

TERMO DE REFERÊNCIA

PROCESSO Nº 01416.007180/2016-15

1. OBJETO DA CONTRATAÇÃO

1.1. Solução Integrada de Segurança de Rede, composta por 2 (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;

1.2. A Licitante deverá apresentar a proposta discriminando os custos dos equipamentos, 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. Em 2013 a Gerência de Tecnologia da Informação da ANCINE iniciou os trabalhos de fortalecimento de sua infraestrutura de segurança, adquirindo solução específica para proteger as redes e sistemas, tanto no Centro de Processamento de Dados da Agência no Rio de Janeiro, como nos escritórios regionais de Brasília e São Paulo;

2.2. Contudo, devido ao encerramento do ciclo de vida do modelo da solução de segurança atualmente em uso na Agência, assim como do suporte técnico, há a necessidade de aquisição de nova solução. Soma-se a isso o desenvolvimento e incorporação de novos projetos da ANCINE, que exigem a expansão das capacidades, desempenho e funcionalidades da Solução de Segurança;

2.3. Diante deste panorama, faz-se necessário a adequação do ambiente com a aquisição de nova solução para dar continuidade e aprimorar o controle da segurança, o aumento da disponibilidade, a facilidade no gerenciamento de redes e a melhoria nos serviços disponibilizados;

2.4. Desta forma, propõe-se a aquisição de Solução Integrada de Segurança, mediante pregão eletrônico.

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. Proteção contra malwares e ataques ao ambiente computacional da ANCINE;

4.1.2. Atualização tecnológica do ambiente de TI;

4.1.3. Maior confidencialidade, integridade, disponibilidade e autenticidade das informações da Agência.

5. QUANTIDADES

SOLUÇÃO INTEGRADA DE SEGURANÇA		
Item	Objeto	Quantitativo

I	Solução Integrada de Segurança de Rede, composta por 2 (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
---	---	----

6. LOCAL DE ENTREGA E DA GARANTIA

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

6.1.1. Endereço: Av. Graça Aranha 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. VISTORIA

8.1. Para o correto dimensionamento e elaboração de proposta, a LICITANTE poderá realizar vistoria no local de entrega da solução, acompanhado por servidor designado para esse fim, de segunda à sexta-feira, das 10h às 12h e das 14h às 17h, devendo o agendamento ser efetuado previamente pelo telefone (21) 3037-6445 e/ou (21) 3037-6424;

8.2. O prazo para vistoria compreende primeiro dia útil seguinte à publicação do Edital, estendendo-se até o dia útil anterior à data prevista para a abertura do Pregão Eletrônico.

9. CONDIÇÕES DE FORNECIMENTO

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

9.1.1. 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;

9.1.2. Apresentar Declaração do Fabricante atestando que a licitante vencedora é Parceiro Autorizado para a revenda/distribuição da solução e que está apta a fornecer o objeto ofertado. Esta declaração deverá estar destinada a ANCINE;

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

9.1.4. 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:

9.1.4.1. produzidos no País;

9.1.4.2. produzidos ou prestados por empresas brasileiras;

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

10. DEVERES E RESPONSABILIDADES DA CONTRATANTE

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

10.2. 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;

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

10.4. Não permitir que os empregados da Contratada realizem horas extras, exceto em caso de comprovada necessidade de serviço, formalmente justificada pela autoridade do órgão para o qual o trabalho seja prestado e desde que observado o limite da legislação trabalhista;

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

10.6. 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;

10.7. 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.

11. DEVERES E RESPONSABILIDADES DA CONTRATADA

11.1. 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;

11.2. 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);

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

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

11.5. 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;

11.6. 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), ficando a Contratante autorizada a descontar da garantia, caso exigido no edital, ou dos pagamentos devidos à Contratada, o valor correspondente aos danos sofridos;

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

11.8. 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;

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

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

11.11. Não será admitida a subcontratação do objeto licitatório.

12. ESPECIFICAÇÕES TÉCNICAS

12.1. As especificações são mínimas e de atendimento obrigatório.

12.2. CARACTERÍSTICAS GERAIS

12.2.1. 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;

12.2.2. 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;

12.2.3. A solução deve ser 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;

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

12.2.5. 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;

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

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

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

12.2.9. Deve incluir licença para todas as funcionalidades solicitadas pelo período de validade do contrato;

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

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

12.2.12. Suportar NetFlow;

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

12.2.14. 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;

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

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

12.2.17. Deve permitir fazer o backup e restore das configurações;

12.3. **REQUISITOS MÍNIMOS DE HARDWARE E DE DESEMPENHO**

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

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

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

12.3.4. Possuir porta console;

12.3.5. Possuir, no mínimo, 1 porta USB;

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

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

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

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

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

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

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

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

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

12.4. **FUNCIONALIDADES DE FIREWALL**

12.4.1. Certificação ICSA para Firewall;

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

- 12.4.3. Permitir a criação de VLANs no padrão IEEE 802.1q;
- 12.4.4. Possuir integração com Servidores de Autenticação RADIUS, LDAP e Microsoft Active Directory;
- 12.4.5. Suportar single-sign-on para Active Directory sem a necessidade de agentes instalados nas máquinas clientes;
- 12.4.6. Suportar configuração off-line;
- 12.4.7. Suportar políticas por FQDNs;
- 12.4.8. Possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);
- 12.4.9. Possuir a funcionalidade de tradução de endereços estáticos ó NAT (Network Address Translation), um para um, N-para-um, vários para um, PAT;;
- 12.4.10. Permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;
- 12.4.11. Possuir a funcionalidade de fazer tradução de endereços dinâmicos utilizando o IP da própria interface;
- 12.4.12. Suporte a roteamento estático e dinâmico RIP V1, V2, OSPF, ISIS e BGPv4;
- 12.4.13. Possuir funcionalidades de DHCP Cliente, Servidor e Relay;
- 12.4.14. Implementar DHCP Client e Servidor também em IPv6;
- 12.4.15. Suportar aplicações multimídia como: H.323, SIP;
- 12.4.16. Tecnologia de firewall do tipo Statefull;
- 12.4.17. 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;
- 12.4.18. Deve ser possível implementar múltiplas interfaces para o sincronismo do cluster, sem a necessidade de link aggregation ou configuração de interfaces redundantes;
- 12.4.19. Deve permitir o funcionamento em modo transparente tipo õbridgeõ sem alterar o endereço MAC do tráfego;
- 12.4.20. Deve suportar PBR - Policy Based Routing;
- 12.4.21. Possuir conexão entre estação de gerencia e appliance criptografada tanto em interface gráfica quanto em CLI (linha de comando);
- 12.4.22. Permitir forwarding de camada 2 para protocolos não IP;
- 12.4.23. Suportar forwarding Multicast, inclusive em modo bridge;
- 12.4.24. Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP, UDP, ICMP e IP;
- 12.4.25. Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;
- 12.4.26. Possuir mecanismo de anti-spoofing de endereços IP;
- 12.4.27. Possuir a funcionalidade de balanceamento e contingência de links;
- 12.4.28. 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;
- 12.4.29. Permitir que o balanceamento entre os diversos links de saída seja feito por peso, sessões, IP de origem e/ou IP de destino;
- 12.4.30. Deve suportar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;
- 12.4.31. Permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS;
- 12.4.32. Permitir a criação de regras baseada em usuário, grupo de usuários, endereço IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação;
- 12.4.33. Possuir serviço de DNS dinâmico incluído e licenciado que permita acesso por nome ao dispositivo,

mesmo que ele possua IP dinâmico;

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

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

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

12.4.37. 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;

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

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

12.4.40. 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;

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

12.4.42. Habilidade de realizar upgrade via interface de gerenciamento;

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

12.4.44. Permitir que regras fiquem ativas em horários específicos;

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

12.4.46. Número de sessões simultâneas;

12.4.47. Status e fluxo das interfaces;

12.4.48. Uso de CPU.

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

12.5. **FUNCIONALIDADES DE RELATÓRIO, LOG E AUDITORIA**

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

12.5.2. 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:

12.5.3. Deve possuir interface em inglês ou português;

12.5.4. Prover uma visualização sumarizada de todas as ameaças analisadas pelo firewall;

12.5.5. Deve ser possível incluir múltiplas entradas nos critérios de pesquisa dos logs;

12.5.6. Ela deve suportar mais de 90 tipos pré-definidos de relatórios sem custo adicional;

12.5.7. Ela deve permitir configurar alertas quando estiver próxima de sua capacidade máxima, previamente definida, para a base de logs;

12.5.8. Deve conseguir gerar relatórios em formato PDF e CSV para detalhamento;

12.5.9. Deve possuir relatórios de *compliance* para HIPAA e PCI;

12.5.10. Deve permitir a automatização da criação e envio de relatórios via e-mail;

12.5.11. Deve possuir acesso baseado em função, permitindo usuários apenas visualizar relatórios e equipamentos liberados de acordo com suas funções;

12.5.12. Deve possuir um relatório executivo com um sumário de informações relevantes ao tráfego passante da rede;

12.5.13. O sistema deve suportar o envio automático e manual de qualquer relatório pré-definido;

- 12.5.14. Suportar o armazenamento de, no mínimo, 1TB de Log;
- 12.5.15. Suportar o envio de relatórios de forma automática por e-mail;
- 12.5.16. Possibilitar a geração de, pelo menos, os seguintes tipos de relatório em formato PDF:
 - 12.5.16.1. Relatório por Protocolo;
 - 12.5.16.2. Relatório de utilização de banda total e por usuário/IP;
 - 12.5.16.3. Relatório de utilização por aplicações mais usadas;
 - 12.5.16.4. Relatório de utilização das aplicações mais bloqueadas;
 - 12.5.16.5. Relatório de utilização Web por categoria e site;
 - 12.5.16.6. Relatório de bloqueio Web por categoria e site;
 - 12.5.16.7. Relatório de utilização de banda da VPN;
 - 12.5.16.8. Relatório de ataques identificados e bloqueados pelo IPS e Antivírus.
- 12.5.17. Suportar a pesquisa de um determinado LOG baseado em, no mínimo, endereço IP de origem, endereço IP de destino e porta de destino;
- 12.5.18. Suportar atualização do sistema pela interface Web.
- 12.5.19. Deve ser capaz de exportar os Logs para servidores externos Syslog.

12.6. **FUNCIONALIDADES DE QOS**

- 12.6.1. 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;
- 12.6.2. Permitir modificação de valores DSCP para o DiffServ;
- 12.6.3. Limitar individualmente a banda utilizada por categoria de página web, tais como sites de compartilhamento, streaming, notícias, compras, esportes, etc;
- 12.6.4. Limitar individualmente a banda utilizada por tipo de aplicação identificada automaticamente, tais como peer-to-peer, streaming, chat, VoIP, web, etc;
- 12.6.5. Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
- 12.6.6. Deve prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;
- 12.6.7. Deve controlar (limitar ou expandir) individualmente a banda utilizada por usuário ou grupo de usuários do Microsoft Active Directory e LDAP;
- 12.6.8. Deve controlar (limitar ou expandir) individualmente a banda utilizada por sub-rede de origem e destino;
- 12.6.9. Deve controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;

12.7. **FUNCIONALIDADES DE ANTIMALWARE**

- 12.7.1. 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;
- 12.7.2. Permitir o bloqueio de malwares;
- 12.7.3. Possuir proteção contra conexões a servidores Botnet;
- 12.7.4. Deve possuir base de dados atualizada automaticamente com IPs botnets e permitir o bloqueio de requisições DNS para esses IP;

12.8. **FUNCIONALIDADE DE ANTISPAM**

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

- 12.8.2. Possuir filtragem de e-mail por palavras chaves;
- 12.8.3. Permitir adicionar rótulo ao assunto da mensagem quando classificado como SPAM;
- 12.8.4. Deve permitir enviar determinados tráfegos de email para um antispam externo;
- 12.8.5. Permitir a checagem de URL no corpo da mensagem de correio eletrônico;
- 12.9. **FUNCIONALIDADE DE FILTRO DE CONTEÚDO (WEBFILTER)**
- 12.9.1. Possuir solução de filtro de conteúdo web integrado à solução de segurança;
- 12.9.2. Possuir pelo menos 50 categorias para classificação de sites web;
- 12.9.3. Possuir base mínima contendo 100 milhões de sites Internet web já registrados e classificados;
- 12.9.4. Possuir a funcionalidade de cota de tempo de utilização por categoria;
- 12.9.5. Permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;
- 12.9.6. Deve permitir a criação de listas de URL específicas para serem bloqueadas ou liberadas;
- 12.10. **FUNCIONALIDADES DE PREVENÇÃO CONTRA INTRUSÃO (IPS)**
- 12.10.1. 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;
- 12.10.2. Deve possuir base de assinaturas de IPS com, pelo menos, 2000 ameaças conhecidas;
- 12.10.3. Deve permitir funcionar em modo transparente e router;
- 12.10.4. Possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente;
- 12.10.5. O sistema de detecção e proteção de intrusão deve possuir integração à plataforma de segurança;
- 12.10.6. 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;
- 12.10.7. 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;
- 12.10.8. Deve prover notificação via Alarmes na console de administração e correio eletrônico;
- 12.10.9. Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;
- 12.10.10. Possuir as seguintes estratégias de bloqueio: pass, drop, reset;
- 12.11. **FUNCIONALIDADES DE VPN**
- 12.11.1. Possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;
- 12.11.2. Possuir suporte a VPNs IPSec site-to-site e client-to-site;
- 12.11.3. Possuir suporte a VPN SSL;
- 12.11.4. Deve permitir VPN SSL;
- 12.11.5. A VPN SSL deve possibilitar o acesso a toda infraestrutura interna através da utilização de clientes instalados nas estações;
- 12.11.6. A VPN SSL deve suportar cliente para plataforma Windows e Linux;
- 12.11.7. Deve permitir a arquitetura de vpn hub and spoke;
- 12.11.8. Deve indicar tentativas de login em VPN malsucedidas nos últimos minutos e horas;
- 12.12. **FUNCIONALIDADES DE CONTROLE DE APLICAÇÕES**
- 12.12.1. Deve reconhecer no mínimo 1000 aplicações;
- 12.12.2. Deve possuir categoria exclusiva, no mínimo, para os tipos de aplicações: P2P, Games, Web, Proxy, Audio/Video e VOIP;
- 12.12.3. Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;
- 12.12.4. Deve suportar inspeção de SSL para identificar corretamente aplicações que funcionem sobre este

protocolo, assim como seus detalhes tais como login, post, download etc;

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

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

12.12.7. 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.

12.13. **FUNCIONALIDADES DE PROTEÇÃO CONTRA VAZAMENTO DE INFORMAÇÕES (DLP)**

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

12.13.2. Deve inspecionar tráfego HTTP;

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

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

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

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

12.13.7. 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;

12.13.8. 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.

12.14. **FUNCIONALIDADES DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS**

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

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

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

12.14.4. 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.

12.15. **REQUISITOS DE IMPLANTAÇÃO**

12.15.1. A CONTRATADA 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;

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

12.15.3. 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;

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

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

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

12.15.7. 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;

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

12.16. **REQUISITOS DE TREINAMENTO**

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

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

12.16.3. 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;

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

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

12.17. **REQUISITOS DE MANUTENÇÃO E GARANTIA**

12.17.1. 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;

12.17.2. 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;

12.17.3. 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;

12.17.4. 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;

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

12.17.6. 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;

12.17.7. 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;

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

12.17.9. 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;

12.17.10. 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;

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

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

12.17.13. 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;

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

12.17.15. 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;

12.17.16. 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:

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

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

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

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

12.17.16.5. 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;

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

13. DO FUNDAMENTO LEGAL E DO JULGAMENTO DAS PROPOSTAS

13.1. 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;

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

14. CLASSIFICAÇÃO DE BENS COMUNS

14.1. Os bens a serem adquiridos enquadram-se nos pressupostos do §1º do Art. 2º do Decreto nº 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.

15. CONDIÇÕES PARA ACEITE DO OBJETO

15.1. 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;

15.2. 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;

15.3. 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;

15.4. 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;

15.5. 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;

16. DO PAGAMENTO

16.1. 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.

16.2. Os pagamentos decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da Lei n.º 8.666, de 1993, deverão ser efetuados no prazo de até 5 (cinco) dias úteis, contados da data da apresentação da Nota Fiscal/Fatura, nos termos do art. 5º, § 3º, da Lei n.º 8.666, de 1993.

16.3. 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.

16.4. O pagamento somente será autorizado depois de efetuado o teste 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.

16.5. 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**.

16.6. 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**:

16.6.1. não produziu os resultados acordados;

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

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

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

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

16.9. 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**.

16.10. 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.

16.11. 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.

16.12. 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.

16.13. 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.

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

16.14.1. 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.

16.15. 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)	I =	(6 / 100)	I = 0,00016438 TX = Percentual da taxa anual = 6%
----------	-----	-------------	--

17. DA FISCALIZAÇÃO

17.1. 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.

18. DA DOTAÇÃO ORÇAMENTÁRIA

18.1. As despesas com a execução desta contratação correrão à conta dos recursos consignados do Orçamento Geral da União para o exercício de 2016.

19. DAS SANÇÕES ADMINISTRATIVAS

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

- 19.1.1. Inexecutar, total ou parcialmente, qualquer das obrigações assumidas em decorrência da contratação;
- 19.1.2. Ensejar o retardamento da execução do objeto;
- 19.1.3. Fraudar na execução do contrato;
- 19.1.4. Comportar-se de modo inidôneo;
- 19.1.5. Cometer fraude fiscal;
- 19.1.6. Não mantiver a proposta.
- 19.2. A Contratada que cometer qualquer das infrações discriminadas no subitem acima ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:
 - 19.2.1. Advertência por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a Contratante;
 - 19.2.2. 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;
 - 19.2.3. Multa compensatória de 20% (vinte por cento) sobre o valor total do contrato, no caso de inexecução total do objeto.
- 19.3. Em caso de inexecução parcial, a multa compensatória, no mesmo percentual do subitem acima, será aplicada de forma proporcional à obrigação inadimplida;
- 19.4. 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;

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

19.6. 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;

19.7. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, a Contratada que:

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

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

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

19.8. 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;

19.9. 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;

19.10. As penalidades serão obrigatoriamente registradas no SICAF.

20. DOS CRITÉRIOS DE SUSTENTABILIDADE AMBIENTAL

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

20.1.1. que os bens sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme ABNT NBR 6154-1 e 6154-2;

20.1.2. que sejam observados os requisitos ambientais para a obtenção de certificação do Instituto Nacional de Metrologia, Normalização e Qualidade Industrial 61 INMETRO como produtos sustentáveis ou de menor impacto ambiental em relação aos seus similares;

20.1.3. 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);

20.1.4. 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 06/01/2017, às 14:44, 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 **Otávio Albuquerque Ribeiro Dos Santos, Gerente de Tecnologia da Informação**, em 06/01/2017, às 14:59, 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 **Glênio França, Secretário de Gestão Interna**, em 06/01/2017, às 18:54, 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 **0296816** e o código CRC **EF535D1D**.

