CONTRATO ADMINISTRATIVO N.º 015/2015
PROCESSO ADMINISTRATIVO N.º 01580.010013/2015-61

CONTRATO DE AQUISIÇÃO DE SOLUÇÃO CORPORATIVA DE ANTIVÍRUS E ATUALIZAÇÃO DE VERSÃO COM SERVIÇO DE SUPORTE TÉCNICO PELO PERÍODO DE 12 (DOZE) MESES QUE ENTRE SI CELEBRAM A AGÊNCIA NACIONAL DO CINEMA – ANCINE E A EMPRESA PCM SERV INFORMÁTICA LTDA - EPP.

A **AGÊNCIA NACIONAL DO CINEMA – ANCINE**, autarquia federal de natureza especial instituída pela Medida Provisória 2228-1, de 06 de setembro de 2001, inscrita no CNPJ sob o n.º 04.884.574/0001-20, com Escritório Central na Cidade do Rio de Janeiro/RJ, na Avenida Graça Aranha n.º 35, Centro, CEP 20030-002, neste ato representada por seu Secretário de Gestão Interna, **Sr. Glênio Cerqueira de França**, nomeado pela Portaria nº 66 de 17/04/2015, publicado no Diário Oficial da União de 20/04/2015, inscrito no CPF sob o n.º [redacted] portador da Cédula de Identidade n.º [redacted] expedida pela SSP/GO, residente e domiciliado nesta Cidade, doravante denominada **CONTRATANTE,** e a empresa **PCM SERV INFORMÁTICA LTDA - EPP**, inscrita no CNPJ sob o n.º 01.403.695/0001-15, estabelecida na Cidade de Santo André - SP, na Av. João XXIII, nº 20 – sala 61 – Vila Boa Vista, CEP 09190 - 500, neste ato representada por seus representantes legais, **Sr. Rodrigo Tadeu Cardoso, Sócio**, inscrito no CPF sob o n,º [redacted] portador da Cédula de Identidade n.º [redacted] expedida pela Secretaria da Segurança Pública do Estado de São Paulo – SSP-SP, e o **Sr. Sidinei Rondão, Sócio**, inscrito no CPF sob o nº [redacted] portador da Cédula de Identidade nº [redacted] expedida pela Secretaria de Segurança Pública do Estado de São Paulo – SSP- SP, doravante denominada **CONTRATADA,** em conformidade com o constante e fundamentado nos autos do Processo Administrativo nº 01580.010013/2015-61, e nas disposições da Lei n.º 8.666, de 1993, e alterações posteriores, da Lei n.º 10.520, de 2002, da Lei n.º 8.078, de 1990, da Instrução Normativa SLTI n.º 04, de 11 de setembro de 2014, e das demais normas que regem a matéria, resolvem celebrar o presente Contrato, decorrente do **Pregão Eletrônico n.º 010/2015,** mediante as cláusulas e condições a seguir enunciadas.

1 CLÁUSULA PRIMEIRA – DO OBJETO

1.1 O objeto do presente Contrato é a **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**, conforme especificações e quantitativos estabelecidos neste instrumento, no Termo de Referência, no Edital e seus anexos, e na Proposta vencedora, os quais integram este instrumento, independente de transcrição.

2 CLÁUSULA SEGUNDA – DA DISCRIMINAÇÃO DO OBJETO

2.1 Para fins de execução do contrato, a CONTRATADA deverá atender os requisitos técnicos e a outras previsões constantes neste Contrato. Todos os detalhes técnicos específicos de cada funcionalidade da solução estão descritos no item 1.3 e constituem o conjunto de funcionalidades obrigatórias da solução completa.

2.1.1 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;

2.1.2 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 dos seguintes fabricantes:

2.1.2.1 Trend Micro;

2.1.2.2 A opção de remoção das soluções acima deve ser feito junto ao processo de instalação do cliente, ou seja, sem a necessidade de se instalar/usar um módulo separado para esta ação;

2.1.2.3 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:

	Item	*Produtos*	*Composta de:*	*Qtde.*
GRUPO	1	Aquisição de Solução Corporativa de Antivírus.	Antivírus para estações de trabalho, servidores e dispositivos móveis.	1050
	2	Aquisição de Solução Corporativa de Antivírus para Servidor E-mail.	Antivírus para correio eletrônico	1200

2.2 LOCAL DA INSTALAÇÃO E ASSISTÊNCIA TÉCNICA:

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

2.3 DETALHAMENTO DAS ESPECIFICAÇÕES

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

2.3.2 Servidor de Administração e Console Administrativa

2.3.2.1 Compatibilidade:

2.3.2.1.1 Microsoft Windows Server 2003 ou superior

2.3.2.1.2 Microsoft Windows Server 2003 x64 ou superior

2.3.2.2 Características:

2.3.2.2.1 Deve permitir administração centralizada por console único de gerenciamento;

2.3.2.2.2 As configurações do Antivírus, AntiSpyware, Firewall, Proteção Contra Intrusos, controle de Dispositivos e Controle de Aplicações deverão ser realizadas através da mesma console;

2.3.2.2.3	A console deve ser acessada via WEB (HTTPS) ou MMC;
2.3.2.2.4	Fornecer atualizações do produto e das definições de vírus e proteção contra intrusos;
2.3.2.2.5	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;
2.3.2.2.6	A console de gerenciamento deve permitir ao administrador travar separadamente os itens e cada subitens de acesso as configurações do cliente;
2.3.2.2.7	Possuir processo de recuperação de senha através de e-mail pela console de gerenciamento.
2.3.2.2.8	Compatibilidade com solução de alta disponibilidade;
2.3.2.2.9	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;
2.3.2.2.10	Capacidade de instalar remotamente a solução de segurança em smartphones e tablets;
2.3.2.2.11	Capacidade de gerenciar estações de trabalho e servidores (tanto Windows como Linux e Mac) protegidos pela solução antivírus;
2.3.2.2.12	Capacidade de gerenciar smartphones e tablets protegidos pela solução antivírus;
2.3.2.2.13	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;
2.3.2.2.14	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 possuir, deve instalar o antivírus automaticamente;
2.3.2.2.15	Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias, etc;
2.3.2.2.16	Deve fornecer informações gerenciais dos computadores;
2.3.2.2.17	Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga altera-las;
2.3.2.2.18	Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão.
2.3.2.2.19	Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;

2.3.2.2.20	Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
2.3.2.2.21	Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
2.3.2.2.22	Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
2.3.2.2.23	Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;
2.3.2.2.24	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.
2.3.2.2.25	Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML.
2.3.2.2.26	Capacidade de gerar traps SNMP para monitoramento de eventos;
2.3.2.2.27	Capacidade de enviar e-mails para contas específicas em caso de algum evento;
2.3.2.2.28	Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;
2.3.2.2.29	Deve possuir compatibilidade com Cisco Network Admission Control (NAC);
2.3.2.2.30	Deve possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por exemplo).
2.3.2.2.31	Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc), inclusive de máquinas que estejam em subnets diferentes do servidor;
2.3.2.2.32	Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
2.3.2.2.33	Capacidade de realizar atualização incremental de vacinas nos computadores clientes;
2.3.2.2.34	Capacidade de reportar vulnerabilidades de softwares presentes nos computadores.
2.3.2.2.35	Capacidade de realizar levantamento instantâneo de hardware de todas as máquinas clientes;
2.3.2.2.36	Capacidade de realizar levantamento instantâneo de aplicativos de todas as máquinas clientes;
2.3.2.2.37	Capacidade de diferenciar máquinas virtuais de máquinas físicas;

2.3.3 Estações Windows

2.3.3.1 Compatibilidade:

2.3.3.1.1 Microsoft Windows XP Professional SP3 ou superior

2.3.3.2 Características:

2.3.3.2.1 Deve prover as seguintes proteções:

2.3.3.2.1.1 Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

2.3.3.2.1.2 Antivírus de Web (módulo para verificação de sites e downloads contra vírus)

2.3.3.2.1.3 Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos)

2.3.3.2.1.4 Antivírus de Mensagens Instantâneas (módulo para verificação de mensagens instantâneas, como ICQ, MSN, IRC, etc)

2.3.3.2.1.5 Firewall com IDS

2.3.3.2.1.6 Autoproteção (contra ataques aos serviços/processos do antivírus)

2.3.3.2.1.7 Controle de dispositivos externos

2.3.3.2.1.8 Controle de acesso a sites por categoria

2.3.3.2.1.9 Controle de execução de aplicativos

2.3.3.2.1.10 Controle de vulnerabilidades do Windows e dos aplicativos instalados

2.3.3.2.1.11 Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

2.3.3.2.2 As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa).

2.3.3.2.3 Capacidade de automaticamente desabilitar o Firewall do Windows (caso exista) durante a instalação, para evitar incompatibilidade com o Firewall da solução;

2.3.3.2.4 Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

2.3.3.2.5 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;

2.3.3.2.6 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;

2.3.3.2.7 Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);

VISTO

2.3.3.2.8	Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
2.3.3.2.9	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 tomá-la a partir da extensão do arquivo;
2.3.3.2.10	Capacidade de verificar somente arquivos novos e alterados;
2.3.3.2.11	Capacidade de verificar objetos usando heurística;
2.3.3.2.12	Capacidade de agendar uma pausa na verificação;
2.3.3.2.13	Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
2.3.3.2.14	O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
2.3.3.2.14.1	Perguntar o que fazer, ou;
2.3.3.2.14.2	Bloquear acesso ao objeto;
2.3.3.2.14.3	Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
2.3.3.2.15	Caso positivo de desinfecção:
2.3.3.2.15.1	Restaurar o objeto para uso;
2.3.3.2.16	Caso negativo de desinfecção:
2.3.3.2.16.1	Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
2.3.3.2.17	Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.
2.3.3.2.18	Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, IMAP, NNTP, SMTP e MAPI, assim como conexões criptografadas (SSL) para POP3 e IMAP (SSL);
2.3.3.2.19	Capacidade de verificar tráfego de ICQ, MSN, AIM e IRC contra vírus e links phishings;
2.3.3.2.20	Capacidade de verificar links inseridos em e-mails contra phishings;
2.3.3.2.21	Capacidade de verificar tráfego SSL nos browsers: Internet Explorer, Firefox e Opera;
2.3.3.2.22	Capacidade de verificação de corpo e anexos de e-mails usando heurística;
2.3.3.2.23	O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:
2.3.3.2.23.1	Perguntar o que fazer, ou;
2.3.3.2.23.2	Bloquear o e-mail;
2.3.3.2.24	Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

2.3.3.2.25	Caso positivo de desinfecção:
2.3.3.2.25.1	Restaurar o e-mail para o usuário;
2.3.3.2.26	Caso negativo de desinfecção:
2.3.3.2.26.1	Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);
2.3.3.2.27	Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena.
2.3.3.2.28	Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados.
2.3.3.2.29	Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador.
2.3.3.2.30	Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (Java Script, Visual Basic Script, etc), usando heurísticas;
2.3.3.2.31	Deve ter suporte total ao protocolo IPv6;
2.3.3.2.32	Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;
2.3.3.2.33	Na verificação de tráfego web, caso encontrado código malicioso o programa deve:
2.3.3.2.33.1	Perguntar o que fazer, ou;
2.3.3.2.33.2	Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;
2.3.3.2.34	Permitir acesso ao objeto;
2.3.3.2.35	O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:
2.3.3.2.35.1	Verificação *on-the-fly*, onde os dados são verificados enquanto são recebidos em tempo real, ou;
2.3.3.2.35.2	Verificação de *buffer*, onde os dados são recebidos e armazenados para posterior verificação.
2.3.3.2.36	Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web.
2.3.3.2.37	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.
2.3.3.2.38	Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa.
2.3.3.2.39	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.

2.3.3.2.40	Deve possuir módulo de bloqueio de *Phishing*, com atualizações incluídas nas vacinas, obtidas pelo *Anti-Phishing Working Group* (http://www.antiphishing.org).
2.3.3.2.41	Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;
2.3.3.2.42	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.
2.3.3.2.43	O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
2.3.3.2.43.1	Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
2.3.3.2.43.2	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.
2.3.3.2.44	Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:
2.3.3.2.44.1	Discos de armazenamento locais
2.3.3.2.44.2	Armazenamento removível
2.3.3.2.44.3	Impressoras
2.3.3.2.44.4	CD/DVD
2.3.3.2.44.5	Drives de disquete
2.3.3.2.44.6	Modems
2.3.3.2.44.7	Dispositivos de fita
2.3.3.2.44.8	Dispositivos multifuncionais
2.3.3.2.44.9	Leitores de smart card
2.3.3.2.44.10	Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc)
2.3.3.2.44.11	Wi-Fi
2.3.3.2.44.12	Adaptadores de rede externos
2.3.3.2.44.13	Dispositivos MP3 ou smartphones
2.3.3.2.44.14	Dispositivos Bluetooth
2.3.3.2.45	Capacidade de liberar acesso a um dispositivo específico e usuários específico por um período de tempo específico, sem a necessidade de desabilitar a proteção, sem desabilitar o gerenciamento central ou de intervenção local do administrador na máquina do usuário.
2.3.3.2.46	Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário.

2.3.3.2.47 Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento.

2.3.3.2.48 Capacidade de configurar novos dispositivos por Class ID/Hardware ID

2.3.3.2.49 Capacidade de limitar o acesso a sites da internet por categoria, por conteúdo (vídeo, áudio, etc), com possibilidade de configuração por usuário ou grupos de usuários e agendamento.

2.3.3.2.50 Capacidade de limitar a execução de aplicativos por hash MD5, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc).

2.3.3.2.51 Capacidade de bloquear execução de aplicativo que está em armazenamento externo.

2.3.3.2.52 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.

2.3.3.2.53 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.

2.3.3.2.54 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.

2.3.4 Estações e Servidores Mac OS X

2.3.4.1 Compatibilidade:

2.3.4.1.1 Mac OS X 10.4.11 ou superior

2.3.5 Características:

2.3.5.1 Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

2.3.5.2 Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

2.3.5.3 A instalação e primeira execução do produto deve ser feita sem necessidade de reinicialização do computador, de modo que o produto funcione com toda sua capacidade;

2.3.5.4 Deve possuir suportes a notificações utilizando o Growl;

2.3.5.5 As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa).

2.3.5.6 Capacidade de voltar para a base de dados de vacina anterior;

2.3.5.7 Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;

2.3.5.8 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;

2.3.5.9 Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);

2.3.5.10 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;

2.3.5.11 Capacidade de verificar somente arquivos novos e alterados;

2.3.5.12 Capacidade de verificar objetos usando heurística;

2.3.5.13 Capacidade de agendar uma pausa na verificação;

2.3.5.14 O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

2.3.5.14.1 Perguntar o que fazer, ou;

2.3.5.14.2 Bloquear acesso ao objeto;

2.3.5.15 Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

2.3.5.16 Caso positivo de desinfecção:

2.3.5.16.1 Restaurar o objeto para uso;

2.3.5.17 Caso negativo de desinfecção:

2.3.5.17.1 Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

2.3.5.18 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

2.3.5.19 Capacidade de verificar arquivos de formato de e-mail;

2.3.5.20 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;

2.3.5.21 Capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento;

2.3.6 Estações de trabalho Linux

2.3.6.1 Compatibilidade:

2.3.6.1.1 Plataforma 32 ou 64 bits:

2.3.6.1.1.1 Red Hat 4 ou superior;

2.3.6.1.1.2 Fedora 3 ou superior;

2.3.6.1.1.3 CentOS 5.2 ou superior;

2.3.6.1.1.4 Ubuntu Server 10.04.2 LTS ou superior;

2.3.6.1.1.5 Debian 4 ou superior;

2.3.6.2 Características:

2.3.6.2.1 Deve prover as seguintes proteções:

2.3.6.2.1.1 Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

2.3.6.2.1.2 As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

2.3.6.2.2 Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

2.3.6.2.2.1 Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

2.3.6.2.2.2 Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

2.3.6.2.2.3 Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;

2.3.6.2.2.4 Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

2.3.6.2.3 Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem necessidade de outros softwares;

2.3.6.2.4 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

2.3.6.2.5 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;

2.3.6.2.6 Capacidade de verificar objetos usando heurística;

2.3.6.2.7 Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena

2.3.6.2.8 Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados

2.3.6.2.9 Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

2.3.7 Servidores Windows

2.3.7.1 Compatibilidade:

2.3.7.1.1 Microsoft Windows Small Business Server 2011 ou superior

2.3.7.1.2 Microsoft Windows Server 2003 ou superior;

2.3.7.1.3 Microsoft Windows Hyper-V Server 2008 ou superior;

2.3.7.2 Características:

2.3.7.2.1 Deve prover as seguintes proteções:

2.3.7.2.2 Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

2.3.7.2.3 Autoproteção contra ataques aos serviços/processos do antivírus

2.3.7.2.4 Firewall com IDS

2.3.7.2.5 Controle de vulnerabilidades do Windows e dos aplicativos instalados

2.3.7.3 Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

2.3.7.4 As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

2.3.7.5 Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

2.3.7.5.1 Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

2.3.7.5.2 Gerenciamento de tarefa (criar ou excluir tarefas de verificação)

2.3.7.5.3 Leitura de configurações

2.3.7.5.4 Modificação de configurações

2.3.7.5.5 Gerenciamento de Backup e Quarentena

2.3.7.5.6 Visualização de relatórios

2.3.7.5.7 Gerenciamento de relatórios

2.3.7.5.8 Gerenciamento de chaves de licença

2.3.7.5.9 Gerenciamento de permissões (adicionar/excluir permissões acima)

2.3.7.6 O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

2.3.7.6.1 Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

2.3.7.6.2 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.

2.3.7.7 Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total.

2.3.7.8 Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc)

2.3.7.9 Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (*uninterruptible Power supply – UPS*)

2.3.7.10 Em caso erros, deve ter capacidade de criar *logs* e *traces* automaticamente, sem necessidade de outros softwares;

2.3.7.11 Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor.

2.3.7.12 Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado nos servidor.

2.3.7.13 Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas.

2.3.7.14 Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

2.3.7.15 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;

2.3.7.16 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

2.3.7.17 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;

2.3.7.18 Capacidade de verificar somente arquivos novos e alterados;

2.3.7.19 Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto-descompressores, .PST, arquivos compactados por compactadores binários, etc)

2.3.7.20 Capacidade de verificar objetos usando heurística;

2.3.7.21 Capacidade de configurar diferentes ações para diferentes tipos de ameaças;

2.3.7.22 Capacidade de agendar uma pausa na verificação;

2.3.7.23 Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;

2.3.7.24 O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

2.3.7.24.1 Perguntar o que fazer, ou;

2.3.7.24.2 Bloquear acesso ao objeto;

2.3.7.24.3 Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

2.3.7.24.4 Caso positivo de desinfecção:

2.3.7.24.5 Restaurar o objeto para uso;

2.3.7.24.6 Caso negativo de desinfecção:

2.3.7.24.7 Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

VISTO

2.3.7.25 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

2.3.7.26 Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena

2.3.7.27 Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados

2.3.7.28 Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

2.3.8 Servidores Linux

2.3.8.1 Compatibilidade:

2.3.8.1.1 Plataforma 32 ou 64 bits:

2.3.8.1.1.1 Red Hat 4 ou superior;

2.3.8.1.1.2 Fedora 3 ou superior;

2.3.8.1.1.3 CentOS 5.2 ou superior;

2.3.8.1.1.4 Ubuntu Server 10.04.2 LTS ou superior;

2.3.8.1.1.5 Debian 4 ou superior;

2.3.8.2 Características:

2.3.8.2.1 Deve prover as seguintes proteções:

2.3.8.2.1.1 Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

2.3.8.2.1.2 As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

2.3.8.2.2 Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

2.3.8.2.2.1 Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

2.3.8.2.2.2 Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

2.3.8.2.2.3 Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;

2.3.8.2.2.4 Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

2.3.8.2.3 Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem necessidade de outros softwares;

2.3.8.2.4 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

2.3.8.2.5 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;

2.3.8.2.6 Capacidade de verificar objetos usando heurística;

2.3.8.2.7 Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena

2.3.8.2.8 Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados

2.3.8.2.9 Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux)

2.3.9 Smartphones e tablets

2.3.9.1 Compatibilidade:

2.3.9.1.1 Apple iOS 4.0 ou superior;

2.3.9.1.2 Symbian OS 9.1 ou superior e Symbian^3, Symbian Anna, Symbian Belle ou superior;

2.3.9.1.3 Windows PHONE;

2.3.9.1.4 Android OS 1.5 ou superior;

2.3.9.2 Características:

2.3.9.2.1 Deve prover as seguintes proteções:

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

2.3.9.2.1.1.1 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.

2.3.9.2.1.1.2 Arquivos abertos no smartphone

2.3.9.2.1.1.3 Programas instalados usando a interface do smartphone

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

2.3.9.2.2 Deverá isolar em área de quarentena os arquivos infectados;

2.3.9.2.3 Deverá atualizar as bases de vacinas de modo agendado;

2.3.9.2.4 Deverá bloquear spams de SMS através de Black lists;

2.3.9.2.5 Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado;

2.3.9.2.6 Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo.

VISTO

2.3.9.2.7 Deverá ter firewall pessoal;

2.3.9.2.8 Possibilidade de instalação remota utilizando o Microsoft System Center Mobile Devive Manager 2008 SP1

2.3.9.2.9 Possibilidade de instalação remota utilizando o Sybase Afaria 6.5

2.3.9.2.10 Capacidade de detectar Jailbreak em dispositivos iOS

2.3.9.2.11 Capacidade de bloquear o acesso a site por categoria em dispositivos

2.3.9.2.12 Capacidade de bloquear o acesso a sites phishing ou malicioso

2.3.9.2.13 Capacidade de criar conteiners de aplicativos, separando dados corporativos de dados pessoais

2.3.9.2.14 Capacidade de configurar White e black list de aplicativos

2.3.10 Gerenciamento de dispositivos móveis (MDM):

2.3.10.1 Compatibilidade:

2.3.10.1.1 Dispositivos conectados através do Microsoft Exchange ActiveSync

2.3.10.1.1.1 Apple iOS

2.3.10.1.1.2 Symbian OS

2.3.10.1.1.3 Windows Mobile e Windows Phone

2.3.10.1.1.4 Android

2.3.10.1.1.5 Palm WebOS.

2.3.10.1.2 Dispositivos com suporte ao Apple Push Notification (APNs) servisse

2.3.10.1.2.1 Apple iOS 3.0 ou superior

2.3.10.2 Caracteristicas:

2.3.10.2.1 Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange

2.3.10.2.2 Capacidade de ajustar as configurações de:

2.3.10.2.2.1 Sincronização de e-mail

2.3.10.2.2.2 Uso de aplicativos

2.3.10.2.2.3 Senha do usuário

2.3.10.2.2.4 Criptografia de dados

2.3.10.2.2.5 Conexão de mídia removível

2.3.10.2.3 Capacidade de instalar certificados digitais em dispositivos móveis

2.3.10.2.4 Capacidade de, remotamente, resetar a senha de dispositivos iOS

2.3.10.2.5 Capacidade de, remotamente, apagar todos os dados de dispositivos iOS

2.3.10.2.6 Capacidade de, remotamente, bloquear um dispositivo iOS

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

2.4.1 Servidores de e-mail Windows

2.4.1.1 Compatibilidade:

2.4.1.1.1 Microsoft Small Business Server 2008 Standard

2.4.1.1.2 Microsoft Small Business Server 2008 Premium

2.4.1.1.3 Microsoft Essential Business Server 2008 Standard

2.4.1.1.4 Microsoft Essential Business Server 2008 Premium

2.4.1.1.5 Microsoft Windows Server 2003 x32 ou superior

2.4.1.1.6 Microsoft Windows Server 2003 x64 ou superior

2.4.1.1.7 Microsoft Exchange Server 2003 ou superior.

2.4.1.2 Características:

2.4.1.2.1 Deve utilizar as tecnologias VSAPI 2.0, 2.5 e 2.6;

2.4.1.2.2 Capacidade de iniciar várias cópias do processo de antivírus;

2.4.1.2.3 As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

2.4.1.2.4 Capacidade de verificar pastas públicas, e-mails enviados, recebidos e armazenados contra vírus, spywares, adwares, worms, trojans e riskwares;

2.4.1.2.5 Capacidade de verificar pastas públicas e e-mails armazenados de forma agendada, utilizando as últimas vacinas e heurística;

2.4.1.2.6 O antivírus, ao encontrar um objeto infectado, deve:

2.4.1.2.6.1 Desinfetar o objeto, notificando o recipiente, destinatário e administradores, ou

2.4.1.2.6.2 Excluir o objeto, substituindo-o por uma notificação;

2.4.1.2.6.3 Bloquear acesso ao objeto;

2.4.1.2.6.4 Apagar o objeto ou tentar desinfetá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

2.4.1.2.6.5 Caso positivo de desinfecção:

2.4.1.2.6.6 Restaurar o objeto para uso;

2.4.1.2.7 Caso negativo de desinfecção:

2.4.1.2.7.1 Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

2.4.1.2.7.2 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

2.4.1.2.8 Capacidade de enviar notificações sobre vírus detectados para o administrador, para o recipiente e remetente da mensagem infectada.

2.4.1.2.9 Capacidade de gravar logs de atividade de vírus nos eventos do sistema e nos logs internos da aplicação;

2.4.1.2.10 Capacidade de detectar disseminação em massa de e-mails infectados, informando o administrador e registrando tais eventos nos logs do sistema e da aplicação.

2.4.2 Servidores de e-mail Linux:

2.4.2.1 Compatibilidade:

2.4.2.1.1 Plataforma 32 ou 64 bits:

2.4.2.1.1.1 Red Hat 4 ou superior;

2.4.2.1.1.2 Fedora 3 ou superior;

2.4.2.1.1.3 CentOS 5.2 ou superior;

2.4.2.1.1.4 Ubuntu Server 10.04.2 LTS ou superior;

2.4.2.1.1.5 Debian 4 ou superior;

2.4.2.1.2 MTA:

2.4.2.1.2.1 Sendmail 8.12.x ou superior;

2.4.2.1.2.2 Qmail 1.03;

2.4.2.1.2.3 Postfix 2.x;

2.4.2.1.2.4 Exim 4.x;

2.4.2.2 Características:

2.4.2.2.1 Capacidade de verificar o tráfego SMTP do servidor contra malware em todos os elementos do e-mail: cabeçalho, corpo e anexo;

2.4.2.2.2 Capacidade de notificar o administrador, o remetente e o destinatário caso um arquivo malicioso seja encontrado no e-mail;

2.4.2.2.3 Capacidade de quarentenar objetos maliciosos;

2.4.2.2.4 Capacidade de salvar backup dos objetos antes de tentativa de desinfecção;

2.4.2.2.5 Capacidade de fazer varredura no sistema de arquivos do servidor;

2.4.2.2.6 Capacidade de filtrar anexos por nome ou tipo de arquivo;

2.4.2.2.7 Capacidade de criar grupos de usuários para aplicar regras de verificação de e-mails;

2.4.2.2.8 Deve permitir gerenciamento via console WEB;

2.4.2.2.9 Deve ser atualizado de maneira automática via internet ou por servidores locais, com frequência horária.

3 CLÁUSULA TERCEIRA – DA GARANTIA

3.1 A CONTRATADA deverá garantir às atualizações de versões de todos os softwares constantes deste Contrato por um período mínimo de 12 (doze) meses a contar, OBRIGATORIAMENTE, da data de assinatura do contrato;

3.1 A garantia de assistência técnica dos softwares licenciados consiste na reparação de eventuais falhas de funcionamento, obrigando-se a empresa CONTRATADA a:

3.2 Efetuar, também sem ônus para a CONTRATANTE, 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;

3.3 A CONTRATADA 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.

3.4 O Suporte Técnico gratuito, através de correio eletrônico, deve ser mantido direto com a equipe de suporte da CONTRATADA, de segunda a sexta-feira das 09:00h às 18:00h, exceto feriados. As mensagens enviadas sábados, domingos e feriados serão analisados no primeiro dia útil subseqüente.

3.5 O tempo de resposta máximo deve ser de 48 (quarenta e oito) horas após o recebimento da mensagem ou solicitação.

3.6 A CONTRATADA 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;

3.7 A CONTRATANTE poderá executar e transferir os produtos licenciados, sem custo adicional, para qualquer plataforma de hardware, sistema operacional ou banco de dados suportados pelo produto;

3.8 A CONTRATANTE, nos casos de alterações na sua estrutura organizacional, poderá incorporar ou transferir os direitos de uso dos produtos licenciados, mediante comunicação à empresa CONTRATADA e providencias para os ajustes contratuais necessários;

3.9 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 mantidos as demais cláusulas e condições do contrato, não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da CONTRATANTE;

3.10 Caso o produto não corresponda ao exigido pela CONTRATANTE, consoante às especificações constantes deste Contrato, a empresa CONTRATADA deverá providenciar sua substituição no prazo máximo de 15 (quinze) dias, independentemente da aplicação das penalidades cabíveis.

4 CLÁUSULA QUARTA – DA INSTALAÇÃO E CONFIGURAÇÃO

4.1 Serão de responsabilidade da CONTRATADA a instalação e a configuração da solução, bem como a desinstalação da solução existente;

4.2 A instalação deverá ser realizada em horário comercial e previamente marcada com a CONTRATANTE;

4.3 A solução deverá ser instalada no servidor indicado pela CONTRATANTE e nas estações de trabalhos, servidores e dispositivos móveis;

4.4 Deverão ser feitas todas as configurações necessárias para o perfeito funcionamento da solução conforme especificação técnica;

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 20 (vinte) dias após o início da instalação, não sendo contabilizados o tempo das janelas de mudança

adequadas para servidores e/ou equipamentos em transito, observadas junto com o setor responsável.

4.6 Deverá ser realizada, pela CONTRATADA, a configuração e a interconexão da maquina servidora com as clientes da solução;

4.7 Deverá ser realizada, pela CONTRATADA, a instalação, customização e operacionalização dos equipamentos envolvidos, atualizações de software, patches, clientes, firmwares e etc. para suas mais recentes versões;

4.8 Deverá ser apresentado, pela CONTRATADA, resultados de testes de funcionamento da solução e de redundância, quando se aplicar;

4.9 Deverão ser realizados, pela CONTRATADA, os seguintes serviços de implementação:

4.9.1 Avaliação do ambiente proposto, pré-requisitos, compatibilidade e interoperabilidade;

4.9.2 Análise de aplicação de patchs, compatibilidade com os sistemas e aplicações da CONTRATANTE;

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;

4.9.4 Implementação dos mecanismos de proteção;

4.9.5 Avaliação da estabilidade e perfeito funcionamento da rede e aplicações da CONTRATANTE sob ponto de vista de interconexão e compatibilidade dos componentes;

4.10 Verificação do desempenho geral da rede e aplicações da CONTRATANTE de acordo com o pré-estabelecido.

5 CLÁUSULA QUINTA – DA VIGÊNCIA

5.1 O prazo de vigência deste Contrato é de 12 (doze) meses, contados a partir da data de sua assinatura; prorrogável na forma do art. 57, §1º, da Lei nº 8.666, de 1993.

6 CLÁUSULA SEXTA – DO PREÇO

6.1 O valor total do presente Contrato é de R$ 60.988,50 (sessenta mil, novecentos e oitenta e oito reais e cinquenta centavos), conforme discriminado no quadro a seguir:

	Item	*Produtos*	*Composta de:*	*Qtde.*	*Preço Unitário*	*Total (R$)*
G1	1	Aquisição de Solução Corporativa de Antivírus.	Antivírus para estações de trabalho, servidores e dispositivos moveis.	1050	R$ 33,33	R$ 34.996,50
	2	Aquisição de Solução Corporativa de Antivírus	Antivírus para correio	1200	R$ 21,66	R$ 25.992,00

		para Servidor E-mail.	eletrônico			
VALOR GLOBAL DO GRUPO						R$ 60.988,50

6.2. Nos valores acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução contratual, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

7 CLÁUSULA SÉTIMA – DA DOTAÇÃO ORÇAMENTÁRIA

7.1 As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria, prevista no orçamento da CONTRATANTE, para o exercício de 2015, na classificação abaixo:

Gestão/Unidade: 20203/203003
Fonte: 0100
Programa de Trabalho: 13.122.2107.2000.0001
Elemento de Despesa: 3.3.90.39.56
PI: 5CNM0170001

Nota de Empenho: 2015NE800602, de 17/06/2015, no valor de R$ 60.988,50 (sessenta mil novecentos e oitenta e oito reais e cinquenta centavos).

8 CLÁUSULA OITAVA – DO PAGAMENTO

8.1 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.

8.2 O pagamento somente será autorizado depois de efetuado o "atesto" pelo servidor competente na nota fiscal apresentada.

8.3 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 CONTRATANTE.

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

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

8.6 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 CONTRATANTE.

8.7 Não havendo regularização ou sendo a defesa considerada improcedente, a CONTRATANTE deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade

fiscal quanto à inadimplência da contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

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

8.9 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.

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

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

8.11.1 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.

8.12 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 CONTRATANTE, 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:

$$I = (TX) \qquad I = \frac{(6/100)}{365} \qquad I = 0,00016438$$

TX = Percentual da taxa anual = 6%.

9 CLÁUSULA NONA – DO REAJUSTE

9.1 O preço contratado é fixo e irreajustável.

10 CLÁUSULA DÉCIMA – DA GARANTIA CONTRATUAL

10.1 A CONTRATADA, no prazo de 10 (dez dias) após a assinatura do Contrato, prestará garantia no valor correspondente a **5% (cinco por cento)** do valor do Contrato, que corresponde a **R$ 3.049,42 (três mil e quarenta e nove reais e quarenta e dois centavos)** e será liberada de acordo com as condições previstas neste Contrato, conforme disposto no art. 56 da Lei nº 8.666, de 1993, desde que cumpridas as obrigações contratuais.A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete

centésimos por cento) do valor do contrato por dia de atraso, até o máximo de 1% (um por cento).

10.1.2 O atraso superior a 30 (trinta) dias autoriza a CONTRATANTE a promover a retenção dos pagamentos devidos à CONTRATADA, até o limite de 1% (um por cento) do valor do contrato a título de garantia, a serem depositados junto à Caixa Econômica Federal, com correção monetária, em favor da CONTRATANTE.

10.2 A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

10.2.1 prejuízo advindo do não cumprimento do objeto do contrato;

10.2.2 prejuízos diretos causados à CONTRATANTE, decorrentes de culpa ou dolo durante a execução do contrato;

10.2.3 multas moratórias e punitivas aplicadas pela CONTRATANTE à CONTRATADA.

10.2.4 obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela CONTRATADA, quando couber.

10.3 A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item 10.2, observada a legislação que rege a matéria.

10.4 A garantia em dinheiro deverá ser efetuada em favor da CONTRATANTE, na Caixa Econômica Federal, com correção monetária.

10.5 No caso de prorrogação do contrato na forma do item 5.1 deste contrato, a garantia deverá ser renovada nas mesmas condições.

10.6 Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a CONTRATADA obriga-se a fazer a respectiva reposição no prazo máximo de 10 (dez) dias úteis, contados da data em que for notificada.

10.7 O garantidor não é parte para figurar em processo administrativo instaurado pela CONTRATANTE com o objetivo de apurar prejuízos e/ou aplicar sanções à CONTRATADA.

10.8 A CONTRATANTE executará a garantia na forma prevista na legislação que rege a matéria.

10.9 Será considerada extinta a garantia:

10.9.1 com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da CONTRATANTE, mediante termo circunstanciado, de que a CONTRATADA cumpriu todas as cláusulas do contrato;

10.9.2 no prazo de três meses após o término da vigência, caso a CONTRATANTE não comunique a ocorrência de sinistros.

11 CLÁUSULA DÉCIMA PRIMEIRA – DA ENTREGA E DO RECEBIMENTO DO OBJETO

11.1 A CONTRATADA deverá disponibilizar a solução, com todos os componentes especificados neste Contrato, em até 30 (trinta) dias corridos após assinatura do Contrato;

11.2 Caso se veja impossibilitada de cumprir o prazo estipulado para a entrega da solução e componentes, a CONTRATADA 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.

12 CLAÚSULA DÉCIMA SEGUNDA – DA FISCALIZAÇÃO

12.1 Nos termos do art. 67 Lei nº 8.666, de 1993, será designado representante para acompanhar e fiscalizar a entrega dos bens, anotando em registro próprio todas as ocorrências relacionadas com a execução e determinando o que for necessário à regularização de falhas ou defeitos observados.

12.2 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 CONTRATANTE ou de seus agentes e prepostos, de conformidade com o art. 70 da Lei nº 8.666, de 1993.

12.3 O representante da CONTRATANTE anotará em registro próprio todas as ocorrências relacionadas com a execução do contrato, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das falhas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

13 CLÁUSULA DÉCIMA TERCEIRA – DAS OBRIGAÇÕES DA CONTRATADA

13.1 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:

13.1.1 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;

13.1.2 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);

13.1.3 Substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste Contrato, o objeto com avarias ou defeitos;

13.1.4 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 11.2 deste Contrato;

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

13.1.6 Indicar preposto para representá-la durante a execução do contrato;

13.1.7 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.

14 CLÁUSULA DÉCIMA QUARTA – DAS OBRIGAÇÕES DA CONTRATANTE

14.1 Receber o objeto no prazo e condições estabelecidas no Edital e seus anexos;

14.2 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;

14.3 Comunicar à Contratada, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;

14.4 Acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através de comissão/servidor especialmente designado;

14.5 Efetuar o pagamento à Contratada no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no Edital e seus anexos;

14.6 A CONTRATANTE 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.

14.7 Disponibilizar acesso administrativo, e janela de mudança adequada para desinstalação do software antivírus anterior.

14.8 Disponibilizar acesso administrativo, e janela de mudança adequada para instalação do software antivírus novo, objeto deste termo/licitação.

14.9 O tempo adequado de janela de mudança para servidores e/ou equipamentos em transito, pode exceder o prazo máximo estabelecido para a maioria dos equipamentos.

14.10 Um plano de mudança deve ser fornecido pela CONTRATANTE, identificando caso a caso, com suas respectivas janelas de mudança.

15 CLÁUSULA DÉCIMA QUINTA – DAS CONDIÇÕES PARA ACEITE DO OBJETO

15.1 O produto objeto deste Contrato 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 neste Contrato e na proposta da CONTRATADA;

15.2 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;

15.3 O recebimento do objeto não exclui a responsabilidade pela qualidade, ficando a CONTRATADA 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 CONTRATANTE;

15.4 Somente será emitido o ACEITE DEFINITIVO DO OBJETO após a conclusão do TESTE do produto.

16 CLÁUSULA DÉCIMA SEXTA – DOS REQUISITOS DE SEGURANÇA

16.1 Pela natureza da atividade da CONTRATANTE, os serviços deverão propiciar a segurança dos dados. As soluções contratadas não deverão fornecer acesso externo não autorizado aos dados da CONTRATANTE.

16.2 A CONTRATADA deverá assinar Termo de Compromisso de Manutenção de Sigilo.

17 CLÁUSULA DÉCIMA SÉTIMA – DAS ALTERAÇÕES

17.1 Eventuais alterações contratuais reger-se-ão pela disciplina do art. 65 da Lei nº 8.666, de 1993.

17.2 A CONTRATADA é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

17.3 As supressões resultantes de acordo celebrado entre as contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

18 CLÁUSULA DÉCIMA OITAVA – 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 10% (dez por cento), ou seja, por 20 (vinte) dias;
18.2.2.1 Em se tratando de inobservância do prazo fixado para apresentação da garantia, ainda que seja para reforço, aplicar-se-á multa de 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso, observado o máximo de 2% (dois por cento), de modo que o atraso superior a 25 (vinte e cinco) dias autorizará a CONTRATANTE a promover a rescisão do contrato;
18.2.2.2 As penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si.
18.2.3 Multa compensatória de 10% (dez por cento) sobre o valor total do contrato, no caso de inexecução total do objeto;
18.2.3.1 Em caso de inexecução parcial, a multa compensatória, no mesmo percentual do subitem acima, será aplicada de forma proporcional à obrigação inadimplida;
18.2.4 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;
18.2.5 Impedimento de licitar e contratar com a União com o consequente descredenciamento no SICAF pelo prazo de até cinco anos;
18.2.6 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;

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

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

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

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

18.4 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.

18.5 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 Contratante, observado o princípio da proporcionalidade.

18.6 As penalidades serão obrigatoriamente registradas no SICAF.

19 CLÁUSULA DÉCIMA NONA – DA RESCISÃO

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

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

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

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

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

19.5.1 Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos.

19.5.2 Relação dos pagamentos já efetuados e ainda devidos.

19.5.3 Indenizações e multas.

20 CLÁUSULA VIGÉSIMA – DOS CRITÉRIOS DE SUSTENTABILIDADE AMBIENTAL

20.1 O FABRICANTE do produto ofertado deverá:

20.1.1 Adotar boas práticas de otimização de recursos/redução de desperdícios/menor poluição, tais como:

20.1.2 Racionalização do uso de substâncias potencialmente tóxicas/poluentes;

20.1.3 Substituição de substâncias tóxicas por outras atóxicas ou de menor toxicidade;

20.1.4 Racionalização/economia no consumo de energia (especialmente elétrica) e água;

20.1.5 Treinamento/capacitação periódicos dos empregados sobre boas práticas de redução de desperdícios/poluição.

21 CLÁUSULA VIGÉSIMA PRIMEIRA – DOS CASOS OMISSOS

21.1 Os casos omissos serão decididos pela CONTRATANTE, segundo as disposições contidas na Lei nº 8.666, de 1993, na Lei nº 10.520, de 2002 e demais normas federais de licitações e contratos administrativos e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

22 CLÁUSULA VIGÉSIMA SEGUNDA – DA PUBLICAÇÃO

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

23 CLÁUSULA VIGÉSIMA TERCEIRA – DO FORO

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

Para firmeza e validade do pactuado, o presente Contrato foi lavrado em 02 (duas) vias de igual teor e forma, que, depois de lidas e achadas em ordem, vão assinadas pelos contraentes e pelas testemunhas abaixo identificadas.

Rio de Janeiro, 06 de Agosto de 2015.

CONTRATANTE: AGÊNCIA NACIONAL DO CINEMA

Glênio Cerqueira de França
Secretário de Gestão Interna

CONTRATADA: PCM SERV INFORMÁTICA LTDA - EPP

Rodrigo Tadeu Cardoso
Sócio

Sidinei Rondão
Sócio

TESTEMUNHAS:

CPF: [redacted]

CPF: [redacted]

Maior Antonio P. da Silva

Mariana P. Cardoso

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

A AGÊNCIA NACIONAL DO CINEMA – ANCINE, autarquia federal de natureza especial instituída pela Medida Provisória 2228-1, de 06 de setembro de 2001, inscrita no CNPJ sob o n.º 04.884.574/0001-20, com Escritório Central na Cidade do Rio de Janeiro/RJ, na Avenida Graça Aranha n.º 35, Centro, CEP 20030-002, doravante denominada **CONTRATANTE**, neste ato representada por seu Secretário de Gestão Interna, **Glênio Cerqueira de França**, nomeado pela Portaria nº 66 de 17/04/2015, publicado no Diário Oficial da União de 20/04/2015, inscrito no CPF sob o n.º [redacted], portador da Cédula de Identidade n.º [redacted], expedida pela SSP/GO, residente e domiciliado nesta Cidade, e, de outro lado, a empresa **PCM SERV INFORMÁTICA LTDA - EPP**, sediada na Cidade de Santo André - SP, na Av. João XXIII, nº 20 – sala 61 – Vila Boa Vista; CEP 09190 - 500, CNPJ n.º 01.403.695/0001-15, doravante denominada **CONTRATADA**, neste ato representada por seus representantes legais, Srs. **Rodrigo Tadeu Cardoso, Sócio**, inscrito no CPF sob o n.º [redacted], portador da Cédula de Identidade n.º [redacted], expedida pela Secretaria da Segurança Pública do Estado de São Paulo – SSP-SP, e **Sr. Sidinei Rondão, Sócio**, inscrito no CPF sob o nº [redacted], portador da Cédula de Identidade nº [redacted], expedida pela Secretaria de Segurança Pública do Estado de São Paulo – SSP- SP; CONSIDERANDO que, em razão do **CONTRATO ADMINISTRATIVO N.º 015/2015**, doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação da CONTRATANTE;

Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante denominado TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sensíveis e sigilosas, disponibilizadas pela CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõe o Decreto 4.553 de 27/12/2002 - Salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

Informação: é o conjunto de dados organizados de acordo com procedimentos executados por meios eletrônicos ou não, que possibilitam a realização de atividades específicas e/ou tomada de decisão.

Informação Pública ou Ostensiva: são aquelas cujo acesso é irrestrito, obtida por divulgação

pública ou por meio de canais autorizados pela CONTRATANTE.

Informações Sensíveis: são todos os conhecimentos estratégicos que, em função de seu potencial no aproveitamento de oportunidades ou desenvolvimento nos ramos econômico, político, científico, tecnológico, militar e social, possam beneficiar a Sociedade e o Estado brasileiros.

Informações Sigilosas: são aquelas cujo conhecimento irrestrito ou divulgação possam acarretar qualquer risco à segurança da sociedade e do Estado, bem como aquelas necessárias ao resguardo da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.

Contrato Principal: contrato celebrado entre as partes, ao qual este TERMO se vincula.

Cláusula Terceira – DAS INFORMAÇÕES SIGILOSAS

Serão consideradas como informação sigilosa, toda e qualquer informação escrita ou oral, revelada a outra parte, contendo ou não a expressão confidencial e/ou reservada. O TERMO informação abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas,

especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de idéias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

Parágrafo Primeiro – Comprometem-se, as partes, a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas informações, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Segundo – As partes deverão cuidar para que as informações sigilosas fiquem restritas ao conhecimento das pessoas que estejam diretamente envolvidas nas atividades relacionadas à execução do objeto do CONTRATO PRINCIPAL.

Parágrafo Terceiro – As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I – Sejam comprovadamente de domínio público no momento da revelação;

II – Tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III – Sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quarta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem e se obrigam a utilizar a informação sigilosa revelada pela outra parte exclusivamente para os propósitos da execução do CONTRATO PRINCIPAL, em conformidade com o disposto neste TERMO.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as informações deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas,

coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto - A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das informações, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das Informações Proprietárias por seus agentes, representantes ou por terceiros;

III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das informações, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

Cláusula Quinta – DA VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

Cláusula Sexta – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das informações, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 87 da Lei nº. 8.666/93.

Cláusula Sétima – DAS DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela

CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, TERMOS e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo a CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar Informações Sigilosas para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Oitava – DO FORO

A CONTRATANTE elege o foro da Seção Judiciária do Rio de Janeiro – Justiça Federal, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

Rio de Janeiro, 06 de Agosto de 2015.

DE ACORDO:

CONTRATANTE: AGÊNCIA NACIONAL DO CINEMA

Glênio Cerqueira de França
Secretário de Gestão Interna

CONTRATADA: PCM SERV INFORMÁTICA LTDA - EPP

Rodrigo Tadeu Cardoso
Sócio

Sidinei Rondão
Sócio

TESTEMUNHAS:

CPF: [redacted]

MAICON ANCHIETA DA SILVA

CPF: [redacted]

Mariana P. Cardoso