Ministério da Justiça e Cidadania - MJC
Conselho Administrativo de Defesa Econômica - CADE
SEPN 515 Conjunto D, Lote 4 Ed. Carlos Taurisano, 1º andar - Bairro Asa Norte, Brasília/DF, CEP 70770-504
Telefone: (61) 3221-8577 e Fax: (61) 3326-9733 - www.cade.gov.br

CONTRATO nº 24/2016

PROCESSO nº 08700.001206/2016-47

CONTRATO DE PRESTAÇÃO DE SERVIÇOS QUE ENTRE SI CELEBRAM O CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA - CADE E A EMPRESA INFOSEC TECNOLOGIA DA INFORMAÇÃO LTDA PARA AQUISI DE SOLUÇÃO ANTIVÍRUS.

CONTRATANTE:

CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA - CADE, AUTARQUIA FEDERAL, vinculada ao Ministério da Justiça, criada pela Lei n° 4.137/1962, constituído em Autarquia Federal por força da Lei nº 8.884/93 e reestruturado pela Lei n° 12.529, de 30 de novembro de 2011, com sede no SEPN, entre quadra 515, Conjunto "D", Lote 04, Edifício Carlos Taurisano, Asa Norte, CEP 70.770-500, em Brasília–DF, inscrita no CNPJ/MF sob o nº 00.418.993/0001-16, doravante designado CONTRATANTE, neste ato representado por sua Coordenadora-Geral de Orçamento, Finanças e Logística, a Sra. **LUANA NUNES SANTANA**, brasileira, solteira, portadora Carteira de Identidade n.º 281537926 – SSP/SP e do CPF n.º 221.509.228-94, no uso da atribuição que lhe confere o art. 4º da Portaria n.º 142, de 08 de agosto de 2012, e

CONTRATADA:

INFOSEC TECNOLOGIA DA INFORMAÇÃO LTDA, inscrito(a) no CNPJ/MF sob nº 11.266.883/0001-00, com sede na SCN Quadra 5, Bloco A, Sala 1212, Torre Sul, Centro Empresarial Brasília Shopping - Asa Norte, CEP 70.715-900, fone 3033-5190, e-mail contato@infosecti.com.br, doravante denominado(a) **CONTRATADA**, neste ato representado por seu Diretor, Sr. **LEONARDO GARCIA ROCHA**, brasileiro, Identidade nº 2332793 - SSP/DF, CPF nº 001.496.351-50, devidamente qualificado(a)s, na forma da Lei nº 8.666, de 21 de junho de 1993, tendo em vista o que consta no Processo nº 08700.011292/2015-15, resolvem celebrar o presente **CONTRATO,** sujeitando-se as partes ao comando da Lei n. 10.520, de 17 de julho de 2002 e Lei 8.666, de 21 de junho de 1993 e alterações posteriores e demais normas pertinentes, observadas as cláusulas e condições seguintes:

DA FINALIDADE

O presente **CONTRATO** tem por finalidade formalizar e disciplinar o relacionamento contratual com vistas à execução dos trabalhos definidos e especificados na Cláusula Primeira – **DO OBJETO**, conforme Parecer n° 134/2016/CGMA/PFE-CADE-CADE/PGF/AGU (nº SEI 0264060), datado de 10/11/2016, da Procuradoria do CADE exarada no Processo nº **08700.001206/2016-47**.

1. **CLÁUSULA PRIMEIRA - DO OBJETO**

1.1. Aquisição de solução de segurança integrada para estações de trabalho e ambiente corporativo, baseado nas soluções de mercado com foco na monitoração e proteção da segurança tecnológica, por conseguinte em sua implantação, configuração, garantia, suporte e transferência de conhecimento para atendimento das necessidades do Conselho Administrativo de Defesa Econômica.

1.2. O Presente Termo de Contrato foi elaborado nos termos constantes do Termo de Referência CGTI 0180471, do Edital de Pregão Eletrônico nº 21/2015 MAPA (nº SEI 0250521 e de seus anexos, da legislação vigente e da minuta aprovada pela Procuradoria Federal Especializada junto ao CADE por meio do Parecer nº 134/2016, bem como a proposta da **CONTRATADA** registrada sob o nº SEI 0250942, de 10 de outubro de 2016, os quais encontram-se vinculados direta ou indiretamente ao presente Contrato e passam a fazer parte integrante deste instrumento, independentemente de sua transcrição.

2. **CLÁUSULA SEGUNDA - DAS ESPECIFICAÇÕES E CARACTERÍSTICAS**

2.1. Os serviços contratados compreenderão as atividades de:

I - Atualização da garantia junto ao fabricante;

II - Suporte técnico 24x7 on-site por um período de 12 (doze) meses;

III - Aquisição de licenças.

2.2. O Prazo de entrega, instalação, configuração e ativação dos sistemas e softwares não será superior a 60 dias corridos.

2.3. A **CONTRATADA** efetuará a instalação, configuração e ativação dos sistemas e softwares, atendendo integralmente às características e às necessidades do Conselho Administrativo de Defesa Econômica - CADE e responsabilizando-se por todas as conexões, materiais, acessórios e mão de obra necessária para o seu bom funcionamento.

2.4. Os sistemas e softwares deverão ser acompanhados de manuais de instalação, operação e manutenção, quando de sua entrega, bem como de todos os acessórios necessários ao seu pleno funcionamento.

2.5. Adicionalmente devem ser contratados também:

a) Serviços de instalação e customização dos produtos;

b) Serviços de suporte técnico on-site na modalidade 24x7 (vinte e quatro horas por dia e sete dias por semana).

Item	Descrição	Unidade	Quant.
1	Renovação da Solução de Segurança, Symantec Protection Suite Enterprise Edition 4.0 ou superior – Usuários	Unidade	450

1.1	Aquisição da Solução de Segurança, Symantec Protection Suite Enterprise Edition 4.0 ou superior – Usuários	Unidade	450

2.6. REQUISITOS TECNOLÓGICOS

2.7. Administração centralizada por console de gerenciamento única das soluções;

2.8. As configurações e gerenciamento da solução deverá ser realizada para maquinas físicas e virtuais através da mesma console;

2.9. Toda a solução padrão deverá funcionar com agente único na estação de trabalho e servidores físicos e virtuais a fim de diminuir o impacto ao usuário final.

2.10. Console de gerenciamento via tecnologia Web (HTTP e HTTPS);

2.11. Mecanismo de comunicação (via push) em tempo real entre servidor e clientes, para entrega de configurações e assinaturas;

2.12. O servidor de gerenciamento deverá possuir compatibilidade para instalação nos sistemas operacionais Microsoft Windows Server 2008, 2008 R2 ou superiores;

2.13. O servidor de gerenciamento deverá possuir compatibilidade para instalação em sistemas operacionais 32-bit e 64bit suportando ambiente virtual XEN, VMWARE e Microsoft Hyper-V;

2.14. Possuir integração com LDAP e Microsoft Active Directory, para importação da estrutura organizacional e autenticação dos Administradores;

2.15. Possibilidade de aplicar regras diferenciadas baseando na localidade lógica da rede;

2.16. Permitir que a localidade lógica da rede seja definida pelo conjunto dos seguintes itens:

2.16.1. IP e range de IP;

2.16.2. Endereço de Servidores de DNS, DHCP e WINS;

2.16.3. Conexão com o servidor de gerência;

2.16.4. Conexões de rede como VPN, Ethernet, Wireless e Modem;

2.17. Possibilidade de aplicar regras diferenciadas por grupos de usuários e máquinas;

2.18. O servidor de gerenciamento deverá permitir o uso de banco de dados relacional Microsoft SQL Server nas versões 2008 e superiores;

2.19. Permitir a opção instalação de Servidores de Gerenciamento adicionais fornecendo assim a possibilidade de trabalhar em modo de Load Balance e Failover.

2.20. Possuir na solução replicação nativa do Banco de Dados entre os Servidores de Gerenciamento com opção de customização do conteúdo à ser replicado (Assinaturas, Pacotes de Instalação, Políticas e Logs);

2.21. Possibilidade de instalação dos clientes em servidores, estações de trabalho e maquinas virtualizadas de forma remota via console de gerenciamento com opção de remoção de soluções previamente instaladas;

2.22. Descobrir automaticamente as estações da rede que não possuem o cliente instalado;

2.23. Fornecer ferramenta de pesquisa de estações e servidores da rede que não possuem o cliente instalado com opção de instalação remota;

2.24. 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;

2.25. Capacidade de criação de contas de usuário com diferentes níveis de acesso de administração e operação;

2.26. Instalação e atualização do software sem a intervenção do usuário;

2.27. Possibilidade de configurar o bloqueio da desinstalação, desabilitar o serviço do cliente, importar e exportar configurações e abrir a console do cliente, por senha;

2.28. Suportar redirecionamentos dos logs para um servidor de Syslog;

2.29. Utilizar os protocolos HTTP e HTTPS para comunicação entre console de gerenciamento e o cliente gerenciado;

2.30. Integrar com solução de Data Loss Prevention, para os e-mails de saída, possibilitando utilização de mais de um servidor de DLP, para um mesmo Gateway de SMTP;

2.31. Priorizar dos servidores de DLP utilizados na integração com o Gateway de SMTP, possibilitando balancear o tráfego a ser analisado;

2.32. Arquivar qualquer mensagem que viole as políticas corporativas, enviando-as para a estrutura de arquivamento do órgão;

2.33. Integrar com servidor de criptografia, para criptografar mensagens e anexos;

2.34. Permitir ou não endereços de email com caracteres especiais, para no mínimo percentagem (%), hífen (-) e caracteres 8-bit;

2.35. Rejeitar conexões que tentem serem abertas pelos comandos “HELO” e “EHLO”, sem que existam gravados seus endereços de “MX” e “A” nos servidores de DNS;

2.36. fazer filtragem do remetente a partir de uma correlação da reputação global, informada pelo fabricante do produto, em conjunto com a reputação local, restringindo conexões indesejadas;

2.37. Implementar pesquisas de reputação, a partir da console do produto, informando seu histórico de reputação, assim como, sua reputação atual;

2.38. Possuir integração com LDAP, para obtenção de detalhes e informações adicionais dos usuários envolvidos num incidente detectado;

2.39. Deve possuir integração com Active Directory, para autenticação de usuários da solução;

2.40. O servidor de gerenciamento contra a fuga de informações deverá utilizar, no mínimo, banco de dados relacional Oracle, por possibilitar sua criptografia;

2.41. Deve ter a capacidade de realizar atualização de versão e patches nos componentes da solução através da console de gerenciamento;

2.42. Deve ter a capacidade para criação das contas de usuário na console de gerenciamento com diferentes níveis de acesso, para no mínimo, administração e operação;

2.43. Deve utilizar cifragem para comunicação, no mínimo, entre console de gerenciamento e monitores, scanners e agentes;

2.44. Deve armazenar no banco de dados do produto, de forma cifrada, todos os dados relativos a incidentes;

2.45. Deve manter um histórico de todas as alterações em configurações e acompanhamentos de incidentes, tanto na console quanto na base de dados;

2.46. Deve permitir criptografar os dados no momento da captura (monitoração, servidores e agentes);

2.47. Deve possuir canais de comunicação autenticados e criptografados entre os componentes do sistema;

2.48. Deve possuir as senhas do sistema com hash, criptografadas e armazenamento seguro das credenciais de acesso aos repositórios de dados;

2.49. Deve ter a capacidade de indexação off-line de dados armazenados em sistemas em redes isoladas, sem conectividade pelo DLP;

2.50. Deve possuir logs detalhados de auditoria de atividade de transações do banco de dados;

2.51. Deve possuir logs detalhados de auditoria de alterações de políticas;

2.52. Deve utilizar somente portas de rede padrão, determinadas, fixas e conhecidas;

2.53. Deve ter suporte a servidores com hardware x86 e sistema operacional Windows e Linux, não requerendo a utilização de appliance;

2.54. A solução deve ser do tipo cliente/servidor, onde a parte servidora mantém todas as configurações definidas pelo administrador e a parte cliente busca ou recebe essas configurações do servidor. O software cliente é instalado em estações de trabalho e outros clientes, como tablets. O software de gerenciamento (parte servidora) é instalado em um ou mais servidores dedicados e dimensionados para esse fim, denominado, neste documento, de Servidores de Gerenciamento;

2.55. Permitir a instalação de Servidores de Gerenciamento adicionais, fornecendo assim a possibilidade de trabalho em redundância onde, no caso de falha de um dos servidores, o outro assume todas as funções da solução, sem provocar indisponibilidade para os endpoints;

2.56. Permitir o gerenciamento de clientes, incluindo inventário de software e hardware, com, no mínimo, os seguintes sistemas operacionais:

2.56.1. Windows Server 2008 e superior, 32 e 64 bits;

2.56.2. Windows 7, 32 e 64 bits;

2.56.3. iOS 6 e superior;

2.56.4. Android 2.2 e superior;

2.57. Permitir a instalação em máquinas virtuais sem impor nenhuma restrição ao funcionamento e aos recursos e funcionalidades;

2.58. Caso a solução ofertada utilize SGBD – Sistema Gerenciadores de Bancos de Dados, este deverá ser fornecido como bundle, ou seja, já embutido no custo da na solução;

2.59. Possibilitar o estabelecimento de alvos de políticas por filtros baseados em qualquer informação disponível sobre os clientes. Exemplos: configurações de sistema operacional, hardware, componentes, softwares e versões;

2.60. Clientes devem ser atualizados automaticamente nos grupos de políticas conforme a inclusão ou exclusão de clientes ou da mudança de suas configurações;

2.61. Implementar, na própria solução, código único para clientes, garantindo consistência para a base de dados mesmo com mudanças de hostname, endereço MAC da placa de rede, endereço IP ou outras informações nos clientes evitando a criação de registros duplicados;

2.62. Permitir forçar comunicação dos clientes a partir da console para atualizar as políticas e inventário;

2.63. Permitir a ativação e desativação do software cliente por meio da console de gerenciamento, sem necessidade de reinicialização do endpoint;

2.64. Permitir integração da solução com o Microsoft Active Directory, possibilitando, no mínimo, as seguintes tarefas:

2.64.1. Importação e sincronização de usuários, computadores, sites, unidades organizacionais e grupos do AD;

2.64.2. Permitir ao administrador criar agendamentos e definir horários ou frequência de importação;

2.64.3. Permitir a importação e sincronização diferencial, ou seja, apenas dos dados que apresentarem modificações em relação à última sincronização realizada, mantendo a alteração mais recente;

2.64.4. Permitir autenticação de usuários da solução, permitindo atribuir papeis na utilização da console de gerência;

2.65. Aplicação de políticas baseadas em grupos de AD;

2.66. Instalação automática do software cliente em computadores de grupos pré-definidos do AD que ainda não estejam sendo gerenciados;

2.67. Permitir o agendamento de instalação, atualização e desinstalação do software cliente via políticas no servidor a partir da console de gerenciamento da solução sem necessidade de reinício (boot) dos endpoints e de forma silenciosa, ou seja, sem interação com usuário;

2.68. Flexibilidade para definição da frequência de comunicação cliente-servidor;

2.69. Controlar banda de rede utilizada pelo cliente na sua comunicação com o servidor utilizando:

2.69.1. Configurações diferenciadas por faixa de horário;

2.69.2. Permissão para configurar exceções para políticas;

2.69.3. Bloqueio a comunicação por faixa de horário com as seguintes opções:

2.69.4. Comunicação total entre cliente-servidor e download;

2.70. Gerenciar a comunicação cliente-servidor com computadores:

2.70.1. Na LAN e/ou WAN;

2.70.2. Na Internet com VPN;

2.70.3. Na Internet;

2.71. Suporte a múltiplos domínios independente de sua estrutura ou relacionamento de confiança;

2.72. Deverá prover funcionalidade de envio de logs a servidor do tipo syslog;

2.73. Deverá permitir a definição de política geral que se aplique aos usuários que não estejam conectados à rede gerenciada pela instituição, para no mínimo:

2.73.1. Prover capacidade de habilitar somente os aplicativos homologados pela instituição, enquanto conectados à rede gerenciada;

2.73.2. Prover capacidade de separar a utilização dos aplicativos privados dos corporativos homologados;

2.74. A solução deverá possuir ferramenta de workflow nativa, devendo permitir customização dos processos;

2.75. A customização deve ser realizada em interface que permita arrastar-e-soltar;

2.76. Deverá apresentar lista de tarefas para prover uma visão de portal para usuário final,

permitindo que visualizem quais atividades requerem ação e processem atividades como parte do workflow;

2.77. Deverá possuir portal para gerenciamento de processos que provê visibilidade de todos os processos para administradores.

2.78. Deve ter a capacidade de delegar o gerenciamento com procedimentos “Self-Healing”, diminuindo tempo de suporte com tarefas padronizadas;

2.79. Deve ter a capacidade de executar de forma automática, sem a necessidade nenhum script e agentes externos ao software, a reparação, correção e falta de aplicações nos dispositivos móveis gerenciados;

2.80. Criptografia de Armazenamento Removível Baseada em Volúmes;

2.81. Serviços de criptografia e funções de interação do usuário suportados para máquinas que não são integrantes do domínio;

2.82. A solução deve proteger dados gravados em dispositivos USB, fire-wire, pen-drives, CD/DVDs, discos rígidos externos, cartões digitais protegidos, ipods, câmeras digitais, e em dispositivos, mesmo quando não identificados como "removíveis";

2.83. **Atualização de Vacinas**

2.84. Atualização incremental, remota e em tempo-real, da vacina dos Antivírus mecanismo de verificação (Engine) dos clientes da rede;

2.85. Permitir criar planos de distribuição das atualizações via comunicação segura entre cliente e Servidores de Gerenciamento, Site do fabricante, Via Servidor de atualização interno e podendo eleger qualquer cliente gerenciado para distribuição das atualizações;

2.86. Permitir eleger qualquer cliente gerenciado como um servidor de distribuição das atualizações com opção de controle de banda, quantidades de definições e espaço em disco utilizado, podendo eleger mais de um cliente para esta função;

2.87. Atualização remota e incremental da versão do software cliente instalado;

2.88. Nas atualizações das configurações e das definições de vírus não poderá utilizar login scripts, agendamentos ou tarefas manuais ou outros módulos adicionais que não sejam parte integrante da solução e sem requerer reinicialização do computador ou serviço para aplicá-la.

2.89. Atualização automática das assinaturas do servidores de gerenciamento e clientes via Internet, com periodicidade mínima diária;

2.90. Capacidade de voltar qualquer vacina e assinatura anterior armazenadas no servidor, utilizando opção e comando do Console podendo utilizar a arquitetura de grupos lógicos da console;

2.91. Um único e mesmo arquivo de vacina de Vírus para todas as plataformas Windows e versões do antivírus.

2.92. Quarentena

2.93. Possuir funcionalidades que permitam o isolamento (área de quarentena) de arquivos contaminados por códigos maliciosos que não sejam conhecidos ou que não possam ser reparados em um servidor central da rede;

2.94. Possibilidade de adicionar manualmente arquivos na quarentena do cliente com opção de restrições na console de gerenciamento;

2.95. **Cliente Gerenciado**

2.96. Suportar máquinas com arquitetura 32-bit e 64-bit;

2.97. O cliente para instalação em estações de trabalho e servidores deverá possuir compatibilidade com os sistemas operacionais Windows 7, Server 2008, 2008 R2, 2012 e superiores;

2.98. Possuir certificação FIPS 140-2;

2.99. Possuir certificação Common Criteria (CC) EAL2+;

2.100. O fabricante deverá possuir certificação ICSA Labs no mínimo nas plataformas Windows XP, Windows Vista e Windows 7;

2.101. **Funcionalidade de Firewall e Detecção e Proteção de Intrusão (IDS\IPS)**

2.102. Suporte aos protocolos TCP, UDP e ICMP;

2.103. Reconhecimento dos tráficos DNS, DHCP e WINS com opção de bloqueio;

2.104. Possuir proteção contra exploração de buffer overflow;

2.105. Possuir proteção contra ataques de Denial of Service (DoS), Port-Scan e MAC Spoofing;

2.106. Possibilidades de criação de assinaturas personalizadas para detecção de novos ataques;

2.107. Possibilidade de agendar a ativação da regra de Firewall;

2.108. Possibilidade de criar regras diferenciadas por aplicações;

2.109. Possibilidade de reconhecer automaticamente as aplicações utilizadas via rede baseado no fingerprint do arquivo;

2.110. Proteger o computador através da criação de uma impressão digital para cada executável existente no sistema, para que somente as aplicações que possuam essa impressão digital executem no computador;

2.111. Funcionalidade de Whitelist e Blacklist para o recurso de Impressão digital para os executáveis, possibilitando bloquear todos os executáveis da lista ou só liberar os executáveis da lista;

2.112. Permitir criação de zona confiável, permitindo que determinados IPs, protocolos ou aplicações se comuniquem na rede;

2.113. Bloqueio de ataques baseado na exploração da vulnerabilidade;

2.114. Gerenciamento integrado à console de gerência da solução;

2.115. Funcionalidade de Antivírus e Anti-Spyware as funcionalidades:

2.116. Proteção em tempo real contra vírus, trojans, worms, cavalos-de-tróia, spyware, adwares e outros tipos de códigos maliciosos.

2.117. Proteção anti-spyware deverá ser nativa do próprio antivírus, ou seja, não dependente de plugin ou módulo adicional;

2.118. As configurações do anti-spyware deverão ser realizadas através da mesma console de todos os itens da solução;

2.119. Permitir a configuração de ações diferenciadas para cada subcategoria de riscos de segurança (Adware, Discadores, Ferramentas de hacker, Programas de brincadeiras, Acesso remoto, Spyware, Trackware e outros);

2.120. Permitir a criação de listas de exclusões com informação da severidade, impacto e grau de remoção da ameaça nos níveis baixo, médio ou alto, onde os riscos excluídos não serão verificados pelo produto;

2.121. Permitir que verificação das ameaças da maneira manual, agendada e em Tempo-Real detectando ameaças no nível do Kernel do Sistema Operacional fornecendo a possibilidade de detecção

de Rootkits;

2.122. Implementar intervalos de tempo para início de verificações agendadas de forma a reduzir impacto em ambientes virtuais;

2.123. Verificação de vírus nas mensagens de correio eletrônico, pelo antivírus da estação de trabalho, suportando clientes Outlook, Notes e POP3/SMTP;

2.124. Capacidade de detecção em tempo real de vírus novos, desconhecidos pela vacina com opção da sensibilidade da detecção (baixo, médio e alto);

2.125. Capacidade de identificação da origem da infecção para vírus que utilizam compartilhamento de arquivos como forma de propagação, informando nome ou IP da origem com opção de bloqueio da comunicação via rede;

2.126. Possuir funcionalidades de otimização de scans em ambientes virtuais, contemplando os virtualizadores VMWare, Citrix e Microsoft, para no mínimo diferenciação automática entre máquinas físicas e virtuais, possibilitando aplicar as funcionalidades específicas para as máquinas virtuais;

2.127. Proteção com as mesmas funcionalidades aplicáveis em máquinas físicas, para no mínimo:

2.127.1. Proteção de antivírus e anti-spyware;

2.127.2. Proteção de heurística e reputação de arquivos em tempo real (real-time);

2.127.3. Proteção de IPS de rede e “host”;

2.127.4. Controle de dispositivos e aplicações;

2.128. Cache local na reputação de arquivos, possibilitando não varrer arquivos categorizados como não maliciosos e já escaneados anteriormente;

2.129. Capacidade de verificar “templates” de máquinas virtuais, excluindo da operação de varredura todos os arquivos categorizados como confiáveis, existentes na máquina virtual utilizada como origem (template);

2.130. Capacidade de implementar varreduras otimizadas em máquinas físicas e virtuais, onde o arquivo verificado pela varredura uma vez, não será verificado novamente, até que ocorra alguma alteração no mesmo;

2.131. Capacidade de realizar monitoramento em tempo real (real-time) por heurística correlacionando com a reputação de arquivos;

2.132. Capacidade de verificar a reputação de arquivos, correlacionando no mínimo as seguintes características:

2.132.1. Origem confiável;

2.132.2. Origem não confiável;

2.132.3. Tempo de existência do arquivo na internet;

2.132.4. Comportamento do arquivo;

2.132.5. Quantidade mínima de usuários que baixaram o arquivo da internet;

2.133. Capacidade de implementar regras distintas por grupo (ex. Departamento), a partir do resultado da reputação, em conjunto com o correlacionamento da quantidade de utilizadores do arquivo e tempo de existência do mesmo;

2.134. Deve ter a capacidade de executar backup de forma manual, assim como, o agendamento dos backups, facilitando assim a criação dos pontos de recuperação;

2.135. Deve ter a capacidade de explorar arquivos de um ponto de recuperação, atribuindo uma

letra de unidade visível no Windows Explorer, podendo executar no mínimo as seguintes tarefas:

2.135.1. Executar o ScanDisk ou CHKDSK;

2.135.2. Executar uma verificação de vírus;

2.135.3. Copiar pastas ou arquivos em um local alternativo;

2.136. Exibir informações do disco sobre a unidade tal como espaço usado e o espaço livre;

2.137. Deve ter a capacidade de configurar a taxa máxima de transmissão utilizada via rede durante a criação do ponto de recuperação quando salvo na rede;

2.138. Deve ter a capacidade de especificar quais mensagens da solução (erros, avisos e informações) serão registradas conforme ocorrerem, determinar onde o arquivo é armazenado, fornecer informações úteis sobre o status dos jobs de backups, dos eventos relacionados, podendo ainda configurar emissão de alertas via e-mail;

2.139. Deve ter a capacidade de executar comandos durante, no mínimo, um dos seguintes estágios da criação de um ponto de recuperação:

2.139.1. Antes da captura dos dados;

2.139.2. Depois da captura dos dados;

2.139.3. Depois da criação de pontos de recuperação;

2.140. Deve ter a capacidade de usar senha e criptografia AES de 128, 192 ou 256 bits para proteger o ponto de recuperação contra acesso e uso não autorizados;

2.141. Deve ter a capacidade de identificar discos externos pelo seu GUID (Globally Unique IDentifier), indiferentemente da letra do drive assinalada pelo Windows, mesmo que a letra do disco seja alterada, o backup deverá ser concluído com sucesso;

2.142. Deve permitir restaurar um computador a partir de um local remoto, utilizando a opção de “inicialização do ambiente de recuperação” no menu de inicialização do Windows;

2.143. Deverá permitir copiar sistema operacional, aplicativos e dados de uma unidade de disco rígido para outra unidade;

2.144. Deverá integra-se com mecanismo de busca (Google Desktop e Microsoft Windows Search) gerando assim um catálogo de todos os arquivos contidos dentro do ponto de recuperação facilitando a pesquisa de arquivos inclusos no ponto de recuperação;

2.145. Deve permitir restaurar os pontos de recuperação para ambientes virtualizados, suportando no mínimo:

2.145.1. VMware Workstation 5, e 6;

2.145.2. VMware ESX Server 3.5 e 4.0;

2.145.3. VMware ESXi Server 3.5 e 4.0;

2.145.4. VMware Server 10 e 2.0;

2.145.5. Vmware Vsphere 4;

2.145.6. Microsoft Hyper-V;

2.146. **Funcionalidade de detecção Proativa de reconhecimento de novas ameaças com as funcionalidades**

2.147. Funcionalidade de detecção de ameaças desconhecidas que estão em memória por comportamento dos processos e arquivos das aplicações;

2.148. Não utilizar a assinatura de vírus para esta funcionalidade e fornecer assinatura

periódicas da técnica de detecção;

2.149. Capacidade de detecção keyloggers, Trojans, spyware e Worms por comportamento dos processos em memória, com opção da sensibilidade distintas da detecção;

2.150. Reconhecimento comportamento malicioso de modificação da configuração de DNS e arquivo Host;

2.151. Possuir a funcionalidade de exclusão de detecção diferenciada do recurso de Antivírus;

2.152. Possibilidade de habilitar o recurso de correlacionamento da funcionalidade de detecção Pró-Ativa com a base de reputação do fabricante;

2.153. Capacidade de detecção de Trojans e Worms por comportamento dos processos em memória, com opção da sensibilidade distintas da detecção;

2.154. Possibilidade de agendar o escaneamento da detecção PróAtiva com periodicidade mínima por minuto e em todos os novos processos;

2.155. Possibilidade de agendar o escaneamento da detecção PróAtiva com periodicidade mínima por minuto e em todos os novos processos;

2.156. **Funcionalidade de Controle de Dispositivos e Aplicações**

2.157. Gerenciar o uso de dispositivos USB e CD/DVD, através de controles de leitura/escrita /execução do conteúdo desses dispositivos e também sobre o tipo de dispositivo permitido (ex: permitir mouse USB e bloquear disco USB);

2.158. Controlar o uso de dispositivos com comunicação infravermelho, firewire, PCMCIA, portas seriais e paralelas, através de mecanismos de permissão e bloqueio identificando pelo "Class ID" e pelo "Device ID" do Dispositivo;

2.159. Permitir criar políticas de bloqueio de dispositivos baseadas na localização atual da estação;

2.160. Gerenciamento integrado à console de gerência da solução;

2.161. Oferecer proteção para o sistema operacional, permitindo a definição de controles de acesso (escrita/leitura) para arquivos, diretórios, chaves de registro e controle de processos;

2.162. Permitir o bloqueio do uso de aplicações baseado em nome, diretório e hash da aplicação;

2.163. **Relatórios e Monitoramentos com as funcionalidades**

2.164. Capacidade de Geração de relatórios, estatísticos e gráficos contendo no mínimo os seguintes tipos pré-definidos:

2.164.1. As 10 máquinas com maior ocorrência de códigos maliciosos;

2.164.2. Os 10 usuários com maior ocorrência de códigos maliciosos;

2.164.3. Localização dos códigos maliciosos;

2.164.4. Sumários das ações realizadas;

2.164.5. Número de infecções detectadas diário, semanal e mensal;

2.164.6. Códigos maliciosos detectados.

2.165. **Console avançada de distribuição e relatórios**

2.166. Console de gerenciamento via tecnologia Web (HTTP e HTTPS) independente da console central da solução;

2.167. Possibilidade de executar inventário do ambiente e descobrir os antivírus e respectivas

versões;

2.168. Detectar e desinstalar soluções de antivírus dos seguintes fabricantes:

2.168.1. McAfee

2.168.2. Symantec

2.168.3. Trend Micro

2.169. Permitir a remoção de outros softwares não desejados;

2.170. Criar tarefas de migração baseadas no resultado do inventário de antivírus;

2.171. Permitir agendamento e implementar controle de banda para minimizar impacto na rede durante o processo de instalação em clientes;

2.172. Possibilidade de recuperar instalação em clientes em caso de falha;

2.173. Oferecer relatórios avançados através da criação de cubos OLAP e tabelas Pivot.

2.174. Os seguintes cubos devem ser disponibilizados para criação de relatórios:

2.174.1. Alertas;

2.174.2. Clientes;

2.174.3. Políticas;

2.174.4. Rastreamento;

2.175. Possibilidade de criação de indicadores de performance para medir eficácia da solução de segurança;

2.176. Exportar os relatórios criados nos formados xls, pdf e html;

2.177. **Proteção na Mensageria**

2.178. Deve ser compatível com os sistemas operacionais Windows Server 2003 e Windows Server 2008, ambos em 32bits e 64bits;

2.179. Deve suportar Cluster Ativo/passivo da solução Exchange;

2.180. Deve ser compatível com Exchange Server, 2010 e 2013;

2.181. Deve ser compatível com VSAPI versões 2.0, 2.5 e 2.6;

2.182. Deve ser compatível com ambientes virtuais Vmware e Hyper-V;

2.183. Deve permitir instalação remota;

2.184. Deve possuir recurso para rastreamento de mensagens (Message Tracking) na própria console de gerenciamento com capacidade de pesquisa por subject, sender e recipient, verificando-se a ação tomada para especifica mensagem, sem necessidade de integração com produtos de terceiros ou “open source”;

2.185. Deve possuir capacidade de realizar o rastreamento da mensagem, citada no item anterior, em todos os appliances /equipamentos da solução ofertada;

2.186. Deve permitir realizar o rastreamento da mensagem, conforme citado anteriormente, utilizando caracteres double-byte para líguas estrangeiras;

2.187. Deve possuir funcionalidade de criação de Alias e Mascaramento de endereço;

2.188. Deve ser possível realizar notificação do administrador por email caso os filtros antispam não recebam atualizações por um determinado período de tempo;

2.189. Deve ser capaz de integração com LDAP Microsoft Active Directory 2008 ou superiores

para sincronização e autenticação;

2.190. Deve permitir a criação de políticas diferenciadas para tratamento de SPAM, Virus, Filtragem de Conteúdo e Controle de reputação (traffic shaping), de acordo com o destinatário da mensagem e reputação de origem;

2.191. Deve ser capaz de sincronizar usuários e grupos do LDAP para reconhecimento do usuários válidos e ações de Virus, Spam e Filtragem de Conteúdo diferenciadas por grupo do LDAP;

2.192. Deve ser capaz de utilizar a integração dos usuários do LDAP, validando existência dos mesmos possibilitando o descarte e rejeição, não enviando mensagens para o servidor de correio eletrônico, sem o devido destinatário dentro da base LDAP, evitando processamento desnecessário por parte do servidor de correio eletrônico;

2.193. Deve possuir mecanismos de backup/restore da configuração existente na solução;

2.194. Deve ser capaz de processar o tráfego de mensagens de entrada e de saída, com políticas diferenciadas para cada sentido de tráfego;

2.195. Deve permitir a execução de múltiplas ações para uma mesma mensagem que for categorizada como SPAM ou violação dos filtros de conteúdo, entre elas:

2.195.1. Apagar mensagem;

2.195.2. Enviar para Quarentena;

2.195.3. Encaminhar mensagem;

2.195.4. Encaminhar em BCC;

2.195.5. Gravar mensagem em disco;

2.195.6. Gravar em pasta de conformidade;

2.195.7. Modificar o assunto;

2.195.8. Adicionar informações ao cabeçalho;

2.195.9. Deferir a mensagem;

2.195.10. Rejeitar a mensagem;

2.196. Deve ter a capacidade de verificação em tempo real de SMTP;

2.197. Deve ter a capacidade de verificação em tempo real de mensagens em trânsito interno;

2.198. Deve ter a capacidade de verificação manual dos message stores;

2.199. Deve ter a capacidade de verificação agendada dos message stores;

2.200. Deve permitir verificar mailbox stores e public foldes;

2.201. Deve permitir definir a “idade mínima” das mensagens a serem verificadas;

2.202. Deve ter a capacidade de definir limites de verificação, no mínimo, baseados em:

2.202.1. Tempo máximo de verificação;

2.202.2. Número máximo de decomposição de arquivos compactados recursivamente;

2.202.3. Tamanho máximo do arquivo descompactado;

2.202.4. Número máximo de arquivos descompactados;

2.203. Deve ser capaz de quando a mensagem for gravada em pasta de conformidade, permitir definir ações distintas para as mensagens aprovadas e reprovadas;

2.204. Deve possuir capacidade de notificar remetente, destinatário, administrador e outros

e-mails, simultaneamente;

2.205. Deve ter precisão de identificação de spam de pelo menos 95% (spam-catching rate);

2.206. Deve ter precisão de filtragem de pelo menos 99,9999% (accuracy rate);

2.207. Deve possuir centro especializado, 24x7, com monitoramento de mais de 2 milhões de mailboxes, para processamento de SPAMs recebidos e criação automática de novos filtros/assinaturas;

2.208. Deve permitir atualização automática dos filtros a cada 10 minutos, sem interrupção dos serviços;

2.209. Deve ter suporte a listas negras e listas brancas com opção por domínio, endereço de e-mail e endereço IP;

2.210. Deve ter a capacidade de bloquear mensagens consideradas como SPAM baseado na utilização de listas DNSBL (DNS BlackHole) ou RBL (Real Time Black List);

2.211. Deve ter a capacidade de reconhecimento de ameaças DiaZero, com assinatura de suspeitos de vírus;

2.212. Deve ter capacidade de utilização de pelo menos as seguintes tecnologias de detecção de spam:

2.212.1. Assinaturas para corpo da mensagem e anexos;

2.212.2. Estrutura da mensagem;

2.212.3. Filtros de reputação local (criado automaticamente através da análise das mensagens recebidas) e global (criado pela rede de monitoramente do fornecedor da solução);

2.212.4. Identificação de idiomas;

2.212.5. Filtros de URLs;

2.212.6. Filtros anti-phishing;

2.213. Deve possuir capacidade para criação de filtros baseados no cabeçalho, remetente, tipos e conteúdo de anexos, dicionários de palavras, assunto e corpo da mensagem, incluindo o uso de expressões regulares;

2.214. Deve permitir a criação de "compliance folders", para armazenagem de mensagens (entrada/saída) que violem alguma política de conteúdo criada pelo Administrador;

2.215. Deve possuir tecnologia para detecção de ataques de Spam, Vírus e Diretório (Usuários Inválidos);

2.216. Deve possuir recurso para a detecção de ataques, que penalize dinamicamente a origem baseado no nível de reputação, com dez níveis de sensibilidade;

2.217. Deve possuir a cada nível da detecção dos ataques, citados anteriormente, o controle do percentual de mensagens que serão recusadas;

2.218. Deve possuir a cada nível da detecção dos ataques, citados anteriormente, o tempo limite para nova tentativa de conexão, número de conexões por IP e número de mensagens por conexão;

2.219. Deve possuir tecnologia para prevenção de ataques de “Bounce Messages”;

2.220. Deve possuir a capacidade de implementar Sender Policy Framework (SPF) e SenderID;

2.221. Deve possuir a capacidade para criação de regras baseada no tipo de arquivo anexado;

2.222. Deve possuir a capacidade para criação de regras baseada na detecção por “Wildcard”;

2.223. Deve possuir a capacidade para criação de regras baseada na detecção por expressões

regulares;

2.224. Deve possuir a capacidade de implementar comunicação segura via TLS (Transport Layer Security);

2.225. Deve possuir capacidade de configurar criptografia TLS por domínio e por política;

2.226. Deve ter capacidade de detecção a pelo menos 10 idiomas (incluindo Português), permitindo o bloqueio de mensagens escritas nos idiomas não desejados;

2.227. Deve possuir a capacidade de atualização automática periódica da lista de IP's confiáveis, citada no item anterior;

2.228. Deve ter a capacidade de deleção total de mensagens enviadas por "Mass-Mailing Worms", com opção de ações diferenciadas por tráfego de entrada e saída;

2.229. Deve ter a capacidade de reconhecimento de Spywares e Adwares;

2.230. Deve possuir recurso para detecção dos ataques de duas escalas para Vírus e Diretório (LDAP), capaz de deferir a conexão SMTP caso a fonte emissora tenha enviado um percentual de mensagens consideradas como usuários inválidos ou infectadas com vírus, em um determinado espaço de tempo, ambos configuráveis pelo administrador;

2.231. Deve possuir módulo de antivírus para detecção de conteúdo malicioso nas mensagens, do mesmo fabricante da solução antispam;

2.232. Deve ter a capacidade de bloquear arquivos anexos por extensão, tipo real do arquivo (True Type File), Mime Type e nome do arquivo;

2.233. Deve ter a capacidade de implementar quarentena por usuário, possibilitando que cada usuário possa administrar sua própria quarentena, removendo mensagens ou liberando as que não são SPAM, diminuindo a responsabilidade do administrador e também a possibilidade de bloqueio de e-mails legítimos;

2.234. O módulo de quarentena deverá ser capaz de enviar uma notificação periódica para os usuários, informando as mensagens consideradas como SPAM que foram inseridas na quarentena (digest);

2.235. Remoção automática das mensagens armazenadas em quarentena de acordo com as configurações definidas pelo administrador;

2.236. Deve permitir que o usuário cadastre endereços de e-mail em listas negras/listas brancas pessoais;

3. CLÁUSULA TERCEIRA - VIGÊNCIA

3.1. O Contrato deverá ter vigência de 12 (doze) meses, a contar do dia 30 de novembro de 2016.

4. CLÁUSULA QUARTA – PREÇO

4.1. O valor do presente Termo de Contrato é de **R$ 88.123,50** (**oitocentos e oitenta mil, cento e vinte e três reais e cinquenta centavos**).

4.1.1. No valor 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;

Item	Descrição	Qtd	Valor Unitário R$	Total R$
1	Renovação da Solução de Segurança, Symantec Protection Suite Enterprise Edition 4.0 ou superior – Usuários	450	R$ 92,53	R$ 41.638,50
1.1	Aquisição da Solução de Segurança, Symantec Protection Suite Enterprise Edition 4.0 ou superior – Usuários	450	R$ 103,30	R$ 46.485,00

5. CLÁUSULA QUINTA – DOTAÇÃO ORÇAMENTÁRIA

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

Programa de Trabalho: **109744**

Funcional Programática: **14.422.2081.2807.0001**– Projetos Estratégicos - TI

Natureza de Despesa: **4. 4. 9. 0. 39. 93. (item 1) e 3 .3 .9. 0. 39. 08 (item 1.1)**

Plano Interno: **CE999PECAD**

5.2. Poderão ser incluídas novas dotações orçamentárias (reforço ou novos recursos provenientes de outras Unidades) mediante a emissão de termo de apostilamento.

6. CLÁUSULA SEXTA – PAGAMENTO

6.1. O pagamento será efetuado em até 30 (trinta) dias após o ateste de recebimento das aquisições pelo fiscal do contrato. Será efetuado pagamento referente ao total de licenças entregues, com base na Ordem de Serviço correspondente, conforme disposto no Art. 73 da Lei nº 8.666/93, observado o disposto no Art. 36, § 3º da IN nº 02, de 30 de abril de 2008, mediante Ordem Bancária;

6.2. A Nota Fiscal/Fatura deverá obrigatoriamente ser atestada pelo fiscal especialmente designado;

6.3. A Nota Fiscal/Fatura deverá vir acompanhada dos seguintes documentos: comprovantes, relatórios, ordens de serviços e outros congêneres. Deverá também ser acompanhada da regularidade fiscal, constatada por meio de consulta "on-line" ao Sistema de Cadastramento Unificado de Fornecedores – SICAF, ou na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 29 da Lei 8.666, de 21 de junho de 1993;

6.4. O pagamento será creditado em favor da **CONTRATADA**, por meio de ordem bancária. Deve ficar explicitado o nome do banco, agência, localidade e número da conta corrente em que deverá ser efetivado o crédito, o qual ocorrerá até 30 dias contados a partir da data final do período de adimplemento de cada parcela;

6.5. No caso de incorreção dos documentos apresentados, inclusive da Nota Fiscal, serão estes restituídos à **CONTRATADA** para as correções que se fizerem necessárias, não respondendo o **CONTRATANTE** por quaisquer encargos resultantes de atrasos na liquidação dos pagamentos correspondentes;

6.6. Na hipótese da ocorrência acima, o prazo para liquidação passará a contar a partir de sua correção;

6.7. Será procedida consulta ***"ON LINE"*** junto ao **SICAF** antes de cada pagamento a ser efetuado à **CONTRATADA**, para verificação da situação dela, relativamente às condições exigidas na contratação, cujos resultados serão impressos e juntados aos autos do processo próprio;

6.8. A **CONTRATADA** deverá estar ciente que, em caso de aplicação da sanção de multa, ela poderá ser recolhida por intermédio de Guia de Recolhimento da União – GRU, ou descontado de fatura ou crédito existente no **CONTRATANTE** em favor da **CONTRATADA**;

6.9. Caso o valor seja superior ao crédito eventualmente existente, a diferença será cobrada administrativamente ou judicialmente, se necessário;

6.10. Eventuais atrasos de pagamento provocados exclusivamente pela Administração, o valor devido deverá ser acrescido de atualização financeira, e sua apuração se fará desde a data de seu vencimento até a data do efetivo pagamento, em que os juros de mora serão calculados à taxa de 0,5% (meio por cento) ao mês, ou 6% (seis por cento) ao ano, mediante aplicação das seguintes fórmulas:

$$I = \frac{(TX/100)}{365}$$

EM = I x N x VP, onde:

I = Índice de atualização financeira;

TX = Percentual da taxa de juros de mora anual;

M = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela em atraso.

6.11. A **CONTRATADA** deverá encaminhar as Notas Fiscais/faturas até o 2º (segundo) dia útil do mês subsequente ao fornecimento do bem ou prestação dos serviços;

6.12. O **CONTRATANTE** disporá do prazo de 03 (três) dias para efetuar o atesto, ou rejeitar os documentos de cobrança por erros ou incorreções em seu preenchimento;

6.13. O **CONTRATANTE** disporá do prazo de 30 (trinta) dias corridos a partir da data final do período de adimplemento de cada parcela, para ultimar o pagamento;

6.14. O **CONTRATANTE** não fará nenhum pagamento a **CONTRATADA** antes de paga ou relevada a multa que porventura lhe tenha sido aplicada;

6.15. A descrição contida na Nota Fiscal/fatura deverá ser idêntica à do objeto a ser contratado, não sendo aceitas quaisquer variações em sua descrição;

6.16. O **CONTRATANTE** rejeitará, todo ou em parte, qualquer material fornecido com imperfeições ou que contenha especificação dessemelhante ao objeto;

6.17. O período de faturamento deverá ser exatamente idêntico ao mês do fornecimento dos

bens;

6.18. Em nenhuma hipótese será efetuado o pagamento de Notas Fiscais/Faturas com o número do CNPJ diferente do que foi apresentado na fase de licitação, mesmo que sejam empresas consideradas matriz e filial, vice-versa ou pertencentes ao mesmo grupo ou conglomerado;

6.19. A **CONTRATADA** regularmente inscrita no Simples Nacional, nos termos da LC nº 123 de 2006, não sofrerá a retenção tributária. 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, a fim de evitar a retenção na fonte de tributos e contribuições, conforme legislação em vigor;

6.20. Na hipótese de a **CONTRATADA** receber valores indevidos, o indébito será apurado em moeda corrente na data do recebimento do valor indevido e atualizado, desde a data da apuração até o efetivo recolhimento;

6.21. A quantia recebida indevidamente será descontada dos pagamentos devidos à **CONTRATADA**, devendo o **CONTRATANTE** notificá-la do desconto e apresentar a correspondente memória de cálculo;

PARÁGRAFO SEGUNDO - Na hipótese de inexistirem pagamentos a serem efetuados, o **CONTRATANTE** deverá notificar a **CONTRATADA** para que recolha, no prazo máximo de 05 (cinco) dias úteis da data do recebimento do comunicado, a quantia paga indevidamente, por meio da Guia de Recolhimento da União – GRU

7. CLÁUSULA SÉTIMA – GARANTIA DOS BENS

7.1. A **CONTRATADA** concederá ao **CONTRATANTE** garantia integral durante 12 (doze) meses, “on-site” com atendimento 24 horas por dia e sete dias por semana, a contar da data de homologação do produto, contra qualquer defeito ou problema em toda a solução, incluindo avarias no transporte dos equipamentos até o local de entrega, mesmo ocorrida sua aceitação/aprovação pelo contratante;

7.2. A **CONTRATADA** garante por, no mínimo, 12 (doze) meses o fornecimento dos componentes de software, para manutenções, suporte técnico ou ampliações, de forma que possam ser mantidas todas as funcionalidades inicialmente contratadas.

7.3. Durante o período de garantia, deve ser efetuada manutenção preventiva, em intervalos predeterminados e de acordo com critérios prescritos pelo **CONTRATANTE**, destinada a reduzir a probabilidade de falha ou a degradação do funcionamento da solução, para tanto, o proponente deve fornecer, quando da assinatura do contrato, cronograma com previsão das manutenções preventivas;

7.4. Manutenção corretiva será efetuada sempre que a solução apresente falhas que impeçam o seu funcionamento normal e/ou requeiram a intervenção de técnico especializado;

7.5. As manutenções preventivas e corretivas serão de responsabilidade da **CONTRATADA**, sem custos adicionais ao **CONTRATANTE**;

7.6. Durante o período de garantia, qualquer componente que apresente defeito ou mau funcionamento, sem indicação de solução, deve ser substituído imediatamente.

8. CLÁUSULA OITAVA - GARANTIA CONTRATUAL

8.1. A garantia contratual irá corresponder a 5% do valor contratado. Neste caso o **CONTRATANTE** exigirá da **CONTRATADA,** no ato da assinatura da **CONTRATADA**, a prestação de garantia contratual pela execução das obrigações assumidas, cabendo a ela optar por uma das

modalidades previstas em Lei: caução em dinheiro ou título da dívida pública, fiança bancária e seguro-garantia.

8.1.1. Para assegurar o integral cumprimento de todas as obrigações contratuais assumidas, inclusive indenização a terceiros e multas eventuais aplicadas, a **CONTRATADA** apresentará garantia após a assinatura do Termo de Contrato em favor do **CONTRATANTE**, mediante a uma das modalidades descritas na Lei 8.666/93 no valor **R$ 4.406,17 (quatro mil quatrocentos e seis reais e dezessete centavos)** correspondente a 5% (cinco por cento) do valor global do Termo de Contrato.

8.2. A exigência de garantia de execução do Contrato, nos moldes do art. 56 da Lei no 8.666, de 1993, com validade durante a execução do Termo de Contrato e 3 (três) meses após o término da vigência contratual;

8.3. A **CONTRATADA** deverá apresentar, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do **CONTRATANTE**, contado da assinatura do Termo de Contrato, comprovante de prestação de garantia, podendo optar por caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária, sendo que, nos casos de contratação de serviços continuados de dedicação exclusiva de mão de obra, o valor da garantia deverá corresponder a cinco por cento do valor total do Termo de Contrato;

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

8.4.1. Prejuízos advindos do não-cumprimento do objeto do Termo de Contrato e do não-adimplemento das demais obrigações nele previstas;

8.4.2. Prejuízos causados à Administração ou a terceiros, decorrentes de culpa ou dolo durante a execução do Termo de Contrato;

8.4.3. Multas moratórias e punitivas aplicadas pela Administração à **CONTRATADA**;

8.4.4. Obrigações trabalhistas, fiscais e previdenciárias de qualquer natureza, não adimplidas pela **CONTRATADA**.

8.5. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados nos itens da subcláusula anterior;

8.6. A garantia em dinheiro deverá ser efetuada na Caixa Econômica Federal em conta específica com correção monetária, em favor do **CONTRATANTE**;

8.7. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor do Termo de Contrato por dia de atraso, observado o máximo de 2% (dois por cento);

8.8. O atraso superior a 25 (vinte e cinco) dias autoriza a Administração a promover a rescisão do Termo de Contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem os incisos I e II do art. 78 da Lei nº 8.666, de 1993;

8.9. O garantidor não é parte interessada para figurar em processo administrativo instaurado pelo **CONTRATANTE** com o objetivo de apurar prejuízos e/ou aplicar sanções à **CONTRATADA**;

8.10. A garantia será considerada extinta:

8.10.1. 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 Administração, mediante termo circunstanciado, de que a **CONTRATADA** cumpriu todas as cláusulas do Termo de Contrato;

8.10.2. Após o término da vigência do Termo de Contrato, deve o instrumento convocatório estabelecer o prazo de extinção da garantia, que poderá ser estendido em caso de

ocorrência de sinistro.

8.11. A garantia prestada pela **CONTRATADA** será liberada ou restituída após o término do Termo de Contrato, caso não haja pendências, observado o disposto no art. 56, § 4º, da Lei nº 8.666, de 21 de junho de 1993, se for o caso;

8.12. Se a garantia for utilizada em pagamento de qualquer obrigação, a **CONTRATADA** se obrigará a fazer a respectiva reposição, no prazo máximo de 48 horas (quarenta e oito) horas, a contar da data em que for notificada pela **CONTRATANTE**;

8.13. Quando se tratar de caução em dinheiro, o adjudicatário fará o devido recolhimento em entidade bancária e conta indicada pela **CONTRATANTE**; em se tratando de fiança bancária, deverá constar do instrumento a renúncia expressa pelo fiador dos benefícios previstos nos arts. nºs. 827 e 836 do Código Civil;

8.14. Encerrada a vigência contratual, a empresa solicitará a devolução da garantia ao fiscal do Termo de Contrato por meio de documento contendo o timbre da empresa e assinado pelo responsável;

8.15. O fiscal verificará possíveis débitos de execução ou de pagamentos. Caso não exista, encaminhará Nota Técnica ao Gestor solicitando a sua devolução;

8.16. O Gestor encaminhará à área responsável o pedido, bem como a Nota Técnica, solicitando providências quanto a devolução;

8.17. A área responsável irá elaborar ofício autorizando a **CONTRATADA** a retirar o valor, junto a instituição em que se encontra a garantia;

8.18. O **CONTRATANTE** não executará a garantia nas seguintes hipóteses:

8.18.1. Caso fortuito ou força maior;

8.18.2. Alteração, sem prévia anuência da seguradora ou do fiador, das obrigações contratuais;

8.18.3. Descumprimento das obrigações pela **CONTRATADA** decorrente de atos ou fatos da Administração;

8.18.4. Prática de atos ilícitos dolosos por servidores da Administração.

9. CLÁUSULA NONA - CONDIÇÕES DE ENTREGA E RECEBIMENTO

9.1. Os bens objetos deste Contrato deverão ser entregues na forma de licença de software;

9.2. São consideradas como condições a garantia do material/equipamento ou bem a ser fornecido, conforme este instrumento;

9.3. O prazo de entrega dos bens é de 60 dias corridos, contados da assinatura do contrato, em remessa única, no seguinte endereço: SEPN 515 Conjunto D, Lote 4 - Ed. Carlos Taurisano CEP 72.770-504, Brasília, DF (61) 3221-8552;

9.4. Na hipótese de a verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo;

9.5. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da **CONTRATADA** pelos prejuízos resultantes da incorreta execução do Termo de Contrato.

10. CLÁUSULA DÉCIMA - FISCALIZAÇÃO

10.1. A Administração do **CONTRATANTE** designará servidor para acompanhamento e fiscalização do fornecimento do objeto, nos termos da Lei nº 8.666, de 21 de junho de 1993;

10.2. O acompanhamento e a fiscalização da execução do Termo de Contrato consistem na verificação da conformidade da prestação dos serviços e da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento do Termo de Contrato;

10.3. O recebimento de material de valor superior a R$ 80.000,00 (oitenta mil reais) será confiado a uma comissão de, no mínimo, 3 (três) membros, designados pela autoridade competente;

10.4. O servidor especialmente designado anotará, em registro próprio, todas as ocorrências relacionadas com a execução do Termo de Contrato, determinando o que for necessário à regularização, bem como dirimir as dúvidas que surgirem no curso da execução, fornecimento ou prestação dos serviços;

10.5. As providências que ultrapassarem a competência do fiscal deverão ser solicitadas aos seus superiores, em tempo hábil, para a adoção de medidas convenientes;

10.6. A fiscalização exercida pelo **CONTRATANTE** não excluirá ou reduzirá a responsabilidade da **CONTRATADA** pela completa e perfeita execução dos serviços/fornecimento dos bens;

10.7. Os esclarecimentos solicitados pela fiscalização deverão ser prestados imediatamente;

10.8. A fiscalização não aceitará, sob nenhum pretexto, a transferência de qualquer responsabilidade da **CONTRATADA** para outras entidades, sejam fabricantes, técnicos, subempreiteiros, dentre outros;

10.9. A fiscalização poderá sustar, recusar, solicitar que seja refeito ou entregue qualquer item que não esteja de acordo com as condições, exigências e especificações estipuladas;

10.10. A fiscalização poderá solicitar a aplicação das penalidades previstas neste Contrato a qualquer momento, desde que observadas irregularidades com as obrigações assumidas;

10.11. O fiscal designado atestará as notas fiscais/faturas emitidas pela **CONTRATADA**, referentes ao objeto, verificando, para tanto, a regularidade da empresa junto ao SICAF, bem como toda a documentação de comprovação do fornecimento do objeto.

11. CLÁUSULA DÉCIMA PRIMEIRA - OBRIGAÇÕES DO CONTRATANTE

11.1. O fornecimento do objeto, bem como as obrigações da **CONTRATADA,** não reduz, diminui, exime ou exclui as obrigações do **CONTRATANTE** perante o fornecimento do objeto;

11.2. Para fornecimento do bem, o **CONTRATANTE** se obriga a dar plenas condições a **CONTRATADA** para desempenhar ou desenvolver suas atividades, exclusivamente em decorrência do fornecimento do bem nas condições estipuladas;

11.3. O **CONTRATANTE** se obriga a efetuar os pagamentos na forma definida na Cláusula específica para tal;

11.4. O **CONTRATANTE** deverá acompanhar o fiel cumprimento das obrigações e/ou condições estipuladas, seja por meio de Comissão ou de fiscal designado para tal, na forma prevista em Lei;

11.5. O **CONTRATANTE** se obriga a prestar todos os esclarecimentos necessários para a **CONTRATADA** cumprir com as suas obrigações;

11.6. Comunicar oficialmente a **CONTRATADA** quaisquer falhas verificadas no cumprimento do Termo de Contrato;

11.7. Registrar e oficializar as ocorrências de desempenho, execução, prestação ou fornecimento, sendo estes considerados insatisfatórios, irregulares, falhas, insuficiências, erros e omissões constatados, durante o fornecimento do objeto, para as devidas providências pela **CONTRATADA**;

11.8. Consoante o artigo 45 da Lei nº 9.784, de 1999, a Administração Pública poderá, sem a prévia manifestação do interessado, motivadamente, adotar providências acauteladoras;

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

11.10. 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;

11.11. Comunicar à **CONTRATADA**, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;

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

12. CLÁUSULA DÉCIMA SEGUNDA - OBRIGAÇÕES DA CONTRATADA

12.1. Para o fornecimento do bem, a **CONTRATADA** obriga-se a cumprir fielmente o objeto, de forma que os produtos avençados mantenham a execução e condução deles nas condições e prazos estipulados;

12.2. A fiscalização, quando exercida por servidor designado para acompanhar a entrega dos produtos, não exime ou reduz a responsabilidade da **CONTRATADA** perante as obrigações aqui estabelecidas;

12.3. Manter, durante toda a execução do Termo de Contrato, compatibilidade com as obrigações assumidas e todas as condições de habilitação e qualificação exigidas na Lei nº 8.666, de 21 de junho de 1993 e suas alterações, para comprovação, sempre que necessário for, junto ao **CONTRATANTE**;

12.4. Não serão aceitos pela Administração quaisquer alegações por parte da empresa **CONTRATADA** quanto ao desconhecimento das condições descritas;

12.5. 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;*

12.6. A **CONTRATADA** não poderá, em hipótese alguma, inserir posteriormente qualquer tipo de insumo, taxa, cobrança adicional ou qualquer outro congênere que não esteja inicialmente previsto no instrumento de convocação ou em sua proposta;

12.7. Todas as despesas de impostos, fretes, seguros, taxas e outros custos que recaiam sobre a prestação dos serviços ou entrega dos bens, serão suportados única e exclusivamente pela **CONTRATADA**;

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

12.9. Comunicar ao **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;

12.10. Qualquer anormalidade no fornecimento será de responsabilidade única e exclusiva da **CONTRATADA;**

12.11. No caso de pedido de suspensão do fornecimento solicitado exclusivamente pela **CONTRATANTE**, a **CONTRATADA** deverá imediatamente suspendê-los até segunda ordem;

12.12. Indicar formalmente preposto apto a representá-la junto à contratante, que deverá responder pela fiel execução do contrato;

12.13. Atender prontamente quaisquer orientações e exigências do fiscal do contrato, inerentes à execução do objeto contratual;

12.14. Reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante;

12.15. Propiciar todos os meios e facilidades necessárias à fiscalização da Solução de Tecnologia da Informação pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcialmente, em qualquer tempo, sempre que considerar a medida necessária;

12.16. Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

12.17. Quando especificada, manter, durante a execução do Contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da Solução de Tecnologia da Informação;

12.18. Manter a produtividade ou a capacidade mínima de fornecimento da Solução de Tecnologia da Informação durante a execução do contrato;

12.19. Fornecer, sempre que solicitado, amostra para realização de Prova de Conceito para fins de comprovação de atendimento das especificações técnicas; e

12.20. Submeter-se à fiscalização do **CONTRATANTE**, no tocante à prestação dos serviços, prestando esclarecimentos solicitados e atendendo imediatamente qualquer reclamação, caso venham a ocorrer;

12.21. Prestar as atividades objeto da licitação, utilizando de mão de obra qualificada e devidamente especializada, necessária à completa e perfeita execução dos serviços, em conformidade com as especificações deste Contrato;

12.22. Responsabilizar-se por todos os ônus referentes aos serviços objeto deste Contrato inclusive salários de pessoal, alimentação, hospedagem e transporte, bem como tudo que as leis trabalhistas e previdenciárias preveem e demais exigências legais para o exercício da atividade objeto desta licitação.

12.23. Ter pleno conhecimento de todas as condições e peculiaridades inerentes aos serviços a serem executados não podendo invocar posteriormente desconhecimento para cobrança de pagamentos adicionais ao **CONTRATANTE** ou a não prestação satisfatória dos serviços.

12.24. Manter sigilo absoluto sobre todas as informações provenientes dos serviços realizados, documentos elaborados e informações obtidas reconhecendo serem estes de propriedade exclusiva do **CONTRATANTE**;

12.25. Substituir imediatamente, a critério do **CONTRATANTE**, a qualquer tempo, e sem nenhum ônus adicional, qualquer profissional do seu corpo técnico cuja presença seja considerada indesejável ou inconveniente, em virtude de comportamento inadequado.

12.26. Assumir inteira responsabilidade por quaisquer danos ou prejuízos causados por seus empregados ou por terceiros sob sua responsabilidade, por negligência, imprudência ou imperícia, não

se excluindo ou reduzindo essa responsabilidade em razão da fiscalização ou do acompanhamento realizado pelo **CONTRATANTE**.

12.27. Fornecer todos os documentos e manuais necessários para garantir o bom funcionamento, suporte e manutenção dos equipamentos e software fornecidos.

12.28. Refazer, sem ônus para o **CONTRATANTE**, dentro do prazo estabelecido, os serviços prestados que apresentem defeitos, erros, danos, falhas e/ou quaisquer outras irregularidades em razão de negligência, má execução, emprego de mão-de-obra e/ou ferramentas inadequadas.

12.29. Manter, durante o período de vigência do contrato, todas as condições que ensejaram a contratação, particularmente no que tange a regularidade fiscal, desempenho e capacidade técnica operativa;

12.30. Os profissionais disponibilizados pela **CONTRATADA** para a prestação dos serviços não terão nenhum vínculo empregatício com o **CONTRATANTE** e deverão estar identificados com crachá de identificação da mesma, estando sujeitos às normas internas de segurança do **CONTRATANTE**, inclusive àqueles referentes à identificação, trajes, trânsito e permanência em suas dependências;

12.31. Não ceder ou transferir a outra empresa, total ou parcialmente, os serviços contratados;

12.32. Responsabilizar-se por eventuais despesas de custeio com deslocamentos de técnicos da **CONTRATADA** ao local de instalação, bem como todas as despesas de transporte, diárias, seguro ou quaisquer outros custos envolvidos;

12.33. Submeter-se à Política de Segurança da Informação e Comunicações e demais normas de segurança vigentes no **CONTRATANTE** e abster-se de veicular publicidade ou qualquer outra informação acerca das atividades desempenhadas, sem prévia autorização do **CONTRATANTE**;

12.34. Providenciar a assinatura do Termo de Compromisso, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes no **CONTRATANTE**, pelo representante legal da CONTRATADA, conforme nº SEI 0249766;

12.35. Providenciar a assinatura do Termo de Ciência da Declaração de Manutenção de Sigilo e das Normas de Segurança vigentes no **CONTRATANTE**, por todos os empregados da contratada diretamente envolvidos na contratação, conforme nº SEI 0249766.

13. CLÁUSULA DÉCIMA TERCEIRA – ALTERAÇÃO SUBJETIVA

13.1. 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 Termo de Contrato, não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do Termo de Contrato.

14. CLÁUSULA DÉCIMA QUARTA – SUBCONTRATAÇÃO

14.1. Não será admitida a subcontratação do objeto licitatório.

15. CLÁUSULA DÉCIMA QUINTA - SANÇÕES ADMINISTRATIVAS

15.1. Pela inexecução total ou parcial das condições pactuadas, erros de execução, demora na entrega dos materiais, a Administração poderá, garantida a prévia defesa, aplicar à **CONTRATADA** as seguintes sanções, sem prejuízo da responsabilidade civil e criminal:

I - advertência;

II - multa (na forma do item 15.6 e 15.7);

III - suspensão temporária do direito de participar, por prazo não superior a **02 (dois) anos**, em licitação, e impedimento de contratar com o Órgão Sancionador;

IV - declaração de inidoneidade para licitar ou contratar com o Órgão Sancionador 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 Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior;

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

VI - 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 o **CONTRATANTE** pelos prejuízos causados.

15.2. As sanções aqui previstas são independentes entre si, podendo ser aplicadas isolada ou acumulativamente;

15.3. Caberá ainda ao fiscal o papel de notificar a empresa **CONTRATADA** quando da inexecução total ou parcial do objeto;

15.4. As sanções previstas de advertência, suspensão temporária e declaração de inidoneidade podem ser aplicadas juntamente com as sanções de multa, facultada a defesa prévia do interessado, no respectivo processo, no prazo de 05 (cinco) dias úteis;

15.5. A sanção de declaração de inidoneidade para licitar ou contratar é de competência exclusiva do Ministro de Estado, do Secretário Estadual ou Municipal, conforme o caso, facultada a defesa do interessado no respectivo processo, no prazo de 10 (dez) dias da abertura de vista, podendo a reabilitação ser requerida após 2 (dois) anos de sua aplicação;

15.6. Segue abaixo quadro contendo os graus de correspondência nos casos de multa e advertência:

Grau	**Correspondência**
1	Advertência por ocorrência
2	0,1% do valor mensal do contrato, por ocorrência e até o 30º dia
3	0,2% do valor mensal do contrato, por ocorrência e até o 30º dia
4	0,1% do valor do contrato, até o 30º dia
5	0,2% do valor do contrato, após o 31º dia, licitado a 10% do valor total do contrato

15.7. Abaixo consta a relação das inexecuções totais ou parciais:

Item	Descrição	Sanções aplicáveis por grau e por reincidência						
		1	2	3	4	5	6	7
1	Atrasar o fornecimento.	1 vez	-	-	1 vez até o 10º dia	-	-	1 vez a partir do 11º dia
2	Fornecer os bens em embalagens dessemelhantes as especificadas no edital, contrato ou pelo fabricante.	1 vez	-	1 vez	-	-	1 vez	1 vez
3	Entregar os bens fora do prazo estipulado.	2 vezes	-	-	1 vez até o 10º dia	-	-	1 vez a partir do 11º dia
4	Entregar os bens em locais diferentes dos estipulados.	1 vez	-	1 vez	-	1 vez	-	1 vez
5	Atrasar injustificadamente a entrega dos bens.	1 vez	-	1 vez	-	1 vez	-	1 vez
6	Entregar os bens em quantidades diferentes da estipulada no edital, contrato, ata ou nota de empenho.	1 vez	-	1 vez	-	-	1 vez	1 vez
7	Entregar os bens com defeitos, avarias ou qualquer outro dano por manipulação incorreta ou falta de zelo.	1 vez	-	-	-	-	1 vez	1 vez
8	Transportar os bens de forma inadequada.	1 vez	-	-	-	-	1 vez	1 vez
9	Não fornecer o objeto na forma estipulada no contrato.	3 vezes	-	-	1 vez	1 vez	-	1 vez

15.8. Se a multa aplicada for superior ao valor da garantia prestada, além da perda desta, responderá a **CONTRATADA** pela sua diferença, que será descontada dos pagamentos eventualmente devidos pela Administração ou cobrada judicialmente;

15.9. As penalidades serão obrigatoriamente registradas no SICAF e, no caso de suspensão de licitar, a **CONTRATADA** deverá ser descredenciada por igual período, sem prejuízo das multas previstas no Termo de Contrato e seus Anexos e demais cominações legais;

15.10. Se o motivo ocorrer por comprovado impedimento ou por motivo de força maior, devidamente justificado e aceito pela Administração do **CONTRATANTE**, a **CONTRATADA** ficará isenta das penalidades mencionadas;

15.11. Aplicar-se-á advertência por faltas consideradas leves, assim entendidas como aquelas que não acarretarem prejuízos significativos ao objeto da contratação;

15.12. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa;

15.13. 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;

15.14. Caso o **CONTRATANTE** determine, a multa deverá ser recolhida no prazo máximo de 10 (dez) dias, a contar da data do recebimento da comunicação enviada pela **CONTRATADA**.

16. CLÁUSULA DÉCIMA SEXTA - RESCISÃO

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

16.2. Os casos omissos de rescisão contratual serão formalmente motivados nos autos do processo, assegurado o contraditório e a ampla defesa;

16.3. A rescisão administrativa ou amigável será precedida de autorização escrita e fundamentada da autoridade competente;

16.4. A rescisão determinada por ato unilateral e escrita pela Administração, nos casos enumerados nos Incisos I a XI do Art. 78, da Lei nº 8.666/93, acarreta as consequências previstas nos Incisos II e IV do Art. 87, do mesmo diploma legal, sem prejuízo das demais sanções previstas; nos casos previstos nos Incisos XII a XVII do Art. 78, será observado o disposto no § 2º do Art. 79;

16.5. Na hipótese de se concretizar a rescisão contratual, poderá o **CONTRATANTE** contratar os serviços das licitantes classificadas em colocação subsequente, observadas as disposições dos Incisos XI do Art. 24, da Lei nº 8.666/93 ou efetuar nova licitação;

16.6. O termo de rescisão será precedido de relatório indicativo dos seguintes aspectos, conforme o caso:

16.6.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

16.6.2. Relação dos pagamentos já efetuados e ainda devidos;

16.6.3. Indenizações e multas.

17. CLÁUSULA DÉCIMA SÉTIMA – ALTERAÇÕES PREVISTAS

17.1. O compromisso firmado pode ser alterado nos casos previstos no Art. 65 da Lei nº 8.666, de 21 de junho de 1993.

18. **CLÁUSULA DÉCIMA OITAVA – CRITÉRIOS DE SUSTENTABILIDADE AMBIENTAL**

18.1. Decreto nº 99.658/90: Regulamenta no âmbito da Administração Pública Federal, o reaproveitamento, a movimentação, a alienação e outras formas de desfazimento de material;

18.2. Decreto nº 6.087/07: Altera os arts. 5º, 15º e 21º do Decreto nº 99.658, de 30 de outubro de 1990, que regulamenta, no âmbito da Administração Pública Federal, o reaproveitamento, a movimentação, a alienação e outras formas de desfazimento de material, e dá outras providências; e

18.3. Instrução Normativa SLTI/MP nº 01/2010: Dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional e dá outras providências.

19. **CLÁUSULA DÉCIMA NONA - CASOS OMISSOS**

19.1. 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.

20. **CLÁUSULA VIGÉSIMA - PUBLICAÇÃO**

20.1. O resumo deste Termo de Contrato será encaminhado até o 5° (quinto) dia útil do mês subseqüente ao de sua assinatura, para publicação no Diário Oficial da União, consoante dispõe o Art. 61, Parágrafo Único da Lei n.° 8.666/93.

21. **CLÁUSULA VIGÉSIMA PRIMEIRA - FORO**

21.1. As partes, em comum acordo, elegem o foro de Brasília/DF, para dirimir as dúvidas oriundas da execução do presente Termo de Contrato, renunciando a qualquer outro por mais privilegiado que seja.

E, por assim estarem justas e acertadas, foi lavrado o presente **CONTRATO** e disponibilizado por meio eletrônico através do Sistema Eletrônico de Informações – SEI, conforme RESOLUÇÃO CADE N° II, DE 24 DE NOVEMBRO DE 2014, publicada no D.O.U. Seção 1, no dia 02 de dezembro de 2014, o qual, depois de lido e achado conforme, vai assinado pelas partes, perante duas testemunhas a tudo presentes.

Documento assinado eletronicamente por **Leonardo Garcia Rocha**, **Usuário Externo**, em 29/11/2016, às 16:58, conforme horário oficial de Brasília e Resolução Cade nº 11, de 02 de dezembro de 2014.

Documento assinado eletronicamente por **Luana Nunes Santana**, **Coordenador(a)-Geral**, em 30/11/2016, às 16:12, conforme horário oficial de Brasília e Resolução Cade nº 11, de 02 de dezembro de 2014.

Documento assinado eletronicamente por **Isaque Moura da Silva**, **Testemunha**, em 30/11/2016, às 16:26, conforme horário oficial de Brasília e Resolução Cade nº 11, de 02 de dezembro de 2014.

Documento assinado eletronicamente por **Marilucy Silva Lima**, **Testemunha**, em 30/11/2016, às 17:09, conforme horário oficial de Brasília e Resolução Cade nº 11, de 02 de dezembro de 2014.

A autenticidade deste documento pode ser conferida no site http://sei.cade.gov.br /sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0272253** e o código CRC **F5D9128F**.

Referência: Processo nº 08700.001206/2016-47 SEI nº 0272253