

TERMO DE REFERÊNCIA

PROCESSO Nº 01416.000665/2016-70

Aquisição de Solução Corporativa de Antivírus

Gerência de Tecnologia da Informação Coordenação de Infraestrutura e Segurança

1. OBJETO

Aquisição de Solução Corporativa de Antivírus para proteção de estações de trabalho, servidores e dispositivos móveis, **com serviço de instalação**, atualização de versão, manutenção da garantia de atualização de versões e suporte técnico pelo período 12(doze) meses, como medida de adequação, padronização e modernização do parque computacional e suporte técnico na Agência Nacional de Cinema.

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

A Solução Corporativa de Proteção contribui para a integridade e disponibilidade da segurança da informação do ambiente computacional da Ancine. Aquisições para viabilizar ações dessa natureza encontram-se devidamente previstas no Plano Diretor de Tecnologia da Informação (PDTI) 2015-2016. Espera-se com a aquisição maior proteção do ambiente de TI da Ancine resultando no aumento da disponibilidade e integridade do ambiente.

3. JUSTIFICATIVA

A ANCINE utiliza a ferramenta de Proteção Corporativa de antivírus como principal garantia de proteção contra códigos maliciosos e segurança das informações armazenadas nos servidores de rede e nas estações de trabalho.

O ambiente computacional da agência deve estar tecnologicamente atualizado para atender as demandas relativas à necessidade de crescimento da rede corporativa. Com o término da garantia de atualização, das atuais licenças dos programas que compõem a solução de antivírus, as atualizações de novas versões dos programas e das bases de dados (lista de vírus e vacinas) não serão executadas automaticamente, acarretando um aumento no tempo para obtenção das vacinas contra novos vírus, gerando vulnerabilidades na rede da agência, assim como possibilitando a entrada de vírus no ambiente da rede corporativa da ANCINE.

4. LOCAL DA INSTALAÇÃO E ASSISTÊNCIA TÉCNICA:

Escritório Central da ANCINE no Rio de Janeiro.
Endereço: Av. Graça Aranha, nº. 35, 6º andar.
Centro – Rio de Janeiro – RJ.

5. PRAZO DE ENTREGA

- 5.1 A licitante vencedora deverá disponibilizar a solução, com todos os componentes especificados neste Termo de Referência, em até 30 (trinta) dias corridos após assinatura do Contrato;

- 5.2 Caso se veja impossibilitada de cumprir o prazo estipulado para a entrega da solução e componentes, a licitante vencedora deverá apresentar justificativas escritas e devidamente comprovadas, apoiando o pedido de prorrogação na ocorrência de fato superveniente, excepcional ou imprevisível, estranho à vontade das partes, que altere fundamentalmente as condições do contrato.

6. CONDIÇÕES DE FORNECIMENTO:

- 6.1. Quando das propostas de fornecimento da solução, os licitantes devem observar as seguintes condições:
- 6.1.1 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;
- 6.1.2 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;
- 6.1.3 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:
- 6.1.3.1 Produzidos no País;
- 6.1.3.2 Produzidos ou prestados por empresas brasileiras;
- 6.1.3.3 Produzidos ou prestados por empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País.

7. OBRIGAÇÕES DA ANCINE

- 7.1 São obrigações da ANCINE:
- 7.1.1 Receber o objeto no prazo e condições estabelecidas no Edital e seus anexos;
- 7.1.2 Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo;
- 7.1.3 Comunicar à Contratada, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;
- 7.1.4 Acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através de comissão/servidor especialmente designado;
- 7.1.5 Efetuar o pagamento à Contratada no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no Edital e seus anexos;
- 7.2 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.
- 7.3 Disponibilizar acesso administrativo, e janela de mudança adequada para desinstalação do software antivírus anterior.
- 7.4 Disponibilizar acesso administrativo, e janela de mudança adequada para instalação do software antivírus novo, objeto deste termo/licitação.
- 7.5 O tempo adequado de janela de mudança para servidores e/ou equipamentos em trânsito, pode exceder o prazo máximo estabelecido para a maioria dos equipamentos.
- 7.6 Um plano de mudança deve ser fornecido pela Ancine, identificando caso a caso, com suas respectivas janelas de mudança.

8. OBRIGAÇÕES DA LICITANTE VENCEDORA

- 8.1 A Contratada deve cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:
- 8.1.1 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;
- 8.1.2 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);
- 8.1.3 Substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste Termo de Referência, o objeto com avarias ou defeitos;

- 8.1.4 Comunicar à Contratante, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação, conforme item 8.2 deste Termo de Referência;
- 8.1.5 Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;
- 8.1.6 Indicar preposto para representá-la durante a execução do contrato;
- 8.1.7 Fornecer, sempre que houver atualização de versão ou da lista de produtos, a relação atualizada das alterações ocorridas nas novas versões dos produtos do fabricante do software.

9. ESPECIFICAÇÕES TÉCNICAS

- 9.1 Para fins de execução do contrato, a CONTRATADA deverá atender os seguintes requisitos técnicos, e também a outras previsões constantes neste Termo de Referência. Todos os detalhes técnicos específicos de cada funcionalidade da solução estão descritos a seguir e constituem o conjunto de funcionalidades obrigatórias da solução completa.
- 9.2 O direito de uso das licenças dos softwares é permanente, sendo o direito de atualização das versões, das atualizações das bases de dados (lista de vírus e vacinas), e dos serviços de suporte pelo período estipulado na cláusula de garantia;
- 9.3 Possibilidade de instalação dos clientes em servidores, estações de trabalho e máquinas virtualizadas de forma remota via console de gerenciamento com opção de remoção de soluções antivírus previamente instaladas;
- 9.4 A opção de remoção das soluções acima deve ser feita junto ao processo de instalação do cliente, ou seja, sem a necessidade de se instalar/usar um módulo separado para esta ação;
- 9.5 A especificação do objeto licitado é composta de licença de software para console de gerenciamento e para estações de trabalho, com serviço de suporte técnico e atualização de versão, de forma a obedecer ao quantitativo explicitado na planilha a seguir:

	Subitem	Produtos	Composta de:	Qtde.
Item I	1	Aquisição de Solução Corporativa de Antivírus.	Antivírus para estações de trabalho, servidores e dispositivos moveis.	1100
	2	Aquisição de Solução Corporativa de Antivírus para Servidor E-mail.	Antivírus para correio eletrônico	1200
	3	Aquisição de Solução Corporativa de Proteção de Ambiente Colaborativo	Antivírus para SharePoint	1100
	4	Instalação e Configuração	Serviço de Instalação e Configuração dos Produtos	1

10. DETALHAMENTO DAS ESPECIFICAÇÕES

10.1 Subitem 1: Aquisição de Solução Corporativa de Antivírus, com as seguintes características técnicas e funcionalidades mínimas:

10.1.1 Servidor de Administração e Console Administrativa

10.1.1.1 Compatibilidade:

- 10.1.1.1.1 Microsoft Windows Server 2008 ou superior
- 10.1.1.1.2 Microsoft Windows Server 2008 x64 ou superior

10.1.1.2 Características:

- 10.1.1.2.1 Deve permitir administração centralizada por console único de gerenciamento;

- 10.1.1.2.2 As configurações do Antivírus, AntiSpyware, Firewall e Proteção Contra Intrusos deverão ser realizadas através da mesma console;
- 10.1.1.2.3 A console deve ser acessada via WEB (HTTPS) ou MMC;
- 10.1.1.2.4 Fornecer atualizações do produto e das definições de vírus e proteção contra intrusos;
- 10.1.1.2.5 A console de gerenciamento deve permitir travar as configurações por senha nos clientes servidores e estações físicos e virtuais definindo permissões para que somente o administrador possa alterar as configurações, desinstalar ou parar o serviço do cliente;
- 10.1.1.2.6 A console de gerenciamento deve permitir ao administrador travar separadamente os itens e cada subitens de acesso as configurações do cliente;
- 10.1.1.2.7 Compatibilidade com solução de alta disponibilidade;
- 10.1.1.2.8 Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;
- 10.1.1.2.9 Capacidade de instalar remotamente a solução de segurança em smartphones e tablets;
- 10.1.1.2.10 Capacidade de gerenciar estações de trabalho e servidores (tanto Windows como Linux e Mac) protegidos pela solução antivírus;
- 10.1.1.2.11 Capacidade de gerenciar smartphones e tablets protegidos pela solução antivírus;
- 10.1.1.2.12 Capacidade de monitorar diferentes subnets de rede, grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção;
- 10.1.1.2.13 Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não tenha proteção instalada, reportar ao Administrador para que seja tomada a decisão de instalação do produto ou não;
- 10.1.1.2.14 Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar as máquinas por VLAN;
- 10.1.1.2.15 Deve fornecer informações gerenciais dos computadores;
- 10.1.1.2.16 Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
- 10.1.1.2.17 Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão.
- 10.1.1.2.18 Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
- 10.1.1.2.19 Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
- 10.1.1.2.20 Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
- 10.1.1.2.21 Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
- 10.1.1.2.22 Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;
- 10.1.1.2.23 Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo.
- 10.1.1.2.24 Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF.

Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows Server;

- 10.1.1.2.25 Deve possuir capacidade de exportação de dados para geração de relatórios;
- 10.1.1.2.26 Capacidade de realização de tarefas (varredura, atualização, instalação, etc), inclusive de máquinas que estejam em subnets diferentes do servidor;
- 10.1.1.2.27 Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);

- 10.1.1.2.28 Capacidade de realizar atualização incremental de vacinas nos computadores clientes;
- 10.1.1.2.29 Capacidade de reportar vulnerabilidades de softwares presentes nos computadores.
- 10.1.1.2.30 Capacidade de realizar levantamento de hardware de todas as máquinas clientes;
- 10.1.1.2.31 Capacidade de realizar levantamento instantâneo de aplicativos de todas as máquinas clientes;
- 10.1.1.2.32 Capacidade de diferenciar máquinas virtuais de máquinas físicas;

10.1.2 Estações Windows

10.1.2.1 Compatibilidade:

Microsoft Windows 7 ou superior

10.1.2.2 Características:

- 10.1.2.2.1 Deve prover as seguintes proteções:
 - 10.1.2.2.1.1 Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
 - 10.1.2.2.1.2 Antivírus de Web (módulo para verificação de sites e downloads contra vírus)
 - 10.1.2.2.1.3 Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos)
 - 10.1.2.2.1.4 Firewall com IDS
 - 10.1.2.2.1.5 Autoproteção (contra-ataques aos serviços/processos do antivírus)
 - 10.1.2.2.1.6 Controle de dispositivos externos
 - 10.1.2.2.1.7 Controle de execução de aplicativos
 - 10.1.2.2.1.8 Controle de vulnerabilidades do Windows e dos aplicativos instalados
- 10.1.2.2.2 As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários periodicamente, independentemente do nível das ameaças encontradas no período (alta, média ou baixa).
- 10.1.2.2.3 Capacidade de automaticamente desabilitar o Firewall do Windows (caso exista) durante a instalação, para evitar incompatibilidade com o Firewall da solução;
- 10.1.2.2.4 Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
- 10.1.2.2.5 Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
- 10.1.2.2.6 Capacidade de adicionar aplicativos a uma lista de "aplicativos confiáveis", onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;
- 10.1.2.2.7 Capacidade de pausar automaticamente varreduras agendadas ou conceder automaticamente recursos caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- 10.1.2.2.8 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não a tomar a partir da extensão do arquivo;
- 10.1.2.2.9 Capacidade de verificar somente arquivos novos e alterados;
- 10.1.2.2.10 Capacidade de verificar objetos usando heurística;
- 10.1.2.2.11 O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
 - 10.1.2.2.11.1 Perguntar o que fazer, ou;
 - 10.1.2.2.11.2 Bloquear acesso ao objeto;
 - 10.1.2.2.11.3 Apagar o objeto ou tentar desinfecção (de acordo com a configuração pré-estabelecida pelo administrador);
- 10.1.2.2.12 Caso positivo de desinfecção:
 - 10.1.2.2.12.1 Restaurar o objeto para uso;
- 10.1.2.2.13 Caso negativo de desinfecção:
 - 10.1.2.2.13.1 Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

- 10.1.2.2.14 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.
- 10.1.2.2.15 Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, e SMTP, assim como conexões criptografadas (SSL) para POP3;
- 10.1.2.2.16 Capacidade de verificar links inseridos em e-mails contra phishings;
- 10.1.2.2.17 Capacidade de verificar tráfego SSL nos browsers mais utilizados no mercado.
- 10.1.2.2.18 Capacidade de verificação de corpo e anexos de e-mails usando heurística;
- 10.1.2.2.19 O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:
 - 10.1.2.2.19.1 Perguntar o que fazer, ou;
 - 10.1.2.2.19.2 Bloquear o e-mail;
- 10.1.2.2.20 Apagar o objeto ou tentar desinfecção (de acordo com a configuração pré-estabelecida pelo administrador);
- 10.1.2.2.21 Caso positivo de desinfecção:
 - 10.1.2.2.21.1 Restaurar o e-mail para o usuário;
- 10.1.2.2.22 Caso negativo de desinfecção:
 - 10.1.2.2.22.1 Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);
- 10.1.2.2.23 Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena.
- 10.1.2.2.24 Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados.
- 10.1.2.2.25 Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador.
- 10.1.2.2.26 Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (Java Script, Visual Basic Script, etc), usando heurísticas;
- 10.1.2.2.27 Deve ter suporte total ao protocolo IPv6;
- 10.1.2.2.28 Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;
- 10.1.2.2.29 Na verificação de tráfego web, caso encontrado código malicioso o programa deve:
 - 10.1.2.2.29.1 Perguntar o que fazer, ou;
 - 10.1.2.2.29.2 Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;
- 10.1.2.2.30 Permitir acesso ao objeto;
- 10.1.2.2.31 O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:
 - 10.1.2.2.31.1 Verificação *on-the-fly*, onde os dados são verificados enquanto são recebidos em tempo real, ou;
 - 10.1.2.2.31.2 Verificação de *buffer*, onde os dados são recebidos e armazenados para posterior verificação.
- 10.1.2.2.32 Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web.
- 10.1.2.2.33 Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas.
- 10.1.2.2.34 Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa.
- 10.1.2.2.35 Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas.
- 10.1.2.2.36 Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;
- 10.1.2.2.37 Deve possuir módulo IDS (*Intrusion Detection System*) para proteção contra *port scans* e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas.

- 10.1.2.2.38 O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
- 10.1.2.2.38.1 Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
- 10.1.2.2.38.2 Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.
- 10.1.2.2.39 Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:
 - 10.1.2.2.39.1 Armazenamento removível
 - 10.1.2.2.39.2 Impressoras
 - 10.1.2.2.39.3 CD/DVD
 - 10.1.2.2.39.4 Dispositivos de fita
 - 10.1.2.2.39.5 Dispositivos multifuncionais
 - 10.1.2.2.39.6 Leitores de smart card
 - 10.1.2.2.39.7 Dispositivos de sincronização Mobile
 - 10.1.2.2.39.8 Wi-Fi
 - 10.1.2.2.39.9 Adaptadores de rede externos
 - 10.1.2.2.39.10 Dispositivos MP3 ou smartphones
 - 10.1.2.2.39.11 Dispositivos Bluetooth
- 10.1.2.2.40 Capacidade de liberar acesso temporário a um dispositivo específico para um usuário específicos, sem a necessidade de desabilitar a proteção, sem desabilitar o gerenciamento central ou de intervenção local do administrador na máquina do usuário.
- 10.1.2.2.41 Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário.
- 10.1.2.2.42 Capacidade de limitar a escrita e leitura em dispositivos de armazenamento.
- 10.1.2.2.43 Capacidade de configurar novos dispositivos por Class ID/Hardware ID
- 10.1.2.2.44 Capacidade de limitar a execução de aplicativos por hash MD5, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor.
- 10.1.2.2.45 Capacidade de bloquear execução de aplicativo que está em armazenamento externo.
- 10.1.2.2.46 Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo.
- 10.1.2.2.47 Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso a web.
- 10.1.2.2.48 Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso a web.

10.1.3 Estações e Servidores Mac OS X

10.1.3.1 Compatibilidade:

- 10.1.3.1.1 Mac OS X 10.7 ou superior

10.1.3.2 Características:

- 10.1.3.2.1 Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
- 10.1.3.2.2 Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
- 10.1.3.2.3 A instalação e primeira execução do produto deve ser feita sem necessidade de reinicialização do computador;
- 10.1.3.2.4 Deve possuir suportes a notificações de ameaças detectadas ao usuário;
- 10.1.3.2.5 As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários periodicamente independentemente do nível das ameaças encontradas no período (alta, média ou baixa).

- 10.1.3.2.6 Capacidade de voltar para a base de dados de vacina anterior;
- 10.1.3.2.7 Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;
- 10.1.3.2.8 Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação.
- 10.1.3.2.9 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não a tomar a partir da extensão do arquivo;
- 10.1.3.2.10 Capacidade de verificar somente arquivos novos e alterados;
- 10.1.3.2.11 Capacidade de verificar objetos usando heurística;
- 10.1.3.2.12 Capacidade de agendar uma pausa na verificação;
- 10.1.3.2.13 O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
 - 10.1.3.2.14 Perguntar o que fazer, ou tentar efetuar a limpeza;
 - 10.1.3.2.15 Bloquear acesso ao objeto;
- 10.1.3.3 Apagar o objeto ou tentar desinfecção (de acordo com a configuração pré-estabelecida pelo administrador);
- 10.1.3.4 Caso positivo de desinfecção:
 - 10.1.3.4.1 Restaurar o objeto para uso;
- 10.1.3.5 Caso negativo de desinfecção:
 - 10.1.3.5.1 Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
- 10.1.3.6 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
- 10.1.3.7 Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o antivírus e iniciar o antivírus pela linha de comando;
- 10.1.3.8 Capacidade de ser instalado e administrado pela mesma console central de gerenciamento;

10.1.4 Estações de trabalho Linux

- 10.1.4.1 Compatibilidade:
 - 10.1.4.1.1 *Plataforma 32 ou 64 bits:*
 - 10.1.4.1.1.1 Red Hat 5.x ou superior;
 - 10.1.4.1.1.2 CentOS 6 ou superior;
 - 10.1.4.1.1.3 Ubuntu Server 11.10 LTS ou superior;
- 10.1.4.2 Características:
 - 10.1.4.2.1 Deve prover as seguintes proteções:
 - 10.1.4.2.1.1 Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
 - 10.1.4.2.1.2 As vacinas devem ser atualizadas pelo fabricante de periodicamente.
 - 10.1.4.2.2 Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
 - 10.1.4.2.2.1 Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
 - 10.1.4.2.2.2 Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfecção ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;
 - 10.1.4.2.2.3 Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
 - 10.1.4.2.2.4 Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.
 - 10.1.4.2.3 Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem necessidade de outros softwares;

- 10.1.4.2.4 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não a tomar a partir da extensão do arquivo;
- 10.1.4.2.5 Capacidade de verificar objetos usando heurística;
- 10.1.4.2.6 Deve possuir módulo de administração remoto.

10.1.5 Servidores Windows

10.1.5.1 Compatibilidade:

- 10.1.5.1.1 Microsoft Windows Server 2008 ou superior;
- 10.1.5.1.2 Microsoft Windows Hyper-V Server 2008 ou superior;

10.1.5.2 Características:

- 10.1.5.2.1 Deve prover as seguintes proteções:
- 10.1.5.2.2 Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
- 10.1.5.2.3 Autoproteção contra ataques aos serviços/processos do antivírus
- 10.1.5.2.4 Firewall com IDS
- 10.1.5.2.5 Controle de vulnerabilidades do Windows e dos aplicativos instalados
- 10.1.5.3 Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
- 10.1.5.4 As vacinas devem ser atualizadas pelo fabricante periodicamente em um espaço de tempo aceitável.
- 10.1.5.5 Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
 - 10.1.5.5.1 Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
 - 10.1.5.5.2 Gerenciamento de tarefa (criar ou excluir tarefas de verificação)
 - 10.1.5.5.3 Leitura de configurações
 - 10.1.5.5.4 Modificação de configurações
 - 10.1.5.5.5 Gerenciamento de Backup e Quarentena
 - 10.1.5.5.6 Visualização de relatórios
 - 10.1.5.5.7 Gerenciamento de relatórios
 - 10.1.5.5.8 Gerenciamento de chaves de licença
 - 10.1.5.5.9 Gerenciamento de permissões (adicionar/excluir permissões acima)
- 10.1.5.6 O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
 - 10.1.5.6.1 Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
 - 10.1.5.6.2 Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.
- 10.1.5.7 Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc.)
- 10.1.5.8 Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (*uninterruptible Power supply – UPS*)
- 10.1.5.9 Em caso erros, deve ter capacidade de criar *logs* e *traces* automaticamente, sem necessidade de outros softwares;
- 10.1.5.10 Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor.
- 10.1.5.11 Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado nos servidores.

- 10.1.5.12 Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, removendo este antivírus;
- 10.1.5.13 Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
- 10.1.5.14 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- 10.1.5.15 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não a tomar a partir da extensão do arquivo;
- 10.1.5.16 Capacidade de verificar somente arquivos novos e alterados;
- 10.1.5.17 Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc)
- 10.1.5.18 Capacidade de verificar objetos usando heurística;
- 10.1.5.19 Capacidade de configurar diferentes ações para diferentes tipos de ameaças;
- 10.1.5.20 O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
 - 10.1.5.20.1 Perguntar o que fazer, ou;
 - 10.1.5.20.2 Bloquear acesso ao objeto;
 - 10.1.5.20.3 Apagar o objeto ou tentar desinfecção (de acordo com a configuração pré-estabelecida pelo administrador);
 - 10.1.5.20.4 Caso positivo de desinfecção:
 - 10.1.5.20.5 Restaurar o objeto para uso;
 - 10.1.5.20.6 Caso negativo de desinfecção:
 - 10.1.5.20.7 Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
- 10.1.5.21 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.
- 10.1.5.22 Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

10.1.6 Servidores Linux

10.1.6.1 Compatibilidade:

10.1.6.1.1 Plataforma 32 e 64 bits:

- 10.1.6.1.1.1 Red Hat 5.x ou superior;
- 10.1.6.1.1.2 CentOS 6 ou superior;
- 10.1.6.1.1.3 Ubuntu Server 11.10 ou superior;

10.1.6.2 Características:

- 10.1.6.2.1 Deve prover as seguintes proteções:
 - 10.1.6.2.1.1 Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
 - 10.1.6.2.1.2 As vacinas devem ser atualizadas pelo fabricante periodicamente.
- 10.1.6.2.2 Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;
- 10.1.6.2.3 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- 10.1.6.2.4 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo;
- 10.1.6.2.5 Capacidade de verificar objetos usando heurística;
- 10.1.6.2.6 Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena

- 10.1.6.2.7 Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados
- 10.1.6.2.8 Deve possuir módulo de administração remota.

10.1.7 Smartphones e tablets

10.1.7.1 Compatibilidade:

- 10.1.7.1.1 Apple iOS 8.0 ou superior;
- 10.1.7.1.2 Windows PHONE 8.1 ou superior;
- 10.1.7.1.3 Android OS 4.1.1 ou superior;

10.1.7.2 Características:

10.1.7.2.1 Deve prover as seguintes proteções:

10.1.7.2.1.1 Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:

- 10.1.7.2.1.1.1 Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser.
- 10.1.7.2.1.1.2 Arquivos abertos no smartphone
- 10.1.7.2.1.1.3 Programas instalados usando a interface do smartphone

10.1.7.2.1.2 Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;

- 10.1.7.2.2 Deverá atualizar as bases de vacinas de modo agendado;
- 10.1.7.2.3 Deverá bloquear spams de SMS através de Black lists;
- 10.1.7.2.4 Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado;
- 10.1.7.2.5 Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo.
- 10.1.7.2.6 Deverá ter firewall pessoal;
- 10.1.7.2.7 Capacidade de detectar Jailbreak em dispositivos iOS
- 10.1.7.2.8 Capacidade de bloquear o acesso a site em dispositivos
- 10.1.7.2.9 Capacidade de bloquear o acesso a sites phishing ou maliciosos
- 10.1.7.2.10 Capacidade de criar containers de aplicativos, separando dados corporativos de dados pessoais
- 10.1.7.2.11 Capacidade de configurar White e black list de aplicativos

10.1.8 Gerenciamento de dispositivos móveis (MDM):

10.1.8.1 Compatibilidade:

- 10.1.8.1.1 Dispositivos conectados através do Microsoft Exchange ActiveSync
 - 10.1.8.1.1.1 Apple iOS
 - 10.1.8.1.1.2 Windows Mobile e Windows Phone
 - 10.1.8.1.1.3 Android
- 10.1.8.1.2 Dispositivos com suporte ao Apple Push Notification (APNs) service
 - 10.1.8.1.2.1 Apple iOS 3.0 ou superior

10.1.8.2 Características:

- 10.1.8.2.1 Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange
- 10.1.8.2.2 Capacidade de ajustar as configurações de:
 - 10.1.8.2.2.1 Sincronização de e-mail
 - 10.1.8.2.2.2 Uso de aplicativos
 - 10.1.8.2.2.3 Senha do usuário
 - 10.1.8.2.2.4 Criptografia de dados

10.1.8.2.2.5 Conexão de mídia removível

- 10.1.8.2.3 Capacidade de instalar certificados digitais em dispositivos móveis
- 10.1.8.2.4 Capacidade de, remotamente, apagar todos os dados de dispositivos iOS
- 10.1.8.2.5 Capacidade de, remotamente, bloquear um dispositivo iOS

10.1.9 Criptografia:

10.1.9.1 Compatibilidade:

- 10.1.9.1.1 Microsoft Windows 7, 8, 8.1 e 10 32bits e superior
- 10.1.9.1.2 Microsoft Windows 7, 8, 8.1 e 10 64bits e superior

10.1.9.2 Características:

- 10.1.9.2.1 O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação.
- 10.1.9.2.2 Utilizar, no mínimo, algoritmo AES com chave de 256 bits.
- 10.1.9.2.3 Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário.
- 10.1.9.2.4 Capacidade de utilizar Single Sign-On para a autenticação de pré-boot.
- 10.1.9.2.5 Permitir criar vários usuários de autenticação pré-boot.
- 10.1.9.2.6 Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento.
- 10.1.9.2.7 Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:
- 10.1.9.2.8 Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes.
- 10.1.9.2.9 Criptografar todos os arquivos individualmente.
- 10.1.9.2.10 Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas.
- 10.1.9.2.11 Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha.
- 10.1.9.2.12 Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente. Nesta modalidade, os arquivos devem estar acessíveis para todas as máquinas gerenciadas pela mesma console de maneira transparente para os usuários.
- 10.1.9.2.13 Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados.

10.1.10 Servidores de gateway

- 10.1.10.1 As vacinas devem ser atualizadas pelo fabricante periodicamente.
- 10.1.10.2 Capacidade de verificar tráfego HTTP 1.0 e 1.1 (RFC 2616), FTP (RFC 959, 2389, Extensões para FTP) e FTP sobre HTTP;
- 10.1.10.3 Capacidade de definir listas de tipos de objetos que não serão verificados;
- 10.1.10.4 Capacidade de definir listas de servidores que não terão o tráfego verificado;
- 10.1.10.5 Capacidade de definir grupos de usuários e aplicar regras de verificação por grupos;
- 10.1.10.6 Capacidade de iniciar várias cópias do processo de antivírus;
- 10.1.10.7 Capacidade de escolher o tamanho reservado na memória para armazenamento dos arquivos que serão verificados;
- 10.1.10.8 Capacidade de escolher o tamanho do buffer do arquivo a ser verificado;
- 10.1.10.9 Capacidade de escolher o número máximo de objetos na fila de verificação;
- 10.1.10.10 Capacidade de definir o tempo máximo de verificação de um objeto;

10.2 Item 2: Aquisição de Solução Corporativa de Antivírus para Servidor de E-mail, com as seguintes características técnicas e funcionalidades mínimas:

10.2.1 Servidores de e-mail Windows

10.2.1.1 Compatibilidade:

- 10.2.1.1.1 Microsoft Windows Server 2008 x32 ou superior
- 10.2.1.1.2 Microsoft Windows Server 2008 x64 ou superior
- 10.2.1.1.3 Microsoft Exchange Server 2010 ou superior.

10.2.1.2 Características:

- 10.2.1.2.1 Deve utilizar as tecnologias VSAPI 2.0, 2.5 e 2.6;
- 10.2.1.2.2 Capacidade de iniciar várias cópias do processo de antivírus;
- 10.2.1.2.3 As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.
- 10.2.1.2.4 Capacidade de verificar pastas públicas, e-mails enviados, recebidos e armazenados contra vírus, spywares, adwares, worms, trojans e riskwares;
- 10.2.1.2.5 Capacidade de verificar pastas públicas e e-mails armazenados de forma agendada, utilizando as últimas vacinas e heurística;
- 10.2.1.2.6 O antivírus, ao encontrar um objeto infectado, deve:
 - 10.2.1.2.6.1 Desinfetar o objeto, notificando o recipiente, destinatário e administradores, ou
 - 10.2.1.2.6.2 Excluir o objeto, substituindo-o por uma notificação;
 - 10.2.1.2.6.3 Bloquear acesso ao objeto;
 - 10.2.1.2.6.4 Apagar o objeto ou tentar desinfetá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
 - 10.2.1.2.6.5 Caso positivo de desinfecção:
 - 10.2.1.2.6.6 Restaurar o objeto para uso;
- 10.2.1.2.7 Caso negativo de desinfecção:
 - 10.2.1.2.7.1 Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
 - 10.2.1.2.7.2 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.
- 10.2.1.2.8 Capacidade de enviar notificações sobre vírus detectados para o administrador, para o recipiente e remetente da mensagem infectada.
- 10.2.1.2.9 Capacidade de gravar logs de atividade de vírus nos eventos do sistema e nos logs internos da aplicação;
- 10.2.1.2.10 Capacidade de detectar disseminação em massa de e-mails infectados, informando o administrador e registrando tais eventos nos logs do sistema e da aplicação.

10.2.2 Servidores de e-mail Linux:

10.2.2.1 Compatibilidade:

10.2.2.1.1 Plataforma 32 ou 64 bits:

- 10.2.2.1.1.1 Red Hat 5.x ou superior;
- 10.2.2.1.1.2 CentOS 5.2 ou superior;
- 10.2.2.1.1.3 Ubuntu Server 10.04.2 LTS ou superior;

10.2.2.1.2 MTA:

- 10.2.2.1.2.1 Sendmail 8.12.x ou superior;
- 10.2.2.1.2.2 Postfix 2.x ou superior;

10.2.2.2 Características:

- 10.2.2.2.1 Capacidade de verificar o tráfego SMTP do servidor contra malware em todos os elementos do e-mail: cabeçalho, corpo e anexo;
- 10.2.2.2.2 Capacidade de notificar o administrador, o remetente e o destinatário caso um arquivo malicioso seja encontrado no e-mail;
- 10.2.2.2.3 Capacidade de quarentenar objetos maliciosos;
- 10.2.2.2.4 Capacidade de salvar backup dos objetos antes de tentativa de desinfecção;
- 10.2.2.2.5 Capacidade de fazer varredura no sistema de arquivos do servidor;
- 10.2.2.2.6 Capacidade de filtrar anexos por nome ou tipo de arquivo;
- 10.2.2.2.7 Capacidade de criar grupos de usuários para aplicar regras de verificação de e-mails;
- 10.2.2.2.8 Deve permitir gerenciamento via console WEB;
- 10.2.2.2.9 Deve ser atualizado de maneira automática via internet ou por servidores locais, com frequência horária.

10.3 Item 3: Aquisição de Solução Corporativa de Proteção de Ambiente Colaborativo, com as seguintes características técnicas e funcionalidades mínimas:

10.3.1 Compatibilidade:

- 10.3.1.1 Microsoft Windows Server 2008 x32 e superior
- 10.3.1.2 Microsoft Windows Server 2008 x64 e superior
- 10.3.1.3 Microsoft Sharepoint Server 2008 e superior.

10.3.2 Características:

- 10.3.2.1 Capacidade de impedir download e uploads de conteúdo em tempo real;
- 10.3.2.2 Capacidade de efetuar varredura em tempo real;
- 10.3.2.3 Deve apresentar interface de gerenciamento;
- 10.3.2.4 Deve apresentar dashboard com resumo das detecções, atualizações e demais informações relativas ao produto;
- 10.3.2.5 Deverá permitir verificação manual e agendada de repositórios de documentos do SharePoint;
- 10.3.2.6 Capacidade de realizar buscas em arquivos compactados;
- 10.3.2.7 Capacidade de gerar relatórios detalhados;
- 10.3.2.8 Deve ser capaz de atualizar definições de vírus de forma automática;
- 10.3.2.9 Deve prover quarentena para arquivos infectados.

10.4 Item 4: Instalação e Configuração

- 10.4.1 Serão de responsabilidade da licitante vencedora a instalação e a configuração da solução, bem como a desinstalação da solução existente;
- 10.4.2 A instalação deverá ser realizada em horário comercial e previamente marcada com a ANCINE;
- 10.4.3 A solução deverá ser instalada no servidor indicado pela ANCINE e nas estações de trabalhos, servidores e dispositivos móveis correspondentes;
- 10.4.4 Deverão ser feitas todas as configurações necessárias para o perfeito funcionamento da solução conforme especificação técnica;
- 10.4.5 A instalação deve ter início em até 5 (cinco) dias após a solicitação pelo setor responsável da licitante e ser concluída no prazo máximo de 30 (trinta) dias após o início da instalação, não sendo contabilizados o tempo das janelas de mudança adequadas para servidores e/ou equipamentos em trânsito, observadas junto com o setor responsável.
- 10.4.6 Deverá ser realizada, pela licitante vencedora, a configuração e a interconexão da máquina servidora com as clientes da solução;
- 10.4.7 Deverá ser realizada, pela licitante vencedora, a instalação, customização e operacionalização dos equipamentos envolvidos, atualizações de software, patches, clientes, etc. para suas mais recentes versões;

- 10.4.8 Deverá ser apresentado, pela licitante vencedora, resultados de testes de funcionamento da solução e duas funcionalidades;
- 10.4.9 Deverão ser realizados, pela licitante vencedora, os seguintes serviços de implementação:
- 10.4.9.1 Avaliação do ambiente proposto, pré-requisitos, compatibilidade e interoperabilidade;
 - 10.4.9.2 Análise de aplicação de *patches*, compatibilidade com os sistemas e aplicações da ANCINE;
 - 10.4.9.3 Definição da estratégia de implementação da solução e conexão com os servidores e clientes, mediante a apresentação das janelas de mudança para servidores e/ou equipamentos em transito, que deverá ocorrer no momento da solicitação de início de implementação tratada no item;
 - 10.4.9.4 Implementação dos mecanismos de proteção e configuração de todas as funcionalidades do produto ofertado;
 - 10.4.9.5 Avaliação da estabilidade e perfeito funcionamento da rede, aplicações e serviços da ANCINE antes, durante e após a implementação da solução;
- 10.4.10 Verificação do desempenho geral da rede, aplicações e serviços da ANCINE antes, durante e após a implementação da solução de acordo com o pré-estabelecido de forma a não gerar impactos no perfeito funcionamento das mesmas.

11. GARANTIA

- 11.1 A LICITANTE VENCEDORA deverá garantir às atualizações de versões de todos os softwares constantes deste Termo de Referência por um período mínimo de 12 (doze) meses a contar, OBRIGATORIAMENTE, da data de assinatura do contrato;
- 11.2 A garantia de assistência técnica dos softwares licenciados consiste na reparação de eventuais falhas de funcionamento, obrigando-se a empresa LICITANTE VENCEDORA a:
- 11.3 Efetuar, também sem ônus para a ANCINE, a entrega das mídias para substituição de versões dos softwares licenciados, se for o caso, com o objetivo de corrigir eventuais falhas e/ou incompatibilidade dos mesmos com o ambiente atualmente instalado, observadas as recomendações constantes dos manuais e das normas técnicas específicas para cada caso;
- 11.4 A LICITANTE VENCEDORA deverá fornecer suporte técnico através do fabricante durante a vigência contratual, por telefone, correio eletrônico ou internet, de modo a assegurar o perfeito funcionamento das licenças dos softwares.
- 11.5 O Suporte Técnico gratuito, através de correio eletrônico, deve ser mantido direto com a equipe de suporte da LICITANTE VENCEDORA, de segunda a sexta-feira das 09:00h às 18:00h, exceto feriados. As mensagens enviadas sábados, domingos e feriados serão analisadas no primeiro dia útil subsequente.
- 11.6 O tempo de resposta máximo deve ser de 48 (quarenta e oito) horas úteis após o recebimento da mensagem ou solicitação.
- 11.7 A LICITANTE VENCEDORA deverá disponibilizar endereço eletrônico, em site próprio ou do fabricante do software, para obtenção automática de novas releases e versões dos produtos licenciados, durante a vigência do contrato e/ou garantia;
- 11.8 A ANCINE poderá executar e transferir os produtos licenciados, sem custo adicional, para qualquer plataforma de hardware, sistema operacional ou banco de dados suportados pelo produto;
- 11.9 A ANCINE, nos casos de alterações na sua estrutura organizacional, poderá incorporar ou transferir os direitos de uso dos produtos licenciados, mediante comunicação à empresa LICITANTE VENCEDORA e providências para os ajustes contratuais necessários;
- 11.10 É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.
- 11.11 Caso o produto não corresponda ao exigido pela ANCINE, consoante às especificações constantes deste Edital, a empresa LICITANTE VENCEDORA deverá providenciar sua substituição no prazo máximo de 15 (quinze) dias, independentemente da aplicação das penalidades cabíveis.

12. DAS SANÇÕES ADMINISTRATIVAS:

- 12.1. Comete infração administrativa nos termos da Lei nº 8.666, de 1993 e da Lei nº 10.520, de 2002, a Contratada que:
- 12.1.1. inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

12.1.2. ensejar o retardamento da execução do objeto;

12.1.3. fraudar na execução do contrato;

12.1.4. comportar-se de modo inidôneo;

12.1.5. cometer fraude fiscal;

12.1.6. não manter a proposta.

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

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

12.2.2. multa moratória de 0,5% (meio por cento) por dia de atraso injustificado sobre o valor total do contrato, até o limite de 20 (vinte) dias, após o que ensejará a rescisão contratual, sem prejuízo da aplicação das correspondentes penalidades oriundas da rescisão;

12.2.3. multa de 10% (dez por cento) sobre o valor total do contrato, no caso de inexecução total do objeto;

10.2.3.1 em caso de inexecução parcial, a multa, no mesmo percentual do subitem acima, será aplicada de forma proporcional à obrigação inadimplida

12.2.4. suspensão de licitar e impedimento de contratar com o órgão ou entidade Contratante, pelo prazo de até dois anos;

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

12.2.6. declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados;

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

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

12.3.2. tenha praticado atos ilícitos visando a frustrar os objetivos da licitação;

12.3.3. demonstre não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

12.4. 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.

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

12.6. As penalidades serão obrigatoriamente registradas no SICAF.

13 CONDIÇÕES PARA ACEITE DO OBJETO

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

13.2 Fica estabelecido o prazo de cinco dias úteis, após recebimento e instalação do objeto, para se efetuar os testes e verificações mencionadas no item anterior;

13.3 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;

- 13.4 Somente será emitido o ACEITE DEFINITIVO DO OBJETO após a conclusão do TESTE do produto.
- 13.5 Os bens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de 5 dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

14 DA SUBCONTRATAÇÃO

- 14.1 Não será admitida a subcontratação do objeto licitatório.

15 DO FUNDAMENTO LEGAL E DO JULGAMENTO DAS PROPOSTAS:

- 15.1 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.
- 15.2 As propostas serão julgadas e adjudicadas pelo menor preço global.

16 DO PAGAMENTO

- 16.1 O pagamento será realizado no prazo máximo de até 5 (cinco) dias úteis, contados a partir da data de aceite DEFINITIVO do objeto, através de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.
- 16.2 O pagamento somente será autorizado depois de efetuado o “atesto” pelo servidor competente na nota fiscal apresentada.
- 16.3 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.
- 16.4 Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.
- 16.5 Antes do pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.
- 16.6 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.
- 16.7 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.
- 16.8 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.
- 16.9 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.
- 16.10 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.
- 16.11 Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.
- 16.12 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.
- 16.13 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:

- 16.14 $EM = I \times N \times VP$, sendo:
- 16.15 EM = Encargos moratórios;
- 16.16 N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
- 16.17 VP = Valor da parcela a ser paga.
- 16.18 I = Índice de compensação financeira = 0,00016438, assim apurado:

$$I = (TX)$$

$$I = (6/100)$$

$$I = 0,00016438$$

$$365$$

$$TX = \text{Percentual da taxa anual} = 6\%.$$

17 CLASSIFICAÇÃO DOS BENS COMUNS

- 17.1 Trata-se de objeto a ser contrato de natureza comum.

18 DOTAÇÃO ORÇAMENTÁRIA

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

19 DA ESTIMATIVA DE CUSTOS

As despesas com a execução desta contratação, no valor estimado de **R\$ 144.797,24** (cento e quarenta e quatro mil, setecentos e noventa e sete reais e vinte e quatro centavos), correrão à conta dos recursos consignados do Orçamento Geral da União para o exercício de 2016.

20 FISCALIZAÇÃO

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.

A fiscalização de que trata este item não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios, e, na ocorrência desta, não implica em corresponsabilidade da Administração ou de seus agentes e prepostos, de conformidade com o art. 70 da Lei nº 8.666, de 1993.



Documento assinado eletronicamente por **Leonardo De Oliveira Alves Sanches, Analista Administrativo**, em 27/10/2016, às 10:08, 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 Ritter Dos Santos, Gerente de Tecnologia da Informação**, em 27/10/2016, às 11:01, 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 **0219561** e o código CRC **AC9EE5E7**.