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 01416.007348/2016-84

1. OBJETO DA CONTRATAÇÃO

1.1. Solução de Análise de Log e Eventos, composta de software, 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. Nos últimos anos o ambiente de TI cresceu fortemente, disponibilizando diversos sistemas e serviços, tanto para os usuários internos quanto para o público externo;

2.2. A quantidade de computadores servidores e ativos de rede atualmente em uso no ambiente de TI produz grande quantidade de registros de log, das mais variadas categorias. Contudo, é necessário que tais registros sejam armazenados, indexados e apresentados de forma organizada para que seja utilizada pela TI da Agência;

2.3. Um dos principais focos da solução reside em reforçar os mecanismos de combate a ataques de redes, gerando informações relevantes dos dados coletados dos dispositivos e equipamentos de um ambiente de TI;

2.4. A contratação permitirá maior efetividade no combate às ameaças de disponibilidade e de integridade da informação, bem como evidenciará, de forma objetiva, as vulnerabilidades existentes na infraestrutura de TI;

2.5. Diante deste panorama, faz-se necessário a adequação do ambiente com a aquisição da solução para dar continuidade e aprimorar o controle da segurança aos serviços e sistemas da Agência;

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).

4. RESULTADOS A SEREM ALCANÇADOS

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

4.1.1. Maior confiabilidade na análise dos registros de log do ambiente de TI;

4.1.2. Maior visibilidade sobre a segurança de TI da ANCINE;

4.1.3. Maior rapidez da resolução de incidentes de segurança.

5. QUANTIDADES

Item	Objeto	Quantitativo

I	Solução de Análise de Log e Eventos, composta de software, 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. 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. 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;

8.1.3. 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:

8.1.3.1. produzidos no País;

8.1.3.2. produzidos ou prestados por empresas brasileiras;

8.1.3.3. 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 instalação e suporte, fixando prazo para a sua correção;

9.4. 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 de acordo com o horário de funcionamento da ANCINE;

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;

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 para passagem de conhecimento;

10.9. Relatar à Contratante eventuais incidentes 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. **LICENCIAMENTO**

11.1.1. A modalidade de licenciamento deverá permitir a quantidade mínima de 100GB por dia de dados indexados ou o equivalente em Eventos Por Segundo (EVP), e a distribuição livre de conectores, ou similar, gerados com o uso do SDK ou API (*Application Programming Interface*), independentemente do número e arquitetura;

11.1.2. Oferecer garantia de atualização e correção pelo período de 36 meses da solução ofertada;

11.1.3. A solução deve ser licenciada de forma que não limite a Agência Nacional do Cinema - ANCINE quanto a quantidade de usuários, dispositivos monitorados e/ou relatórios gerados. Caso a solução ofertada apresente modalidade de licenciamento por usuários, dispositivos monitorados e/ou relatórios gerados, deverá ser apresentado os valores prevendo licenciamento ilimitado para os itens apresentados;

11.1.4. A distribuição dos módulos da solução do ambiente tecnológico da Contratante deve ser livre, no sentido de permitir sua distribuição pelo ambiente sem a necessidade de licenças adicionais, dentro do limite de processamento e indexação licenciados, conforme item requisitos de capacidade e performance;

11.2. **CARACTERÍSTICAS GERAIS**

11.2.1. A solução, como um todo, deve ser virtualmente ilimitada no volume de dados coletados, processados e armazenados, sendo limitada apenas ao volume de dados licenciados no presente certame;

11.2.2. Coletor de dados em tempo real: coletar, aplicar *parsing*, normalizar, classificar, agregar informações, sumarizar, processar regras, compactar e armazenar os dados recebidos dos elementos geradores de eventos presentes no ambiente tecnológico;

11.2.3. Correlacionador: processar regras tanto em tempo de coleta como em tempo de análise, analisar e correlacionar eventos globais advindos dos dispositivos do ambiente tecnológico e aplicar regras de correlacionamento e análise conforme regras configuráreis antes, durante e após o processamento. Essas regras de correlacionamento serão definidas e customizadas na fase de instalação e configuração da solução;

11.2.4. Armazenamento de eventos dos dispositivos do ambiente tecnológico: receber as informações e dados enviados pelos ambientes tecnológicos, ou de diferentes fontes, compactar, organizar e armazenar e gerenciar todo o ciclo de armazenamento da solução, garantido a integridade do dado no formato raw;

11.2.5. Console de monitoramento e operação: visualizar os dados dos dispositivos do ambiente tecnológico exibindo resultados que proporcionem o controle sobre o ambiente corporativo do ponto de vista de:

11.2.5.1. monitoramento em tempo real da performance das aplicações, redes e servidores,

11.2.5.2. análise da performance da operação e impacto no negócio,

11.2.5.3. análise de incidentes,

11.2.5.4. segurança da informação na perspectiva de SIEM (alertas) e forense (correlação, pesquisas ad hoc e relatórios);

11.2.5.5. análise de segurança da informação garantindo a integridade dos eventos e evidências;

11.2.6. A console de monitoramento deve possuir uma base de conhecimento na interface do usuário para pesquisa e solução relativa ao incidente e criação de novos painéis de monitoramento;

11.2.7. Administração da solução: visualizar os painéis de monitoramento e incidentes exibindo resultados que proporcionem o controle sobre a segurança corporativa, fornecendo várias formas de classificação e visualização dinâmicas dos eventos;

11.2.8. A solução de correlacionamento deve implementar o recebimento de eventos de análise comportamental de rede. A solução poderá implementar a análise de fluxos (flows) e de eventos por uma única interface de gerência. A solução deve receber os fluxos por pelo menos um dos seguintes protocolos: Netflow, Jflow, cFlow, Sflow, Flowlog, Packeteer. Por meio das informações coletadas dos flows, a solução deve permitir

demonstração sobre utilização da rede Inbound e Outbound, visualização de protocolos utilizados na rede e criação de regras de alerta sobre protocolos indesejados;

11.2.9. Permitir investigação de ataques, anomalias, alvos de ataque, atacantes da rede. Deve correlacionar eventos e atividades de rede, bem como identificar os alvos;

11.2.10. Capacidade de emitir relatórios executivos, operacionais e de conformidade a normas de mercado e flexibilidade na criação de novos relatórios pelos próprios usuários, sem interferência de componentes externos ou a necessidade de customização em código complexa que exija serviços profissionais terceiros;

11.2.11. Visualizar os dados dos dispositivos do ambiente tecnológico de forma centralizada, fornecendo um conjunto de funções e indicadores gerenciais específicos, contemplando o panorama de monitoramento e segurança no ambiente da instituição e flexibilidade na criação de novos relatórios pelos próprios usuários, sem interferências de componentes externos ou a necessidade de customização em código complexa que exija serviços profissionais terceiros;

11.2.12. Desenvolvimento de regras para o correlacionamento: possibilitar a criação de regras de correlacionamento, através de ferramenta gráfica. A solução deverá prover módulo de construção e testes de regras. Toda a construção das regras deverá ser feita em ambiente gráfico e as regras deverão possibilitar ações, como por exemplo, enviar e-mails e traps SNMP;

11.2.13. Toda comunicação deverá ter a capacidade de trafegar de forma criptografada (SSL);

11.2.14. Deve permitir a criação de usuários com diferentes níveis de acesso;

11.2.15. Deve permitir autenticação de usuário no mínimo em uma base LDAP/Active Directory, RADIUS, e base local;

11.2.16. A comunicação entre os dispositivos do ambiente tecnológico geradores os dados e a solução deve ser feita no mínimo por meio dos protocolos a seguir: SYSLOG, SDEE, SNMPv2 e SNMPv3, além da capacidade de mapeamento de pastas de redes ou serviços nativos de coleta de dados;

11.2.17. A solução deve possuir capacidade de acesso via web de forma segura (HTTPS), para monitoração, gerenciamento e geração de relatórios;

11.2.18. Os conectores, ou solução similar, deverão coletar de forma nativa as plataformas: Windows, Linux, AIX, HPUX, sempre na última versão;

11.2.19. Em tempo real, coletar e aplicar *parsing* (segmento do dado) nos eventos do dispositivo monitorado;

11.2.20. Filtrar e selecionar os eventos que serão inseridos na solução;

11.2.21. Definir prioridade para o evento, alerta e incidente;

11.2.22. Correlacionar os eventos recebidos através de regras de correlacionamento e análise conforme regras configuráreis antes, durante e após o processamento dos dados recebidos;

11.2.23. Gerar alertas com base nas regras criadas;

11.2.24. Verificar conformidade com as políticas, controles e normas internas e externas;

11.2.25. Armazenar os eventos e os alertas, com pesquisa imediata aos eventos de origem que os geraram, apontando os eventos raw;

11.2.26. Permitir pesquisas nos eventos históricos, fornecendo capacidade de “drill-down”, ou seja, visualizar detalhes dos eventos, inclusive dado “raw”, quando aplicável, para

análise forense e investigação de incidentes;

11.2.27. Enviar mensagens por e-mail, sms, trap SNMP;

11.3. **FONTE DE DADOS (DISPOSITIVOS DO AMBIENTE TECNOLÓGICO)**

11.3.1. Todo serviço técnico para coleta dos dados dos dispositivos do ambiente tecnológico devem estar inclusos na proposta técnica;

11.3.2. A solução deve ser capaz de coletar dados dos mais diversos dispositivos do ambiente tecnológico, garantindo que quaisquer alterações do atual ambiente tecnológico sejam suportados. Para fins de dimensionamento do serviço técnico, considerar-se-á inicialmente os seguintes dispositivos:

Device type	Total
DHCP server	6
Linux server	29
Windows server 2003	13
3Com Switch	2
Brocade Communications Systems Device	2
Cisco switch	23
Extreme Networks switch	4
Firewall UTM	4
Firewall WAF	1
Windows server 2003	1
VNX 5300	1
cisco 3925E	2
Cisco C3560	1
Cisco C3400	1

11.4. **MONITORAMENTO AVANÇADO DE TI E COMPLIANCE**

11.4.1. Painel de gerenciamento centralizado de todos os dispositivos do ambiente tecnológico;

11.4.2. Identificar rapidamente a causa raiz dos incidentes detectados no ambiente em console única;

11.4.3. Criação de relatórios e alertas em tempo real para todos os ativos da TI, correlacionando os eventos independente de dispositivos do ambiente tecnológico de origem;

11.4.4. Capacidade de monitoramento de ambientes virtualizados em todas as suas camadas (virtualização, aplicação, sistemas operacionais, rede, servidores físicos e storages);

11.4.5. Criação de relatórios e dashboards de monitoramento dos SLA's acordados, tanto com fornecedores internos como externos e configuração de alertas em caso de violação dos mesmos;

11.4.6. Alertas configuráveis para: notificação em painel de monitoramento, envio de e-mail e execução de scripts;

11.4.7. Capacidade de análises preditivas com base em dados históricos, antevendo por meio de gráficos e alertas eventuais tendências a degradação ou queda de serviços e sistemas;

11.4.8. Monitoramento, via performance das aplicações, dos serviços mais críticos ao negócio, conforme necessidade da equipe de sustentação de aplicações com flexibilidade na geração de regras e relatórios;

11.4.9. Fornecer informações sobre consumo e performance dos dispositivos do ambiente tecnológico para capacity planning;

11.4.10. Implementar relatórios do grau de conformidade com normas reguladores de mercado, para no mínimo as seguintes normas: COBIT, PCI 2.0;

11.4.11. Emissão de relatórios de conformidade do ambiente monitorado em relação à norma ISO/IEC 27001 e ISO/IEC 27002, com base nos eventos recebidos;

11.4.12. Possibilitar criação de regras, painéis gráficos (dashboards) e relatórios para monitorar normas internas;

11.4.13. Capacidade de criação de novas regras, padrões de monitoramento e alertas, além de alteração das existentes;

11.4.14. Capacidade de criar de correlacionamento que possibilitem, numa única regra, inserir múltiplas ações, inclusive diferentes entre si, com base na ordem dos eventos correlacionados pela regra (primeiro, subsequente ou em casa evento) e nos thresholds de correlacionamento;

11.4.15. Permitir testar as regras com eventos reais capturados anteriormente e mantidos na base de dados da solução, sem afetar a execução das regras em produção;

11.4.16. **SEGURANÇA DA INFORMAÇÃO**

11.4.17. Efetuar a análise dos eventos de segurança da informação em tempo real, garantindo a integridade do dado raw como evidência legal;

11.4.18. Informar os eventos que compõem um alerta e/ou incidente de segurança, identificado pelas regras de correlação da solução, referenciando estes eventos raw a partir do evento de alerta/incidente;

11.4.19. Executar regras de correlação pré-programadas. Deve permitir a criação de

novas regras e a edição das existentes;

11.4.20. Identificar anomalias baseadas em eventos, tendências e análise de dados históricos;

11.4.21. Permitir o correlacionamento de eventos e alerta com dados existentes em listas (watchlist); permite também a criação de novas listas e a edição das existentes, tanto de forma automatizada quanto manual;

11.4.22. Deve ter capacidade de sumarizar múltiplos alertas idênticos automaticamente;

11.4.23. Deve identificar e correlacionar diferentes assinaturas de diferentes dispositivos possibilitando a identificação única de ataques particulares;

11.4.24. Permitir execução de regras agendadas, que rodam em frequência e horário especifico, sem ficarem ativas em tempo real;

11.4.25. Capacidade de fazer o correlacionamento entre eventos oriundos de qualquer tipo de dados dos dispositivos do ambiente tecnológico, nativamente e em tempo real;

11.4.26. Reinserir no próprio fluxo de correlacionamento os alertas gerados a partir de regras de correlação, visando correlacionar este alerta como novos eventos e/ou outros alertas no intuito de detectar padrões mais complexos de ameaças ou violações de conformidade;

11.4.27. Priorizar os eventos e alertas com base pelo menos nos seguintes critérios:

11.4.27.1. severidade do evento;

11.4.27.2. criticidade do ativo.

11.4.28. Desativar temporariamente regras que estejam gerando número excessivo de alertas num curto espaço de tempo, visando proteger o sistema contra-ataques onde se tenta inundar a interface com alertas para ocultar outros ataques em andamento;

11.4.29. Armazenar os eventos, alertas e incidentes na base de dados da solução;

11.4.30. Em tempo real, coletar e aplicar *parsing* (segmento do dado) nos eventos do dispositivo monitorado;

11.4.31. Filtrar e selecionar os eventos que serão inseridos na solução. Deve permitir a criação e alteração de filtros;

11.4.32. Fazer a agregação de eventos semelhantes que ocorrem dentro de um limite de tempo ou quantidade de eventos específicos, sendo que permite agregar tanto os eventos cuja única diferença seja o horário de ocorrência, quanto especificar quais campos do evento normalizado devem ser considerados para fins de agregação;

11.4.33. Armazenar o evento bruto (raw) por tempo virtualmente ilimitado (conforme políticas internas de retenção) para consultas futuras;

11.4.34. Deve ser capaz de ajustar o horário dos eventos, caso necessário, com base em limites de diferença de hora entre os eventos originais e a hora correta obtida pelo sistema através de sincronização de NTP com os servidores locais;

11.4.35. Suportar pesquisa automática dos ataques que foram detectados e permitir o armazenamento destas informações para fins de forense computacional e referências futuras;

11.4.36. Deve implementar funcionalidade de agendar relatórios de segurança em múltiplos perfis. Os relatórios deverão ser gerados automaticamente (agendados) com frequência e intervalo de tempo a serem definidos pela instituição, conforme perfis dos elementos gerenciados;

11.4.37. Apresentar relatórios de eventos, alertas e incidentes em nível técnico e gerencial os quais devem ter a possibilidade de serem gerados em PDF e HTML;

11.4.38. Capacidade de gerar alerta no primeiro, subsequente e em todos os eventos compatíveis em uma regra, inclusive com ações diferentes em cada um dos estágios;

11.4.39. Capacidade de gerar alerta no primeiro, subsequente e em todos os *thresholds* do correlacionamento em uma regra, inclusive com ações diferentes em cada um dos estágios;

11.4.40. Deverá possuir detalhes sobre cada incidente, incluindo:

11.4.40.1. contexto adicional a partir de fontes de ativos e de identidade externa;

11.4.40.2. o evento (s) – prima que constitui o incidente;

11.4.40.3. capacidade de alterar manualmente severidade do incidente, proprietário e status, bem como adicionar notas a um incidente.

11.5. **ARMAZENAMENTO**

11.5.1. A solução deve ser virtualmente ilimitada no armazenamento dos dados de origem, assim como os dados usados nos relatórios, alertas e painéis de monitoramento, atendendo aos requisitos de retenção de dados da própria contratante;

11.5.2. Capacidade de definir política de retenção dos dados em on-line, near-line e off-line, onde:

11.5.2.1. on-line: dado mantido no banco de dados da solução, disponíveis apara consulta imediata;

11.5.2.2. near-line: dados que não estão no banco de dados da solução, mas encontram-se arquivados em dispositivos de acesso direto pelo mesmo, podendo ser recuperados imediatamente para consulta;

11.5.2.3. off-line: dados que estão arquivados em mídias externas de backup (CD, DVD, fita. etc), sem acesso direto pela solução e que precisam ser restaurados e reativados para consulta.

11.5.3. A política de retenção de dados da contratante pode ser alterada conforme sua melhor conveniência, portanto a solução deve ser flexível para tal;

11.5.4. Armazenamento dos eventos em formato original (“raw”), garantindo a sua integridade por meio de hash’s de segurança;

11.5.5. Armazenar logs por tempo determinado e configurável, conforme necessidade;

11.5.6. Permite o expurgo dos dados de forma manual e automática. Quando automática, permite a configuração do período de expurgo;

11.5.7. Prever acesso único e exclusivo aos dados, implementação de políticas de controle de acesso, auditoria e controle de tráfego dos dados;

11.5.8. Possuir a compressão automática de dados indexados para reduzir os requisitos de armazenamento;

11.5.9. Possuir controle granular sobre o que acontece com os dados à medida que envelhece. Dados antigos podem ser rolou para armazenamento externo / mais barato e / ou excluídos;

11.6. **DIMENSIONAMENTO DA SOLUÇÃO**

11.6.1. Todas as funções supra citadas deverão ser executadas pela mesma solução tecnológica. Caso sejam necessários componentes externos, os mesmos devem fazer parte da solução proposta;

11.6.2. A solução deve ser escalável e flexível, podendo ser executada em servidores padrões de mercado (arquitetura x86 ou 64) independente de fabricante ou appliance do próprio fabricante, a serem providenciados pela própria Instituição conforme os requisitos informados pela fornecedora;

11.6.3. Solução deve possuir capacidade de se integrar com Storages (SAN/NAS) de mercado para armazenamento de dados;

11.6.4. Os dados dos dispositivos do ambiente tecnológico devem ser armazenados em base de dados única (parte integrante da solução);

11.6.5. A solução deve garantir o processamento do fluxo de eventos gerados pelos dispositivos, sem limitação por dispositivo em qualquer momento (pico vale ou operação normal);

11.6.6. A arquitetura de TI (requisitos de servidores e dispositivos de rede) devem ser apresentada pela fornecedora e ser parte integrante do projeto técnico;

11.7. **RECURSOS TECNOLÓGICOS**

11.7.1. Coleta, normalização, classificação, correlação e armazenamento dos dados dos dispositivos do ambiente tecnológico;

11.7.2. Monitoramento em tempo real dos dispositivos do ambiente tecnológico;

11.7.3. Correlacionamento de eventos entre múltiplas fontes;

11.7.4. Classificação de alertas em níveis de criticidade;

11.7.5. Deve possuir mecanismos que proporcionem a exibição da informação de forma amigável e compreensível após coleta e normalização dos eventos;

11.7.6. Deve classificar eventos de acordo com os grupos de ativos afetados e sua criticidade para o negócio da empresa, por meio de parâmetros pré-definidos;

11.7.7. Deve possuir regras de correlação prontas baseados em padrões de mercado;

11.7.8. Deve permitir a criação de regras de correlação específicas e customizadas, diferentes da nativa, e possuir capacidade de copiá-las para outras instâncias;

11.7.9. Deve suportar criação de regras de maneira gráfica, não necessitando de linguagem de script ou de programação;

11.7.10. Deve permitir a identificação de anomalias a partir de eventos inéditos e através de análise histórica do comportamento de rede (flows);

11.7.11. Deve permitir a emissão de alertas para outros sistemas e usuário via SNMP, SMTP e SYSLOG conforme o caso;

11.7.12. Ter a capacidade de armazenar os dados, aplicando a função de hash com o objetivo de verificar integridade de eventos e flows, para futuras análises forenses (Perícia Técnica);

11.7.13. Deve possuir um banco de dados próprio ou, caso não possua, banco de dados não relacional para armazenamento dos dados coletados. Caso seja utilizado banco de dados de terceiros, as licenças devem ser fornecidas juntamente com a solução. Deve possibilitar que os dados no banco sejam extraídos em forma de relatório em CSV ou encaminhados via CEF para outras soluções.

11.7.14. Os eventos devem ser armazenados em formato “raw” e formato “correlacionado”;

11.7.15. Manter todos os eventos coletados em base de dados própria, otimizada para tratamento de grandes volumes de dados;

11.7.16. Suportar, através de ferramentas de monitoramento, funcionalidades e

capacidade de apresentar múltiplas janelas com diferentes visualizações, para melhoria na gestão da atividade de monitoramento de segurança e acompanhamento de incidente conhecido como “dashboard”;

11.7.17. Implementar filtros de condições nos eventos coletados incluindo a capacidade de armazenar um filtro para utilização futura;

11.7.18. Permitir pesquisas ad hoc nos eventos gerados sem necessidade de parsing ou pré-processamento dos eventos recebidos a fim de agilizar o processo de análise e forense;

11.7.19. Plataforma universal de dados, permitindo coletar e analisar os dispositivos do ambiente tecnológico a fim de aumentar a capacidade analítica da solução em caso de investigações de segurança avançadas, sem necessidade de customizações a serem realizadas pelo fornecedor ou provedor de serviços especializados;

11.7.20. Arquitetura escalável para volume de dados virtualmente ilimitados, executada sobre servidores arquitetura x86 ou x64, independente de fornecedor e com os principais Sistemas Operacionais do mercado (Windows e Unix-based) em suas principais versões;

11.7.21. Possibilidade de definir o timestamp conforme o dado de origem;

11.7.22. Gerenciamento de ciclo de vida do dado, da coleta, armazenamento (como movimentação automática entre disco local e storage) e rotação (armazenamento externo e/ou eliminação do dado) – com regras e parâmetros;

11.7.23. Arquitetura tolerante a falhas e com balanceamento de carga, com replicação dos dados e serviços;

11.7.24. Indexar todos os dados, não modificando o formato original e torná-lo pesquisável (nenhum esquema pré-definido, ou normalização de dados / redução em tempo de coleta);

11.7.25. Possuir capacidade de colocar diferentes tipos de dados em diferentes índices para desempenho de pesquisa ideal ou fins de segregação de dados;

11.7.26. A solução deve possuir sistema de auditoria de uso. Cada evento de auditoria deve possuir, no mínimo, os seguintes campos:

11.7.26.1. data e horário da ação executada pelo usuário;

11.7.26.2. identificação do usuário que executou a ação;

11.7.26.3. informação sobre a ação executada;

11.7.26.4. identificador sequencial do evento;

11.8. **RELATÓRIOS**

11.8.1. Deve possuir funcionalidade emissão de relatórios com capacidade para geração destes relatórios para arquivo PDF e HTML;

11.8.2. Permitir o agendamento de geração de relatórios periódicos e notificar/enviar automaticamente os relatórios gerados para os destinatários dos mesmos;

11.8.3. Deverá apresentar painéis gráficos (dashboards) com indicativos de situações diversas, facilmente configuráveis e com ferramentas que facilitem a criação pelos usuários;

11.8.4. Deverá permitir a fácil criação de uma vasta gama de efeitos visuais (não se limitando a, relatórios pré-definidos e fixos):

11.8.4.1. tabelas;

11.8.4.2. gráfico com agrupamento em período de tempo;

11.8.4.3. gráficos de linhas;

11.8.4.4. gráficos de barras;

11.8.4.5. gráficos de área;

11.8.4.6. gráficos de pizza;

11.8.4.7. gráficos de dispersão;

11.8.4.8. medidores radiais, enchimento e marcadores;

11.8.4.9. mapas Geo – IP;

11.8.5. Deverá permitir para todos os gráficos, capacidade fácil mudar títulos, legendas e rótulos do eixo e as configurações;

11.8.6. Deverá ter capacidade de integração com as estruturas externas de visualização e opções (D3, Tableau, etc..) para visualizações adicionais por meio de conectores ODBC ou similares;

11.8.7. Capacidade de geração de relatórios Ad Hoc e compartilhamento do resultado final com outros usuários;

11.8.8. Possuir relatórios e dashboards com capacidades de *drill-down*, detalhando do indicador gerencial para o evento raw que o compõe;

11.8.9. Deverá possuir os relatórios e dashboards contem simples opções de filtragem e caixas de formulário para ajudar os usuários a filtrar os dados para o que é de seu interesse;

11.8.10. Gerar relatórios ocultando campos sensíveis dos eventos (senhas, números de cartões de credito, importâncias monetárias e outros similares);

11.8.11. Capacidade de criação de novos painéis gráficos (dashboards) e alteração dos existentes;

11.8.12. Capacidade de criação de modelos de relatórios e alteração dos existentes através de interface gráfica;

11.9. **CONSOLE DE ADMINISTRAÇÃO**

11.9.1. Funcionalidades para a administração da solução com interface gráfica via browser que atenda de forma intuitiva, utilizada para as atividades de administração, configuração e gerenciamento do ambiente;

11.9.2. Possuir acesso controlado e autenticado por usuário;

11.9.3. Possuir capacidade de integração com Microsoft Active Directory e bases LDAP (Lightweight Directory Access Protocol) inclusive na sua versão Open Source OPENLDAP, para autenticação de usuários;

11.9.4. Fornecer visualização e ações diferenciadas por perfis de acesso;

11.9.5. As visualizações e ações devem ser customizadas por grupos de usuários, conforme critério da instituição;

11.9.6. Ter capacidade de efetuar a segregação de funções dos usuários da solução;

11.9.7. Segregação de visualização de eventos, alertas, conteúdo de dashboard e de relatórios por usuários, sem necessidade de criar visualizações, dashboards e relatórios customizados para cada grupo de usuários;

11.9.8. Capacidade de gerenciamento e configuração centralizados de todos os componentes distribuídos da solução;

11.9.9. Capacidade de atualização centralizada de todos os componentes da solução.

11.10. **REQUISITOS DE IMPLANTAÇÃO**

11.10.1. A CONTRADADA será responsável pela instalação e configuração da Solução,

de acordo com a necessidade e as políticas de segurança do Ambiente de TI;

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

11.10.3. 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;

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

11.10.5. A instalação e suporte deverá ser realizado por técnico certificado na Solução;

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

11.10.7. A Contratada deverá substituir, sempre que exigido pela Contratante, o técnico certificado na solução cuja atuação, permanência ou comportamento forem julgados prejudiciais, inconvenientes ou insatisfatórios à instalação e suporte;

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

11.11. **REQUISITOS DE TREINAMENTO**

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

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

11.11.3. 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;

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

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

11.12. **REQUISITOS DE MANUTENÇÃO E GARANTIA**

11.12.1. 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;

11.12.2. A instalação e suporte deverás ser prestado mediante manutenção corretiva, preventiva e suporte técnico, a fim de manter a Solução em perfeitas condições de uso, sem qualquer ônus adicional para a Contratante;

11.12.3. Entende-se por manutenção corretiva aquela destinada a remover os defeitos apresentados pela Solução: *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;

11.12.4. Entende-se por manutenção preventiva aquela destinada a atualizar *drivers*,

BIOS e outros componentes de *software* o u *hardware* que sejam disponibilizados pelo fabricante;

11.12.5. 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;

11.12.6. 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;

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

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

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

11.12.10. 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;

11.12.11. 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. 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 em parcela única, 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 ANCINE no 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 Lima**, **Analista Administrativo**, em 18/04/2017, às 12:02, 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 19/04/2017, às 13:29, 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 19/04/2017, às 13:34, 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 **0386148** e o código CRC **E1F95021**.