Rua Teixeira de Freitas, 31 - 5o andar, Rio de Janeiro/RJ - CEP 20021-902
Telefones: (21) 3037-6493 - www.ancine.gov.br

TERMO DE REFERÊNCIA

PROCESSO Nº 01416.007744/2016-10

1. OBJETO DA CONTRATAÇÃO

1.1. Solução de Balanceamento de Carga e Proteção de Aplicações, composta por 2(dois) equipamentos em alta disponibilidade, com 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.

2. JUSTIFICATIVA DA CONTRATAÇÃO

2.1. Com o crescimento dos serviços disponibilizados pela ANCINE, e com adoção em 2016 de um sistema de *Autonomous System*, que proporcionou maior controle e independência do ambiente de TI, a Agência se tornou mais exposta a ataques e a exploração de vulnerabilidades oriundas da Internet;

2.2. É fato que as redes do Governo Federal sofrem inúmeras tentativas de ataques diários e, portanto, faz-se necessário contar com tecnologias que promovam a correta e robusta proteção do ambiente computacional;

2.3. Uma Solução de Controle de Aplicações é capaz de analisar todo o tráfego entrante no ambiente, verificando quais requisições são legítimas e quais são tentativas de explorar a fragilidade de serviços e sistemas corporativos;

2.4. Desda forma, a solução tem como premissa a proteção do ambiente, contudo, outros recursos contemplados na aquisição são capazes de agregar funcionalidades importantes para a otimização dos serviços disponibilizados ao usuários. Dentre os recursos está a funcionalidade de balanceamento de carga, capaz de viabilizar a utilização de outro escritório da Agência como site de contingência de serviços de TI em caso de problema com o site primário.

3. ALINHAMENTO ESTRATÉGICO E OPERACIONAL

3.1. Esse projeto está alinhado ao Planejamento Estratégico Institucional desta Agência aprovado pelo Plano Diretor de Tecnologia da Informação (PDTI) 2015-2016, mais especificamente ao Plano de Ações de IDs: A3-3 e A4-3, referente à descrição de ação “Expandir e Otimizar Serviços de TI por meio de Aquisição e Implementação de Infraestrutura Física e Lógica de TI”.

4. RESULTADOS A SEREM ALCANÇADOS

4.1. Os benefícios a serem alcançados com a presente contratação são:

4.1.1. Maior proteção das aplicações e serviços da ANCINE;

4.1.2. Possibilidade de criar ambiente de contingência para serviços corporativos;

4.1.3. Proteção contra ataques distribuídos (DDOS);

4.1.4. Proteção contra invasões e comprometimento de aplicação corporativas;

4.1.5. Otimização de aplicações corporativas.

5. QUANTIDADES

5.1

SOLUÇÃO INTEGRADA DE SEGURANÇA		
Item	**Descrição**	**Quantitativo**
1	Solução de Balanceamento de Carga e Proteção de Aplicações, composta por 2(dois) equipamentos em alta disponibilidade, com 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

6. LOCAL DE ENTREGA E DA GARANTIA

6.1. Tempo de garantia se dará por **36 meses**.

6.2. Os equipamentos e seus acessórios deverão ser entregues nos seguintes endereços:

6.2.1. Endereço: Av. Graça Aranha, 35 - 6º andar, Centro - Rio de Janeiro

7. PRAZO DE ENTREGA

7.1. O prazo para entrega será de, no máximo, 60(sessenta) dias corridos após assinatura do contrato;

7.2. Caso se veja impossibilitada de cumprir o prazo estipulado para a entrega de um dos itens do certame ou ainda de sua totalidade, a LICITANTE VENCEDORA 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.

8. CONDIÇÕES DE FORNECIMENTO

8.1. Quando das propostas de fornecimento da solução, os licitantes devem observar as seguintes condições:

8.1.1. Declarar expressamente que os preços ofertados incluem todos os custos e despesas, tais como: custos diretos e indiretos, tributos incidentes, taxa de administração, transporte, mão-de-obra, encargos sociais, trabalhista, seguros, lucro e outros necessários ao cumprimento integral do objeto;

8.1.2. Quando da habilitação no procedimento licitatório, as licitantes deverão apresentar atestados de Capacidade Técnica, através de cópia autenticada, concedido(s) por pessoa jurídica de direito público ou privado, comprovando que tenha prestado serviço(s) compatível(is) com o objeto ora licitado, entendendo-se como serviço(s) compatível(is) aquele(s) referente(s) a serviços de instalação e configuração dos produtos;

8.1.3. Será assegurado o direito de preferência previsto no art. 3°, da Lei nº 8.248, de 1991, conforme procedimento estabelecido nos arts. 5° e 8° do Decreto n° 7.174, de 2010;

8.1.4. Mantido o eventual empate entre propostas, o critério de desempate será aquele previsto no artigo 3º, § 2º, da Lei nº 8.666, de 1993, assegurando-se a preferência, sucessivamente, aos bens:

8.1.4.1. produzidos no País;

8.1.4.2. produzidos ou prestados por empresas brasileiras;

8.1.4.3. produzidos ou prestados por empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País.

9. DEVERES E RESPONSABILIDADES DA CONTRATANTE

9.1. Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta;

9.2. Exercer o acompanhamento e a fiscalização dos serviços, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;

9.3. Notificar a Contratada por escrito da ocorrência de eventuais imperfeições no curso da execução dos serviços, fixando prazo para a sua correção;

9.4. No caso em que os empregados da Contratada realizem horas extras, a contratante deverá justificar formalmente a autoridade do órgão para o qual o trabalho seja prestado e observar o limite da legislação trabalhista, exceto em caso de comprovada necessidade de serviço;

9.5. Pagar à Contratada o valor resultante da prestação do serviço, no prazo e condições estabelecidas no Edital e seus anexos;

9.6. Efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura fornecida pela contratada, em conformidade com o art. 36, §8º da IN SLTI/MPOG N. 02/2008;

9.7. A Administração não responderá por quaisquer compromissos assumidos pela Contratada com terceiros, ainda que vinculados à execução do presente objeto, bem como por qualquer dano causado a terceiros em decorrência de ato da Contratada, de seus empregados, prepostos ou subordinados.

10. DEVERES E RESPONSABILIDADES DA CONTRATADA

10.1. Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Edital e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, fabricante, modelo, procedência e prazo de garantia ou validade;

10.2. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

10.3. Substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste Termo de Referência, o objeto com avarias ou defeitos;

10.4. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

10.5. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

10.6. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com os artigos 14 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990), caso exigido no edital, ou dos pagamentos devidos à Contratada, o valor correspondente aos danos sofridos;

10.7. Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas na legislação específica, cuja inadimplência não transfere responsabilidade à Contratante;

10.8. Atender as solicitações da Contratante quanto à substituição dos empregados alocados, no prazo fixado pelo fiscal do contrato, nos casos em que ficar constatado descumprimento das obrigações relativas à execução do serviço, conforme descrito neste Termo de Referência;

10.9. Relatar à Contratante toda e qualquer irregularidade verificada no decorrer da prestação dos serviços;

10.10. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato.

11. ESPECIFICAÇÕES TÉCNICAS

11.1. **CARACTERÍSTICAS GERAIS**

11.1.1. A solução deve ser composta por 2(dois) dispositivos de harware tipo *appliance*, configurados em alta disponibilidade, sendo que cada um deve ser licenciado com *throughput* de, pelo menos, 5Gbps Layer 4 e Layer7;

11.1.2. Deve ser fornecido fonte redundante para os equipamentos compostos na solução;

11.1.3. Os equipamentos devem possuir pelo menos 256GB de disco e 8GB de memória RAM;

11.1.4. A solução deve ser capaz de usar compressão de dados em nível de software com *throughput* de pelo menos 2Gbps;

11.1.5. Deve ser acompanhada de todos os cabos necessários para a instalação do equipamento;

11.1.6. Suportar todas as aplicações comuns de um Switch Layer 7, como:

11.1.6.1. Server Load-Balancing;

11.1.6.2. Firewall Load-Balancing;

11.1.6.3. Proxy Load-Balancing;

11.1.6.4. Global Load-Balancing;

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

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

11.1.8. Permitir a clonagem de pools, de forma que a solução envie uma cópia do tráfego para um pool adicional, como por exemplo um pool de IDSs ou Sniffers, para fins de análise de tráfego de rede ou mesmo para identificação de padrões de acesso não permitidos ou indicações de atividade maliciosas ou ataques de rede;

11.1.9. Possuir recursos para balancear servidores com qualquer hardware, sistema operacional e tipo de aplicação;

11.1.10. A solução deve possuir recurso de ativação de grupo prioritário, no qual o administrador pode especificar a quantidade mínima de servidores que devem estar disponíveis em cada grupo e a prioridade dos grupos.

11.1.11. Caso o número de servidores disponíveis fique menor do que o estipulado pelo administrador, a solução deve automaticamente distribuir o tráfego para o próximo grupo com maior prioridade não afetando o serviço.

11.1.12. Caso o número de servidores disponíveis volte ao valor mínimo estipulado pelo administrador, a solução deve automaticamente retirar o grupo com menor prioridade de balanceamento, voltando ao estado original.

11.1.13. Possuir capacidade de abrir um número reduzido de conexões TCP com o servidor e inserir os HTTP requests gerado pelos clientes nestas conexões, reduzindo a necessidade de estabelecimento de conexões nos servidores e aumentando a performance do serviço;

11.1.14. Suportar os seguintes métodos de balanceamento:

11.1.14.1. Round Robin;

11.1.14.2. Least Connections;

11.1.14.3. Weighted Percentage (por peso);

11.1.14.4. Servidor ou equipamento com resposta mais rápida baseado no tráfego real;

11.1.14.5. Weighted Percentage dinâmico (baseado no número de conexões)

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

11.1.15. A solução deve permitir aplicar criptografia de cookies para a poteção dos cookies utilizados pela aplicação web;

11.1.16. Possuir recursos para balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência de sessão dos seguintes tipos:

11.1.16.1. Por cookie: inserção de um novo cookie na sessão;

11.1.16.2. Por cookie: utilização do valor do cookie da aplicação, sem adição de cookie;

11.1.16.3. Por endereço IP destino;

11.1.16.4. Por endereço IP origem;

11.1.16.5. Por sessão SSL;

11.1.16.6. Através da análise da URL acessada.;

11.1.16.7. Através da análise de qualquer parâmetro no header HTTP;

11.1.16.8. Através da análise do MS Terminal Services Session (MSRDP)

11.1.16.9. Através da análise do SIP Call ID ou Source IP;

11.1.16.10. Através da análise de qualquer informação da porção de dados (camada 7);

11.1.17. A solução deve utilizar Cache Array Routing Protocol (CARP) no algoritmo de HASH;

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

11.1.18.1. Layer 3 – ICMP;

11.1.18.2. Conexões TCP e UDP pela respectiva porta no servidor;

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

11.1.20. Possuir recursos para balanceamento de carga de servidores SIP para VoIP (equipamento SIP PROXY);

11.1.21. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor real;

11.1.22. Possuir recursos para limitar o número de sessões estabelecidas com cada

servidor virtual;

11.1.23. Possuir recursos para limitar o número de sessões estabelecidas com cada grupo de servidores;

11.1.24. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor físico:

11.1.24.1. Realizar Network Address Translation (NAT);

11.1.24.2. Realizar Proteção contra Denial of Service (DoS);

11.1.24.3. Realizar Proteção contra Syn flood;

11.1.24.4. Realizar Limpeza de cabeçalho HTTP;

11.1.25. A solução deve permitir o controle da resposta ICMP por servidor virtual;

11.1.26. Possuir recursos para que a configuração seja baseada em perfis, permitindo uma fácil administração;

11.1.27. Possuir capacidade de geração e gestão de perfis hierarquizados, permitindo maior facilidade na administração de políticas similares;

11.1.28. Permitir a criação de Virtual Servers com endereço IPv4 e os servidores reais com endereços IPv6;

11.1.29. Possuir recursos para executar compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente;

11.1.30. Definir qual tipo de compressão será habilitada, como: gzip1 a gzip9, deflate;

11.1.31. Possuir capacidade para definir compressão especificamente para certos tipos de objetos;

11.1.32. Possuir recursos para fazer aceleração de SSL, onde os certificados digitais são instalados no equipamento e as requisições HTTP são enviadas aos servidores sem criptografia;

11.1.33. Deve possuir capacidade de importação dos certificados e chaves criptográficas, para transações seguras entre cliente/servidor, podendo assim operar em modo “man in the middle”, ou seja, descriptografar, otimizar e criptografar o tráfego SSL sem comprometer a segurança da conexão SSL estabelecida previamente entre cliente/servidor. Caso haja falha na leitura da conexão SSL, esta deverá, se assim definido, prosseguir em regime de passthrough.

11.1.34. A solução deve possuir a funcionalidade de espelhamento de conexões SSL.

11.1.35. A solução deve possuir a capacidade de redirecionar o SSL Offload (troca de chaves) de determinado serviço para outro appliance físico que tenha mais capacidade para tratamento SSL. Dessa forma deve ser possível otimizar recursos executando tarefas que exigem muito desempenho para serem tratadas em hardware especializado.

11.1.36. Possuir recursos para configurar o equipamento para criptografar em SSL a requisição ao enviar para o servidor, permitindo as demais otimizações em ambiente 100% criptografado;

11.1.37. A solução deve permitir aplicar criptografia de cookies para a proteção dos cookies utilizados pela aplicação web;

11.1.38. Possuir recursos para fazer aceleração de SSL, onde os certificados digitais são instalados no equipamento e as requisições POP3S, IMAPS e SMTPS são enviadas aos servidores sem criptografia;

11.1.39. Suportar a utilização de memória RAM como cache de objetos HTTP, para responder às requisições dos usuários sem utilizar recursos dos servidores;

11.1.40. Possuir capacidade, no uso do recurso de cache, em definir quais tipos de

objeto serão armazenados em cache e quais nunca devem ser cacheados;

11.1.41. Garantir que o recurso de cache possa ajustar quanta memória será utilizada para armazenar objetos;

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

11.1.43. Deve ser capaz de realizar DHCP relay;

11.1.44. Deve possuir relatórios em tempo real das aplicações, com pelos menos os seguintes gráficos:

11.1.44.1. Tempo de resposta da aplicação;

11.1.44.2. Latência;

11.1.44.3. Conexões para conjunto de servidores, servidores individuais;

11.1.44.4. Por URL;

11.1.44.5. A ferramenta de relatórios deve possuir pelo menos os seguintes filtros para a geração dos gráficos:

11.1.44.6. Servidores virtuais

11.1.44.7. Servidores balanceados

11.1.44.8. URLs

11.1.44.9. Países de origem, baseados em geolocalização (GEOIP)

11.1.44.10. Dispositivos de origem do cliente (user agent)

11.1.45. Deve possuir framework unificado para configuração da aplicação

11.1.46. Deve possuir criptografia IPSEC para comunicação entre os balanceadores;

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

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

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

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

11.1.51. A solução deve suportar Equal Cost Multipath (ECMP);

11.1.52. A solução deve realizar Bidirectional Forward Detection (BFD);

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

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

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

11.1.56. A solução deve realizar SSL Forward Proxy;

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

11.1.58. A solução deve ter suporte a criptografia Perfect Forward Secrecy não apenas para troca de chaves RSA.

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

11.1.59.1. Deve ser possível configurar o tamanho máximo da fila;

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

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

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

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

11.1.63. Permitir tráfego por parâmetros de QoS (Quality of Service) ou rate-shaping, com pelo menos 2 (duas) filas para priorização de tráfego baseada na camada de aplicação;

11.1.64. Através dessa priorização de tráfego e restrição de largura de banda deverá ser possível permitir um melhor nível de serviço para clientes preferenciais em detrimento dos demais clientes.

11.1.65. A solução deve permitir a priorização de tráfego de entrada para determinadas aplicações.

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

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

11.1.68. Fornecer recursos para o uso de servidores (reals) no mesmo Virtual Server;

11.1.69. Possuir suporte ao protocolo SPDY e HTTP 2.0;

11.1.70. O equipamento deve possuir suporte ao espelhamento de conexões FTP, Telnet, HTTP, UDP, SSL.

11.1.71. O equipamento deverá permitir a sincronização das configurações:

11.1.72. De forma automática; e

11.1.73. Manualmente, forçando a sincronização apenas no momento desejado;

11.1.74. Permitir a configuração das interfaces de alta disponibilidade do cluster (heartbeat), com opções para:

11.1.74.1. Compartilhar a rede de heartbeat com a rede de dados; e

11.1.74.2. Utilizar uma rede exclusiva para o heartbeat.

11.1.75. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra-ataques;

11.1.76. Permitir a criação de políticas através de interface gráfica web para manipulação de tráfego através de lógica para pelo menos os seguintes operadores:

11.1.77. GEOIP, http-basic-auth, http-cookie, http-header, http-host, http-method, http-referer, http-set-cookie, http-status, http-uri e http-version

11.1.78. Deve ser possível tomar as seguintes ações através dessas políticas:

11.1.78.1. Bloqueio de tráfego

11.1.78.2. Reescrita e manipulação de URL

11.1.78.3. Registro de tráfego (log)

11.1.78.4. Adição de informação no cabeçalho HTTP

11.1.78.5. Redirecionamento do tráfego para um membro específico

11.1.78.6. Selecionar uma política específica para Aplicação Web

11.1.79. A solução deve ser capaz de analisar a performance de aplicações web.

11.1.80. A solução deve possuir relatórios das aplicações.

11.1.81. Deve prover métricas de aplicações como: Transações por Segundo; Tempo de latência do cliente e servidor; Throughput de requisição e resposta; Sessões

11.1.82. A solução deverá gerar informações para permitir análises históricas e auxiliar nos processos de manutenções preventivas, de troubleshooting, de planejamento de capacidade e de análise da experiência dos usuários finais no acesso das aplicações.

11.1.83. As informações coletadas deverão permitir a análise dos dados por aplicações, por URL's, por clientes e por servidores, permitindo assim a identificação mais precisa dos eventuais ofensores do tráfego suportado pela solução.

11.1.84. A solução deverá gerar informações estatísticas de acesso identificando para cada aplicação os métodos de acesso HTTP (GET e Post), o tipo de sistema operacional utilizado pelos clientes, e os browsers utilizados.

11.1.85. A geração de informações históricas deverá permitir:

11.1.85.1. O detalhamento do tempo de resposta total de carregamento de uma URL e ou Página;

11.1.85.2. Permitir a correlação de métricas de uso de rede com o comportamento das aplicações.

11.1.86. A solução de balanceamento global de Data Center deve operar, no mínimo, nas seguintes formas:

11.1.86.1. DNS autoritativo;

11.1.86.2. DNS secundário;

11.1.86.3. DNS resolver;

11.1.86.4. DNS cache;

11.1.86.5. Balanceamento de DNS servers;

11.1.87. Capacidade de uso de chave criptográfica TSIG para comunicação segura entre servidores DNS, obedecendo no mínimo os padrões: HMAC MD5, HMAC SHA-1 ou HMAC SHA-256;

11.1.88. A solução deve realizar o offload dos servidores de DNS, funcionando como o DNS secundário;

11.1.89. A solução deve servir as respostas as requisições onde o DNS é o autoritativo a partir da memória RAM;

11.1.90. A solução deve possuir certificação ICSA;

11.1.91. A solução deve possuir proteções contra-ataques DNS, no mínimo:

11.1.91.1. Inspeção de protocolo;

11.1.91.2. Validação de protocolo;

11.1.91.3. UDP flood;

11.1.91.4. Pacotes mal formados;

11.1.91.5. Ataque thwarting teardrop;

11.1.91.6. Ataque ICMP;

11.1.92. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra-ataques;

11.1.93. A solução deve ser capaz de realizar balanceamento dos servidores DNS;

11.1.94. A solução deve ser capaz de realizar filtragem de pacotes;

11.1.95. A solução deve prover segurança do protocolo DNS, protegendo contra-ataques de negação de serviço, NXDOMAIN e reflexão de DNS;

11.1.96. A solução deve realizar stateful inspection;

11.1.97. A solução deve possuir base de Geolocalização IP;

11.1.98. A solução deve implementar DNS64;

11.1.99. A solução deve suportar pelo menos os seguintes tipos de requisição DNS: SOA, A, AAAA, CNAME, MX, NS, PTR, SRV, TXT;

11.1.100. Deve ser capaz de gerar estatísticas sobre consultas de DNS por: Aplicação, nome da query, tipo da query, endereço IP do cliente;

11.1.101. Deve ser possível configurar a solução de modo inline a estrutura de DNS existente e transparente sem requerer grandes mudanças na infraestrutura;

11.1.102. Deve prover as respostas a queries DNS da própria RAM CACHE;

11.1.103. A solução de alta disponibilidade será realizada baseada em respostas a requisições DNS. A resposta a requisições DNS devem conter apenas endereços que estejam disponíveis no momento, e balanceadas por usuário, de acordo com as políticas definidas;

11.1.104. A solução deverá aceitar resolução de nomes baseada em topologia, onde requisições de DNS são respondidas baseado no país, continente, ou endereço IP de onde veio a requisição;

11.1.105. Deve ser possível ajustar quantos endereços são enviados em uma única resposta;

11.1.106. Suporte a monitoração de estado de saúde de servidores, serviços e links de conexão a provedor de serviço, garantindo a disponibilidade do serviço oferecido;

11.1.107. Suportar pelo menos os seguintes algoritmos de balanceamento:

11.1.107.1. Round Robin;

11.1.107.2. Global Availability;

11.1.107.3. Ratio;

11.1.107.4. LDNS Persist;

11.1.107.5. Geografia;

11.1.107.6. Disponibilidade da Aplicação;

11.1.107.7. Capacidade do Virtual Server;

11.1.107.8. Least Connections;

11.1.107.9. Round trip time;

11.1.107.10. Hops;

11.1.107.11. Kilobytes per Second.

11.1.108. Implementar persistência da conexão do usuário entre aplicações ou data centers;

11.1.109. A solução deve suportar o controle de grupos de aplicações, e permitir que um usuário seja redirecionado para outro datacenter quando houver falha em qualquer das aplicações de um mesmo grupo;

11.1.110. Deve permitir que as políticas sejam configuradas individualmente por aplicação sendo balanceada;

11.1.111. A solução deve permitir que a contingência seja automática, mas que o retorno

seja manual;

11.1.112. A solução deve ser capaz de lidar com clientes IPv6 quando o site atende apenas com IPv4 (requests AAAA ou A6);

11.1.113. Possuir suporte a IPv6 no balanceamento global entre datacenters;

11.1.114. Ter capacidade de tratar informações das camadas L4-L7 (FTP, SMTP, URL, HTTP Header, TCP e UDP) para a tomada de decisão de encaminhamento a servidor real, em IPv4 e IPv6;

11.2. **CARACTERÍSTICAS DE SEGURANÇA - WEB APPLICATION FIREWALL**

11.2.1. A solução de segurança em camada de aplicação deve funcionar nas mesmas maquinas virtuais ofertadas na solução de aceleração e distribuição de carga com a finalidade de reduzir o tempo de latência e o impacto nas transações da CONTRATANTE;

11.2.2. A solução deve operar nos modos ativo-ativo e ativo-standby;

11.2.3. O equipamento oferecido deverá proteger a infra-estrutura web de ataques contra a camada de aplicação (Camada 7);

11.2.4. Deve possuir tecnologia para mitigação de DDoS em camada 7 baseado em analise comportamental, usando o aprendizado e analíticos de big data;

11.2.5. A solução deve possuir a capacidade de capturar tráfego no formato TCP Dump relativos a ataques DoS L7, Web Scraping e força bruta permitindo uma análise mais aprofundada por parte do administrador;

11.2.6. A solução deve suportar o uso de firewall camada 7;

11.2.7. O equipamento oferecido deverá possuir a certificação ICSA para Firewall de Aplicação (Web Application Firewall);

11.2.8. Permitir a utilização de um modelo positivo de segurança para proteger contra-ataques conhecidos aos protocolos HTTP e HTTPS e às aplicações web acessíveis através destes;

11.2.9. Possuir política de segurança de aplicações web pré-configurada na solução;

11.2.10. Permitir a criação de políticas diferenciadas por aplicação;

11.2.11. A solução deverá se integrar a soluções de análise (Scanner) de vulnerabilidade do site. O resultado desta análise deve ser utilizado para configurar as políticas do equipamento;

11.2.12. A solução deve permitir a integração com soluções de análise de vulnerabilidades (Scanner) de terceiros como, por exemplo: Trustwave App Scanner (Cenzic), White Hat Sentinel, IBM AppScan, Qualys;

11.2.13. A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação;

11.2.14. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar e aumentar a proteção contra-ataques recentes;

11.2.15. A solução deve se integrar com outras soluções de segurança e análise de logs de outros fabricantes;

11.2.16. Deve possuir tecnologia de detecção de anomalias, permitindo a detecção de DoS ataques de força bruta e ataques de sequestro de sessão. Deve ser possível filtrar relatórios por origens;

11.2.17. A solução deve permitir incluir em blacklist os endereços IPs que repetidamente falharem a desafios no browser. Portanto o sistema não precisa usar recursos para mitigar trafego enviado por esses endereços Ips. Ao entrar em Blacklist o sistema automaticamente bloqueia os pacotes enviados por esse endereço por um período de

tempo;

11.2.18. A solução deve suportar e fazer a proteção do tráfego em cima de protocolo WebSocket;

11.2.19. A solução deve possibilitar o uso de múltiplas formas de logging remoto ao mesmo tempo para a mesma aplicação. Portanto dever ser possível por exemplo logar os requests válidos e os requests inválidos em servidor de SIEM;

11.2.20. A solução deverá possuir funcionalidade de proteção positiva e segura contra-ataques, como:

11.2.20.1. Acesso por Força Bruta;

11.2.20.2. Ameaças Web AJAX/JSON;

11.2.20.3. DoS e DDoS camada 7;

11.2.20.4. Buffer Overflow;

11.2.20.5. Cross Site Request Forgery (CSRF);

11.2.20.6. Cross-Site Scripting (XSS);

11.2.20.7. SQL Injection;

11.2.20.8. Parameter tampering;

11.2.20.9. Cookie poisoning;

11.2.20.10. HTTP Request Smuggling;

11.2.20.11. Manipulação de campos escondidos;

11.2.20.12. Manipulação de cookies;

11.2.20.13. Roubo de sessão através de manipulação de cookies;

11.2.20.14. Sequestro de sessão;

11.2.20.15. Força bruta no browser;

11.2.20.16. XML bombs/DoS;

11.2.20.17. Checagem de consistência de formulários;

11.2.20.18. Checagem do cabeçalho do “user-agent” para identificar clientes inválidos;

11.2.21. Deve ser capaz de identificar e bloquear ataques através de assinaturas, com atualização periódica da base pelo fabricante.

11.2.21.1. As assinaturas devem ser atualizadas durante o período do contrato sem que seja necessário nenhum custo adicional por parte da CONTRATANTE na aquisição de novas licenças ou subscrições.

11.2.21.2. As assinaturas devem fazer parte da solução de WAF ofertada;

11.2.21.3. Deve possuir regras de verificação personalizadas – política de segurança configurada;

11.2.22. Deve prevenir contra vazamento de dados sensíveis (mensagens de erro HTTP, códigos das aplicações, entre outros) dos servidores de aplicação, retirando os dados ou mascarando a informação nas páginas enviadas aos usuários;

11.2.23. Deve permitir a customização da resposta de bloqueio;

11.2.24. Permitir a liberação temporária ou definitiva (white-list) de endereços IP bloqueados por terem originados ataques detectados pela solução;

11.2.25. Deve permitir limitar o número de conexões e requisições por IP de origem para cada endereço IP Virtual;

11.2.26. Deve permitir adicionar, automaticamente e manualmente, em uma lista de bloqueio, os endereços IP de origem que ultrapassarem o limite estabelecido, por um período de tempo determinado através de configuração;

11.2.27. Deve permitir criar lista de exceção (white list) por endereço IP específico ou faixa de sub-rede;

11.2.28. A solução deve suportar o modelo de segurança positiva definido pelo OWASP, pelo menos o que consta no TOP 10;

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

11.2.30. Deverá implantar, no mínimo, as seguintes funcionalidades:

11.2.30.1. Proteção contra Buffer Overflow;

11.2.30.2. Checagem de URL;

11.2.30.3. Checagem de métodos HTTP utilizados (GET, POST, HEAD, OPTIONS, PUT, TRACE, DELETE, CONNECT);

11.2.30.4. Proteção contra envios de comandos SQL escondidos nas requisições enviadas a bases de dados (SQL Injection);

11.2.30.5. Proteção contra Cross-site Scripting;

11.2.30.6. Funcionalidade de Cookie Encryption;

11.2.30.7. Checagem de consistência de formulários;

11.2.30.8. Checagem do cabeçalho “user-agent” para identificar clientes inválidos.

11.2.31. Deve ser possível definir uma lista de métodos permitidos e proibidos para cada URL separadamente;

11.2.32. Deve suportar a criação de políticas por geo-localização, permitindo que o tráfego de determinado(s) País/Países seja(m) bloqueado(s);

11.2.33. Possuir mecanismo de aprendizado automático capaz de identificar todos os conteúdos das aplicações, incluindo URLs, parâmetros URLs, campos de formulários, o que se espera de cada campo (tipo de dado, tamanho de caracteres), cookies, arquivos XML e elementos XML;

11.2.34. O equipamento oferecido deverá possuir uma funcionalidade de criação automática de políticas, onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real observado à aplicação;

11.2.35. O perfil aprendido de forma automatizada deve poder ser ajustado, editado ou bloqueado;

11.2.36. O equipamento oferecido deve possuir proteção baseada em assinaturas para prover proteção contra ataques conhecidos;

11.2.37. Deve ser possível desabilitar algumas assinaturas específicas em determinados parâmetros, como uma exceção a regra geral;

11.2.38. A atualizações de assinaturas deverão passar por um período configurável de testes, ondes nenhuma requisição que viole a assinatura será bloqueada, apenas informada no relatório. Este processo deve ser automatizado, não sendo necessário criar regras específicas a cada atualização de assinatura;

11.2.39. O equipamento oferecido deve permitir o bloqueio de ataques DoS na camada 7, possuindo também a opção de apenas registrar o ataque, sem tomar nenhuma ação de bloqueio;

11.2.40. O equipamento oferecido deve possuir as seguintes formas de detecção de ataques DoS na camada de aplicação:

11.2.40.1. Número de requisições por segundo enviados a uma URL específica;

11.2.40.2. Número de requisições por segundo enviados de um IP específico;

11.2.40.3. Detecção através de código executado no cliente com o objetivo de detectar interação humana ou comportamento de robôs (bots);

11.2.40.4. Número máximo de transações por segundo (TPS) de um determinado IP;

11.2.40.5. Aumento de um determinado percentual do número de transações por segundo (TPS);

11.2.40.6. Aumento do tempo de resposta (latência de aplicação) de uma determinada URL;

11.2.41. O equipamento oferecido deverá permitir o bloqueio de ataques de força bruta de usuário/senha em páginas de acesso (login) que protegem áreas restritas. Este bloqueio deve limitar o número máximo de tentativas e o tempo do bloqueio deverá ser configurável;

11.2.42. O equipamento oferecido deverá permitir o bloqueio de determinados endereços IPs que ultrapassarem um número máximo de violações por minuto. O período de bloqueio deverá ser configurável e durante este período todas as requisições do cliente serão bloqueadas automaticamente;

11.2.43. O equipamento oferecido deverá permitir o bloqueio de robôs (bots) que acessam a aplicação através de detecção automática, não dependendo de cadastros manuais. Robôs conhecidos do mercado, como Google, Yahoo e Microsoft Bing deverão ser liberados por padrão;

11.2.44. O equipamento oferecido deverá permitir o cadastro de robôs que podem acessar a aplicação;

11.2.45. Possuir política de segurança de aplicações para pelo menos as seguintes aplicações:

11.2.45.1. Microsoft ActiveSync v1.0, v2.0;

11.2.45.2. Microsoft OWA in Exchange 2003, 2007, 2010;

11.2.45.3. Microsoft SharePoint 2003, 2007, 2010;

11.2.45.4. Oracle 10g Portal;

11.2.45.5. Oracle Application 11i;

11.2.45.6. Oracle PeopleSoft Portal.

11.2.46. O equipamento oferecido deverá implementar proteção ao JSON (JavaScript Object Notation);

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

11.2.48. Implementar a segurança de web services, através dos seguintes métodos:

11.2.48.1. Criptografar/Decriptografar partes das mensagens SOAP;

11.2.48.2. Assinar digitalmente partes das mensagens SOAP;

11.2.48.3. Verificação de partes das mensagens SOAP;

11.2.49. Prevenir o vazamento de informações, permitindo o bloqueio ou a remoção dos dados confidenciais;

11.2.50. Prevenir que erros de aplicação ou infra-estrutura sejam mostrados ao usuário;

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

11.2.52. Deverá proteger o protocolo FTP com pelo menos os seguintes métodos:

11.2.52.1. Determinar os comandos FTP permitidos;

11.2.52.2. Requests FTP anônimos;

11.2.52.3. Checar compliance com o protocolo FTP;

11.2.52.4. Proteger contra-ataques de força bruta nos logins;

11.2.53. Deverá proteger o protocolo SMTP com pelo menos os seguintes métodos:

11.2.53.1. A comunicação deve ser aderente a RFC 2821;

11.2.53.2. Limitar o número de mensagens;

11.2.53.3. Validar registro SPF do DNS;

11.2.53.4. Determinar quais métodos SMTP podem ser utilizados.

11.2.54. Deverá armazenar os logs localmente ou exportar para Syslog server;

11.2.55. Deverá proteger contra atraques CSRF (*Cross-Site Request Forgery*), podendo ser possível especificar quais URLs serão examinadas;

11.2.56. Deverá possuir controle de fluxo por aplicação permitindo definir o fluxo de acesso de uma URL para outra da mesma aplicação. Dessa forma qualquer tentativa de acesso a um determido site que não siga o fluxo passando pelas URLs pré-definidas deverá ser bloqueado como uma tentativa de acesso ilegal impedindo ataques de diretório;

11.2.57. A solução deve fornecer relatórios consolidados de ataques com pelo menos os seguintes dados: Resumo geral com as políticas ativas, anomalias e estatísticas de tráfego, Ataques DoS, Ataques de Força Bruta, Ataques de Robôs, Violações, URL, Endereços IP, Países, Severidade e PCI Compliance;

11.2.58. Deverá permitir o agendamento de relatórios a serem entregues por email;

11.2.59. Fornecer os seguintes Gráficos de alertas por:

11.2.59.1. Política de segurança;

11.2.59.2. Tipos de ataques;

11.2.59.3. Violações;

11.2.59.4. URL;

11.2.59.5. Endereços IP;

11.2.59.6. Países;

11.2.59.7. Severidade;

11.2.59.8. Código de resposta;

11.2.59.9. Métodos;

11.2.59.10. Protocolos;

11.2.59.11. Usuário;

11.2.59.12. Sessão.

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

11.2.61. Deve ser possível verificar o endereço de origem do pacote IP no cabeçalho IP e no parâmetro X-forwarded-for (XFF);

11.2.62. Deve possuir, pelo menos, as seguintes categorias de endereços IP: Windows Exploits, Web Attacks, Botnets, Scanners, Denial of Service, Reputation, Phishing Proxy, Anonymous Proxy;

11.3. **GERENCIAMENTO**

11.3.1. Deve implementar uma configuração de endereçamento IP estático ou dinâmico (DHCP/BOOTP) para o gerenciamento;

11.3.2. Deve implementar o SNTP (Simple Network Time Protocol) ou NTP (Network Time Protocol);

11.3.3. Permitir acesso in-band via SSH;

11.3.4. Manter internamente múltiplos arquivos de configurações do sistema;

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

11.3.6. Possuir auto-complementação de comandos na CLI;

11.3.7. Possuir ajuda contextual;

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

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

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

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

11.3.12. Possuir Interface Gráfica via Web;

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

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

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

11.3.16. Suportar a rollback de configuração e imagem;

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

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

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

11.3.20. A interface Gráfica deverá permitir a reinicialização do equipamento;

11.3.21. Reinicialização do equipamento por comando na CLI;

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

11.3.23. Possuir traps SNMP;

11.3.24. Possui suporte a monitoração utilizando RMON através de pelo menos 4 grupos: statistics, history, alarms e events

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

11.3.26. Implementar Debugging: CLI via console e SSH;

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

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

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

11.3.30. É recomendável que a Solução tenha suporte a sFlow;

11.4. **REQUISITOS DE IMPLANTAÇÃO**

11.4.1. A CONTRADADA será responsável pela instalação e configuração de todas as funcionalidades da Solução descrita neste documento, de acordo com a necessidade e políticas de segurança do Ambiente de TI da ANCINE;

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

11.4.3. Após a entrega final da solução, 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 na solução, em regime de operação assistida, para auxiliar a equipe técnica da Contratante no que se fizer necessário acerca da operação dos equipamentos instalados;

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

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

11.4.6. O técnico da Contratada deverá capacitar a equipe técnica da Contratante e sanar todas as dúvidas em relação à solução adquirida;

11.4.7. 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;

11.4.8. A Contratada arcará com todas as despesas relativas aos seus profissionais e técnicos envolvidos nas atividades de operação assistida.

11.5. **REQUISITOS DE TREINAMENTO**

11.5.1. A Contratada deverá apresentar um Plano de Treinamento, que deverá ser validado pela equipe técnica da Contratante antes do início do treinamento;

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

11.5.3. 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;

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

11.5.5. O Contratado arcará com todas as despesas relativas aos seus profissionais e técnicos envolvidos nas atividades de treinamento.

11.6. **REQUISITOS DE MANUTENÇÃO E GARANTIA**

11.6.1. Os serviços de assistência técnica, incluídos na garantia da Solução, 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;

11.6.2. 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;

11.6.3. 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;

11.6.4. 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;

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

11.6.6. 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;

11.6.7. 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;

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

11.6.9. 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;

11.6.10. 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;

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

11.6.12. Quanto à solução dos problemas, a Contratada está obrigada a resolver 100% dos chamados técnicos solicitados;

11.6.13. 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;

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

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

11.6.16. 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:

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

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

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

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

11.6.21. 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;

11.6.22. A realização de assistência técnica preventiva, caso não seja solicitada pela 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.

12. DO FUNDAMENTO LEGAL E DO JULGAMENTO DAS PROPOSTAS

12.1. A presente aquisição se dará mediante procedimento licitatório, na modalidade Pregão Eletrônico, com esteio legal nos termos da Lei nº 10.520/2002 e Decreto nº 5.450/2005 e, ainda, subsidiariamente, na Lei nº 8.666/1993;

12.2. As propostas serão julgadas e adjudicadas pelo menor preço global.

13. CLASSIFICAÇÃO DE BENS COMUNS

13.1. Os bens a serem adquiridos enquadram-se nos pressupostos do §1º do Art. 2º do Decreto n° 5.450, de 2005, e também do parágrafo único do Art. 1º da Lei. Nº 10.520, de 2002, já que seus padrões de desempenho e qualidade podem ser objetivamente definidos por este edital e seus anexos, por meio de especificações usuais no mercado.

14. CONDIÇÕES PARA ACEITE DO OBJETO

14.1. O objeto deste Termo de Referência será aceito pela Gerência de Tecnologia da Informação (GTI) após verificação de conformidade das características da solução entregue em relação às especificações técnicas constantes no presente Termo de Referência e na proposta da licitante vencedora;

14.2. A Ancine poderá efetuar, caso necessário, Prova de Conceito (PoC) da solução, a fim de se averiguar as características da solução face ao exigido no presente Termo de Referência;

14.3. Fica estabelecido o prazo de 5 (cinco) dias úteis, após recebimento e instalação da solução, para se efetuar os testes e verificações, e prazo de 10 (dez) dias úteis em caso de necessidade de PoC;

14.4. O recebimento do objeto não exclui a responsabilidade pela qualidade, ficando a licitante vencedora obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, os produtos objeto desta contratação, não excluindo ou reduzindo essa responsabilidade, a fiscalização ou o acompanhamento exercido pela ANCINE;

14.5. Somente será emitido o ACEITE DEFINITIVO DO OBJETO após verificação, por parte da Gerência de Tecnologia da Informação da Ancine, de atendimento de todos os itens da solução ofertada na especificação do presente Termo de Referência;

15. DO PAGAMENTO

15.1. O pagamento será realizado após o Aceite Definitivo do objeto, através de ordem bancária, para crédito em banco, agência e conta corrente indicados pela Contratada;

15.2. O pagamento somente será autorizado depois de efetuado o “atesto” pelo servidor competente na nota fiscal apresentada;

15.3. Havendo erro na apresentação da Nota Fiscal 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 ANCINE;

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

15.5. Antes do pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital;

15.6. 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 ANCINE;

15.7. Não havendo regularização ou sendo a defesa considerada improcedente, a ANCINE 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;

15.8. Persistindo a irregularidade, a ANCINE deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa;

15.9. 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;

15.10. Somente por motivo de economicidade, segurança nacional ou outro interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da ANCINE, não será rescindido o contrato em execução com a contratada inadimplente no SICAF;

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

15.11.1. A Contratada regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, 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.

15.12. 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 ANCINE, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

EM = I x N x 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)	I = (6/100) 365	I = 0,00016438 TX = Percentual da taxa anual = 6%.

16. DA FISCALIZAÇÃO

16.1. A fiscalização do objeto do presente Termo de Referência será exercida por um representante da ANCINE, designado para esta finalidade específica, ao qual competirá dirimir as dúvidas que surgirem no curso da prestação dos serviços e de tudo dará ciência à Administração, conforme art. 67 da lei nº. 8.666, de 1993.

17. DA DOTAÇÃO ORÇAMENTÁRIA

17.1. As despesas com a execução desta contratação correrão à conta dos recursos consignados do Orçamento Geral da União para o exercício de 2017.

18. DAS SANÇÕES ADMINISTRATIVAS

18.1. Comete infração administrativa nos termos da Lei nº 8.666, de 1993 e da Lei nº 10.520, de 2002, a Contratada que:

18.1.1. Inexecutar, total ou parcialmente, qualquer das obrigações assumidas em decorrência da contratação;

18.1.2. Ensejar o retardamento da execução do objeto;

18.1.3. Fraudar na execução do contrato;

18.1.4. Comportar-se de modo inidôneo;

18.1.5. Cometer fraude fiscal;

18.1.6. Não mantiver a proposta.

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

18.2.1. Advertência por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a Contratante;

18.2.2. 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;

18.2.3. Multa compensatória de 20% (vinte por cento) sobre o valor total do contrato, no caso de inexecução total do objeto.

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

18.4. 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;

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

18.6. 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;

18.7. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de

1993, a Contratada que:

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

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

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

18.8. 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 nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999;

18.9. 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;

18.10. As penalidades serão obrigatoriamente registradas no SICAF.

19. DOS CRITÉRIOS DE SUSTENTABILIDADE AMBIENTAL

19.1. O fabricante do produto ofertado deverá respeitar, no que couber, os seguintes itens:

19.1.1. que os bens sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme ABNT NBR – 15448-1 e 15448-2;

19.1.2. que sejam observados os requisitos ambientais para a obtenção de certificação do Instituto Nacional de Metrologia, Normalização e Qualidade Industrial – INMETRO como produtos sustentáveis ou de menor impacto ambiental em relação aos seus similares;

19.1.3. que os bens não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoH (*Restriction of Certain Hazardous Substances*), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenil-polibromados (PBBs), éteres difenil-polibromados (PBDEs);

19.1.4. que os bens devam ser, preferencialmente, acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento.

Documento assinado eletronicamente por **Leonardo De Oliveira Alves Sanches**, **Analista Administrativo**, em 25/01/2017, às 15:41, conforme horário oficial de Brasília, com fundamento no art. 11 da RDC/ANCINE nº 66 de 1º de outubro de 2015.

Documento assinado eletronicamente por **Otavio Albuquerque Ritter Dos Santos**, **Gerente de Tecnologia da Informação**, em 26/01/2017, às 09:14, conforme horário oficial de Brasília, com fundamento no art. 11 da RDC/ANCINE nº 66 de 1º de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ancine.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0316908** e o código CRC **761FE59C**.