** Suportar o armazenamento de, no mínimo, 1TB de Log;
- 10.5.15.** Suportar o envio de relatórios de forma automática por e-mail;
- 10.5.16.** Possibilitar a geração de, pelo menos, os seguintes tipos de relatório em formato PDF:

- 10.5.16.1.** Relatório por Protocolo;
- 10.5.16.2.** Relatório de utilização de banda total e por usuário/IP;
- 10.5.16.3.** Relatório de utilização por aplicações mais usadas;
- 10.5.16.4.** Relatório de utilização das aplicações mais bloqueadas;
- 10.5.16.5.** Relatório de utilização Web por categoria e site;
- 10.5.16.6.** Relatório de bloqueio Web por categoria e site;
- 10.5.16.7.** Relatório de utilização de banda da VPN;
- 10.5.16.8.** Relatório de ataques identificados e bloqueados pelo IPS e Antivírus.

- 10.5.17.** Suportar a pesquisa de um determinado LOG baseado em, no mínimo, endereço IP de origem, endereço IP de destino e porta de destino;
- 10.5.18.** Suportar atualização do sistema pela interface Web;
- 10.5.19.** Deve ser capaz de exportar os Logs para servidores externos Syslog.

10.6. FUNCIONALIDADES DE QOS

- 10.6.1.** Permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (*Shaping*), criação de filas de prioridade, gerência de congestionamento e QoS;
- 10.6.2.** Permitir modificação de valores DSCP para o DiffServ;
- 10.6.3.** Limitar individualmente a banda utilizada por categoria de página web, tais como sites de compartilhamento, streaming, notícias, compras, esportes, etc;

10.6.4. Limitar individualmente a banda utilizada por tipo de aplicação identificada automaticamente, tais como peer-to-peer, streaming, chat, VoIP, web, etc;

10.6.5. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

10.6.6. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;

10.6.7. Deve controlar (limitar ou expandir) individualmente a banda utilizada por usuário ou grupo de usuários do Microsoft Active Directory e LDAP;

10.6.8. Deve controlar (limitar ou expandir) individualmente a banda utilizada por sub-rede de origem e destino;

10.6.9. Deve controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino.

10.7. FUNCIONALIDADES DE ANTIMALWARE

10.7.1. Deve possuir antivírus em tempo real, para ambiente de gateway Internet integrado à plataforma de segurança para os seguintes protocolos: HTTP, SMTP, IMAP, POP3 e FTP;

10.7.2. Permitir o bloqueio de malwares;

10.7.3. Possuir proteção contra conexões a servidores Botnet;

10.7.4. Deve possuir base de dados atualizada automaticamente com IPs botnets e permitir o bloqueio de requisições DNS para esses IP.

10.8. FUNCIONALIDADE DE ANTISPAM

10.8.1. Possuir verificação na funcionalidade de anti-spam da verificação do cabeçalho SMTP do tipo MIME;

10.8.2. Possuir filtragem de e-mail por palavras chaves;

10.8.3. Permitir adicionar rótulo ao assunto da mensagem quando classificado como SPAM;

10.8.4. Deve permitir enviar determinados tráfegos de email para um antispam externo;

10.8.5. Permitir a checagem de URL no corpo da mensagem de correio eletrônico.

10.9. FUNCIONALIDADE DE FILTRO DE CONTEÚDO (WEBFILTER)

10.9.1. Possuir solução de filtro de conteúdo web integrado à solução de segurança;

10.9.2. Possuir pelo menos 50 categorias para classificação de sites web;

10.9.3. Possuir base mínima contendo 100 milhões de sites Internet web já registrados e classificados;

10.9.4. Possuir a funcionalidade de cota de tempo de utilização por categoria;

10.9.5. Permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;

10.9.6. Deve permitir a criação de listas de URL específicas para serem bloqueadas ou liberadas.

10.10. FUNCIONALIDADES DE PREVENÇÃO CONTRA INTRUSÃO (IPS)

- 10.10.1.** Permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão;
- 10.10.2.** Deve possuir base de assinaturas de IPS com, pelo menos, 2000 ameaças conhecidas;
- 10.10.3.** Deve permitir funcionar em modo transparente e router;
- 10.10.4.** Possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente;
- 10.10.5.** O sistema de detecção e proteção de intrusão deve possuir integração à plataforma de segurança;
- 10.10.6.** Dever 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;
- 10.10.7.** Deve 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;
- 10.10.8.** Deve prover notificação via Alarmes na console de administração e correio eletrônico;
- 10.10.9.** Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;
- 10.10.10.** Possuir as seguintes estratégias de bloqueio: pass, drop, reset.

10.11. FUNCIONALIDADES DE VPN

- 10.11.1.** Possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;
- 10.11.2.** Possuir suporte a VPNs IPSec site-to-site e client-to-site;
- 10.11.3.** Possuir suporte a VPN SSL;
- 10.11.4.** Deve permitir VPN SSL;
- 10.11.5.** A VPN SSL deve possibilitar o acesso a toda infraestrutura interna através da utilização de clientes instalados nas estações;
- 10.11.6.** A VPN SSL deve suportar cliente para plataforma Windows e Linux;
- 10.11.7.** Deve permitir a arquitetura de vpn hub and spoke;
- 10.11.8.** Deve indicar tentativas de login em VPN malsucedidas nos últimos minutos e horas.

10.12. FUNCIONALIDADES DE CONTROLE DE APLICAÇÕES

- 10.12.1.** Deve reconhecer no mínimo 1000 aplicações;
- 10.12.2.** Deve possuir categoria exclusiva, no mínimo, para os tipos de aplicações: P2P, Games, Web, Proxy, Audio/Video e VOIP;
- 10.12.3.** Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;

10.12.4. Deve suportar inspeção de SSL para identificar corretamente aplicações que funcionem sobre este protocolo, assim como seus detalhes tais como login, post, download etc;

10.12.5. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

10.12.6. Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;

10.12.7. Permitir identificar graficamente quais as aplicações que estão sendo utilizadas, assim como a quantidade de sessões e tráfego relacionadas a elas nos últimos minutos e horas.

10.13. FUNCIONALIDADES DE PROTEÇÃO CONTRA VAZAMENTO DE INFORMAÇÕES (DLP)

10.13.1. Deve bloquear que dados sensíveis saiam da rede, assim como a entrada de dados não requisitados;

10.13.2. Deve inspecionar tráfego HTTP;

10.13.3. Sobre o tráfego de email, deve inspecionar o protocolo SMTP;

10.13.4. Deve verificar para aplicações do tipo email, se o anexo das mensagens de correio entrantes/saíntes possui um tamanho máximo especificado pelo administrador;

10.13.5. Deve utilizar expressões regulares para composição das regras de verificação dos tráfegos;

10.13.6. Deve tomar minimamente as ações de bloquear, banir usuário e colocar em quarentena;

10.13.7. Deve permitir o armazenamento em solução específica de armazenamento de logs, o conteúdo do tráfego que coincidir com o tráfego esperado pela regra de DLP para minimamente os protocolos de Email, HTTP e Mensageiros Instantâneos;

10.13.8. Deve permitir a composição de múltiplas regras de DLP formando uma regra única mais específica que usa lógica booleana para fazer a comparação com o tráfego que atravessa o Sistema.

10.14. FUNCIONALIDADES DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS

10.14.1. Deve possuir a capacidade de análise de ameaças não conhecidas incluída na própria solução;

10.14.2. A funcionalidade deve ser capaz de mitigar técnicas modernas de evasão de defesas provendo um ambiente que simula fisicamente o hardware de um computador;

10.14.3. Deve funcionar de maneira automatizada, analisando automaticamente os arquivos suspeitos;

10.14.4. Deve permitir envio de alertas por e-mail, acesso em tempo real de análise de logs e a possibilidade de aprofundamento nos relatórios para informações mais completas.

10.15. REQUISITOS DE IMPLANTAÇÃO

10.15.1. A **CONTRADADA** será responsável pela instalação, configuração e migração das regras e controles da solução atual para a solução de segurança adquirida pela **CONTRATANTE**, de acordo com a necessidade e as políticas de segurança do Ambiente de TI;

10.15.2. A **CONTRATADA** deverá realizar o serviço instalação, configuração e migração nas dependências da Sede da **CONTRATANTE**, localizada na Avenida Graça Aranha, 35, Centro . Rio de Janeiro;

10.15.3. Após a entrega final dos equipamentos, sua instalação e configuração, a **CONTRATADA** deverá disponibilizar, sem ônus para a **CONTRATANTE**, durante o período mínimo de 02 (dois) dias úteis, não necessariamente consecutivos, um técnico certificado pelo fabricante, em regime de operação assistida, para auxiliar a equipe técnica da **CONTRATANTE** no que se fizer necessário acerca da operação dos equipamentos instalados;

10.15.4. Todas as despesas necessárias à prestação do serviço, inclusive com deslocamento e hospedagem de profissionais da **CONTRATADA**, são de exclusiva responsabilidade da **CONTRATADA**;

10.15.5. O serviço deverá ser realizado por técnico certificado na Solução;

10.15.6. O técnico da **CONTRATADA** deverá capacitar a equipe técnica da **CONTRATANTE** e sanar todas as dúvidas em relação à solução adquirida;

10.15.7. A **CONTRATADA** deverá substituir, sempre que exigido pela **CONTRATANTE**, o técnico cuja atuação, permanência ou comportamento forem julgados prejudiciais, inconvenientes ou insatisfatórios à execução dos serviços;

10.15.8. A **CONTRATADA** arcará com todas as despesas relativas aos seus profissionais e técnicos envolvidos nas atividades de operação assistida.

10.16. REQUISITOS DE TREINAMENTO

10.16.1. A **CONTRATADA** deverá apresentar um Plano de Treinamento, que deverá ser validado pela equipe técnica da **CONTRATANTE** antes do início do treinamento;

10.16.2. O treinamento deverá contemplar toda a solução adquirida e carga horária mínima de 08 horas e ser ministrado por técnico certificado pelo fabricante;

10.16.3. O treinamento deverá ser realizado em cada uma das ferramentas e módulos, com conteúdo teórico e prático, e com programas mínimos que abordem toda a instalação, configuração e operação;

10.16.4. O treinamento deverá prever a capacitação mínima de até 5 (cinco) participantes e ser realizado nas dependências da ANCINE no Rio de Janeiro;

10.16.5. A **CONTRATADA** arcará com todas as despesas relativas aos seus profissionais e técnicos envolvidos nas atividades de treinamento.

10.17. REQUISITOS DE MANUTENÇÃO E GARANTIA

10.17.1. Os serviços de assistência técnica, incluídos na garantia dos equipamentos, deverão ser prestados pelo período mínimo de 36 (trinta e seis) meses, devendo ser iniciados no primeiro dia útil após o aceite definitivo dos equipamentos, sem qualquer ônus adicional para a **CONTRATANTE**;

10.17.2. O serviço de assistência técnica deverá ser prestado mediante manutenção corretiva, preventiva e suporte técnico, a fim de manter os equipamentos em perfeitas condições de uso, sem qualquer ônus adicional para a **CONTRATANTE**;

10.17.3. Entende-se por manutenção corretiva aquela destinada a remover os defeitos apresentados pelos equipamentos, *drivers*, BIOS e outros componentes de *software* e *hardware*. Compreende a substituição de peças, ajustes nos equipamentos, atualização de versões de *drivers*, BIOS e outros componentes de *software* e *hardware* disponibilizados pelo fabricante e outras correções necessárias;

10.17.4. As peças substituídas durante a manutenção corretiva deverão ser de primeiro uso e apresentar padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento;

10.17.5. Entende-se por manutenção preventiva aquela destinada a atualizar *drivers*, BIOS e outros componentes de *software* ou *hardware* que sejam disponibilizados pelo fabricante;

10.17.6. Compete à **CONTRATADA** enviar à **CONTRATANTE** as versões atualizadas dos componentes de *software*, *drivers*, *firmwares* ou BIOS e as instruções para sua instalação, ou comunicar sua disponibilidade para *download* a partir de *site* na *Internet*, sem ônus para o **CONTRATANTE**;

10.17.7. Entende-se por suporte técnico aquele efetuado mediante suporte telefônico, *chat*, correio eletrônico ou suporte no local (*on-site*) para solução de problemas de *hardware* ou *software* que os equipamentos venham a apresentar, assim como apoio à configuração e utilização dos mesmos;

10.17.8. A assistência técnica (*on-site*) será prestada nas instalações do escritório da **CONTRATANTE** no Rio de Janeiro;

10.17.9. Caso seja necessário enviar o equipamento para um centro de assistência técnica fora das instalações da **CONTRATANTE**, a **CONTRATADA** arcará com os custos de transporte e seguro, além daqueles relacionados à manutenção do equipamento;

10.17.10. O envio de equipamentos para centros de assistência técnica em outra localidade não exime a **CONTRATADA** do cumprimento dos prazos de assistência técnica estabelecidos e **RESPECTIVAS** penalidades;

10.17.11. A **CONTRATADA** deverá manter Central de Atendimento para abertura de chamados gratuitos em regime 12x7 ou superior, sem limite de chamados;

10.17.12. Quanto à solução dos problemas, a **CONTRATADA** está obrigada a resolver 100% dos chamados técnicos solicitados;

10.17.13. Solicitações feitas pela **CONTRATANTE** sobre capacidade, instalação e configuração básica da solução devem ter o atendimento realizado e concluído em até 03 (três) dias úteis;

10.17.14. O prazo para substituição de hardware (equipamentos e componentes) deve ser de até 03 (três) dias úteis;

10.17.15. Solicitações de atendimento para os casos em que houver impacto crítico nas operações do ambiente computacional da **CONTRATADA** devem ser atendidos e concluídos em até 8 (oito) horas úteis;

10.17.16. Havendo necessidade de substituição de *hardware* (equipamentos), a **CONTRATADA** deverá efetuar a substituição por mesmo modelo de peça, ou por modelo superior em características técnicas, do mesmo fabricante, sem ônus para o **CONTRATANTE**, quando comprovados defeitos que comprometem seu desempenho, nas seguintes hipóteses, sem prejuízo de outras situações que caracterizem necessidade de troca;

10.17.17. Caso ocorram 04 (quatro) ou mais defeitos que comprometam seu uso normal, dentro de qualquer intervalo de 30 (trinta) dias;

10.17.18. Caso a soma dos tempos de paralisação do equipamento ultrapasse 80 (oitenta) horas, dentro de qualquer intervalo de 30 (trinta) dias;

10.17.19. O equipamento somente poderá ser substituído por outro equivalente ou superior;

10.17.20. Em caso de substituição de peças que contenham informações armazenadas, ou substituição integral do equipamento, as suas informações deverão ser apagadas;

10.17.21. Os serviços deverão ser, preferencialmente, executados sem impacto na utilização do ambiente de TI da **CONTRATANTE**, de forma que os serviços mais críticos poderão ser executados em horário do almoço, noturno e finais de semana, a critério da **CONTRATANTE**;

10.17.22. A realização de assistência técnica preventiva, caso não seja solicitada pelo

10.17.23. CONTRATANTE, deverá ser comunicada a este com antecedência mínima de 2 (dois) dias úteis, devendo o horário ser negociado de forma a não haver impacto no ambiente de produção do **CONTRATANTE**.

11. CLÁUSULA DÉCIMA PRIMEIRA É OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

11.1. As obrigações da **CONTRATANTE** e da **CONTRATADA** são aquelas previstas no Termo de Referência.

12. CLÁUSULA DÉCIMA SEGUNDA É SANÇÕES ADMINISTRATIVAS

12.1. Comete infração administrativa nos termos da Lei n.º 8.666, de 1993 e da Lei n.º 10.520, de 2002, a **CONTRATADA** que:

- 12.1.1.** Inexecutar, total ou parcialmente, qualquer das obrigações assumidas em decorrência da contratação;
- 12.1.2.** Ensejar o retardamento da execução do objeto;
- 12.1.3.** Fraudar na execução do Contrato;
- 12.1.4.** Comportar-se de modo inidôneo;
- 12.1.5.** Cometer fraude fiscal;
- 12.1.6.** Não manter a Proposta.

12.2. A **CONTRATADA** que cometer qualquer das infrações discriminadas no subitem acima ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

- 12.2.1.** Advertência por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a **CONTRATANTE**;
- 12.2.2.** Multa moratória de 0,5% (meio por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias;
- 12.2.3.** Multa compensatória de 20% (vinte por cento) sobre o valor total do Contrato, no caso de inexecução total do objeto.

12.3. Em caso de inexecução parcial, a multa compensatória, no mesmo percentual do subitem acima, será aplicada de forma proporcional à obrigação inadimplida.

12.4. Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos.

12.5. Impedimento de licitar e contratar com a União com o consequente descredenciamento no SICAF pelo prazo de até cinco anos.

12.6. Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a **CONTRATADA** ressarcir a **CONTRATANTE** pelos prejuízos causados.

12.7. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei n.º 8.666, de 1993, a **CONTRATADA** que:

12.7.1. Tenha sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

12.7.2. Tenha praticado atos ilícitos visando a frustrar os objetivos da licitação;

12.7.3. Demonstre não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

12.8. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à **CONTRATADA**, observando-se o procedimento previsto na Lei n.º 8.666, de 1993, e subsidiariamente a Lei n.º 9.784, de 1999.

12.9. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

12.10. As penalidades serão obrigatoriamente registradas no SICAF.

13. CLÁUSULA DÉCIMA TERCEIRA É RESCISÃO

13.1. O presente Termo de Contrato poderá ser rescindido nas hipóteses previstas no art. 78 da Lei n.º 8.666, de 1993, com as consequências indicadas no art. 80 da mesma Lei, sem prejuízo das sanções aplicáveis.

13.2. É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

13.3. Os casos de rescisão contratual serão formalmente motivados, assegurando-se à **CONTRATADA** o direito à prévia e ampla defesa.

13.4. A **CONTRATADA** reconhece os direitos da **CONTRATANTE** em caso de rescisão administrativa prevista no art. 77 da Lei nº 8.666, de 1993.

13.5. O termo de rescisão será precedido de Relatório indicativo dos seguintes aspectos, conforme o caso:

13.5.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

13.5.2. Relação dos pagamentos já efetuados e ainda devidos;

13.5.3. Indenizações e multas.

14. CLÁUSULA DÉCIMA QUARTA É VEDAÇÕES

14.1. É vedado à CONTRATADA:

14.1.1. caucionar ou utilizar este Termo de Contrato para qualquer operação financeira;

14.1.2. interromper a execução contratual sob alegação de inadimplemento por parte da **CONTRATANTE**, salvo nos casos previstos em lei.

15. CLÁUSULA DÉCIMA QUINTA É CASOS OMISSOS.

15.1. Os casos omissos serão decididos pela **CONTRATANTE**, segundo as disposições contidas na Lei n.º 8.666, de 1993, na Lei n.º 10.520, de 2002 e demais normas federais de licitações e contratos administrativos e, subsidiariamente, segundo as disposições contidas na Lei n.º 8.078, de 1990 - Código de Defesa do Consumidor - e normas e princípios gerais dos contratos.

16. CLÁUSULA DÉCIMA SEXTA É PUBLICAÇÃO

16.1. Incumbirá à **CONTRATANTE** providenciar a publicação deste instrumento, por extrato, no Diário Oficial da União, no prazo previsto na Lei n.º 8.666, de 1993.

17. CLÁUSULA DÉCIMA SÉTIMA É FORO

17.1. O Foro para solucionar os litígios que decorrerem da execução deste Termo de Contrato será o da Seção Judiciária do Rio de Janeiro - Justiça Federal.

Para firmeza e validade do pactuado, o presente Termo de Contrato foi lavrado em duas (duas) vias de igual teor, que, depois de lido e achado em ordem, vai assinado pelos contraentes.

Rio de Janeiro, de..... de 2017

CONTRATANTE:

Responsável legal da CONTRATANTE

CONTRATADA:

Responsável legal da CONTRATADA

TESTEMUNHAS: