Governo do Estado do Rio de Janeiro
Secretaria de Estado de Ciência, Tecnologia e Inovação
Fundação Centro de Ciências e de Educação Superior a Distância do Estado do Rio de Janeiro

MINUTA DO TERMO DE REFERÊNCIA

1. PROPÓSITO

O presente Termo de Referência tem por objetivo descrever a contratação de Licenças para uso de software corporativo antivírus, em conformidade com a Lei nº 8.666/1993 (Regulamenta o art. 37, inciso XXI, da Constituição Federal, que institui normas para licitações e Contratos da Administração Pública e dá outras providências) e o Decreto Estadual nº 46.642/2019 (Regulamenta a fase preparatória das contratações no âmbito do Estado do Rio de Janeiro).

1.1 Justificativa da contratação

A FUNDAÇÃO CECIERJ, através da Diretoria de Suporte Técnico em Informática - DEPSTI, busca a cada dia melhorar a sua rede de processamento e dados com o objetivo de dar mais celeridade nas atividades administrativas através da otimização de recursos que garantam a eficiência funcional dos equipamentos de informática, bem como a utilização de ferramentas que visem diminuir custos. Para tanto faz-se necessário a aquisição de software corporativo antivírus, que com tecnologias avançadas, visa proteger a rede corporativa contra os riscos e ameaças de vírus durante a execução das tarefas diárias, evitando, com isso, problemas como lentidão do sistema, perda de arquivos e exploração de informações sigilosas. Em virtude da introdução de novos equipamentos empregados nos processos de trabalho da Fundação nos últimos anos, o que resultou na expansão de sua rede corporativa, vislumbrou-se a necessidade de se adquirir uma tecnologia de maior porte para a corporação.

O software corporativo antivírus deve disponibilizar os seguintes recursos: emissão de relatórios sobre o grau de infecção, gerenciamento dos equipamentos com o mesmo software, centralização das atualizações a partir de único servidor, console de gerenciamento de estação de trabalho, interface

de fácil acesso, eficácia na remoção das infecções virtuais e recursos adicionais como teclado anti-fraude e mecanismo anti-phishing.

O uso de software de antivírus baseia-se na política de prevenção de riscos adotada pela DSTI, cuja finalidade visa monitorar e controlar o tráfego de dados que circula entre as redes internas e a Internet, garantindo, com isso, a segurança e o bom funcionamento dos computadores da rede corporativa local (Intranet) contra ameaças maliciosas de vírus que possam causar perda de arquivos e a exploração de informações sigilosas das atividades administrativas, de dados pessoais do efetivo e das ações estratégicas públicas desenvolvidas pela Fundação CECIERJ.

1.2 Instrumentos de planejamento

A aquisição do licenciamento do software de antivírus encontra-se alinhado ao Plano Anual de Contratações dentro do escopo do projeto de manutenção do parque tecnológico da Fundação CECIERJ.

As despesas decorrentes da presente licitação correrão à conta do orçamento próprio da Fundação CECIERJ e que já estão alocadas no orçamento da Fundação CECIERJ para o exercício de 2021.

1.3 Objetivo da contratação

Tal investimento é necessário a fim de atender os seguintes resultados:

- remoção das infecções virtuais;
- gerenciamento dos equipamentos com o mesmo software;
- centralização das atualizações a partir de único servidor;
- console de gerenciamento de estação de trabalho;
- interface de fácil acesso e emissão de relatórios sobre o grau de infecção;
- recursos anti-fraude;
- mecanismo anti-phishing;
- monitorar e controlar o tráfego de dados que circula entre as redes internas e a Internet.

2. DESCRIÇÃO DO OBJETO

2.1 Definição sucinta do Objeto

O objeto a ser fornecido deverá atender às seguintes especificações técnicas mínimas, de acordo com os padrões de mercado, visando não restringir a competitividade e nem atrelar a marca específica.

- Servidor de Administração e Console Administrativa:
- Compatibilidade:
- Microsoft Windows Server 2008 (x86/x64) ou superior;
- Microsoft Windows Server 2008 Core;
- Microsoft Windows Server 2008 R2 (x86/x64) ou superior;
- Microsoft Windows Server 2008 R2 Core;
- Microsoft Windows Server 2012;
- Microsoft Windows Small Business Server 2003 SP2;
- Microsoft Windows Small Business Server 2008;
- Microsoft Windows Small Business Server 2011;
- Características:
- A console deve ser acessado via WEB (HTTPS) ou MMC;
- Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;
- Capacidade de remover remotamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;
- Capacidade de remover remotamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;
- 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;
- Capacidade de instalar remotamente a solução de segurança em smartphones e tablets Symbian, Windows Mobile, BlackBerry e Android, utilizando estações como intermediadoras;
- Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS;
- Capacidade de instalar remotamente qualquer “app” em smartphones e tablets de sistema iOS;
- Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;
- Capacidade de gerenciar smartphones e tablets (tanto Symbian quanto Windows Mobile, BlackBerry, Android e iOS) protegidos pela solução antivírus;
- Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;
- Capacidade de atualizar os pacotes de instalação com as últimas vacinas, haja vista quando o pacote for utilizado em uma instalação, já contenha as vacinas mais recentes; Capacidade de fazer

distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;

- Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;
- Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;
- Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas a proteção;
- Capacidade de monitorar 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;
- 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;
- 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;
- Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;
- Deve fornecer as seguintes informações dos computadores:
- Se o antivírus está instalado;
- Se o antivírus está iniciado;
- Se o antivírus está atualizado;
- Minutos/horas desde a última conexão da máquina com o servidor administrativo;
- Minutos/horas desde a última atualização de vacinas;
- Data e horário da última verificação executada na máquina;
- Versão do antivírus instalado na máquina;
- Se é necessário reiniciar o computador para aplicar mudanças;
- Data e horário de quando a máquina foi ligada;
- Quantidade de vírus encontrados (contador) na máquina;
- Nome do computador;
- Domínio ou grupo de trabalho do computador;
- Data e horário da última atualização de vacinas;
- Sistema operacional com Service Pack;
- Quantidade de processadores;
- Quantidade de processadores; Quantidade de memória RAM;
- Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);

- Endereço IP;
- Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;
- Atualizações do Windows Update instaladas;
- Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;
- Vulnerabilidades de aplicativos instalados na máquina;
- Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
- Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como: Mudança de gateway; Mudança de subnet DNS; Mudança de domínio; Mudança de servidor DHCP; Mudança de servidor DNS; Mudança de servidor WINS; Aparecimento de nova subnet;
- Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
- Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
- Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
- Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
- 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;
- 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;
- Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;
- Capacidade de gerar traps SNMP para monitoramento de eventos;
- Capacidade de enviar e-mails para contas específicas em caso de algum evento;
- Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;
- Deve possuir compatibilidade com Cisco Network Admission Control (NAC);

- Deve possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por exemplo);
- 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;
- Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
- Capacidade de realizar atualização incremental de vacinas nos computadores clientes;
- Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;
- Capacidade de realizar inventário de hardware de todas as máquinas clientes;
- Capacidade de realizar inventário de aplicativos de todas as máquinas clientes;
- Capacidade de diferenciar máquinas virtuais de máquinas físicas.
- Estações Windows
- Compatibilidade:
- Microsoft Windows Embedded POSReady 7 (x86/x64);
- Microsoft Windows Embedded Standard 7 (x86/x64) SP1;
- Microsoft Windows XP Professional (x86/x64) SP2 ou superior;
- Microsoft Windows Vista (x86/x64) SP2 ou superior;
- Microsoft Windows 7 (x86/x64) ou superior;
- Microsoft Windows 8 Pro/Enterprise (x86/x64);
- Microsoft Windows 8.1 Enterprise (x86/x64).
- Microsoft Windows 10 Pro/Enterprise (x86/x64);
- Características:
- Deve prover as seguintes proteções:
- Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
- Antivírus de Web (módulo para verificação de sites e downloads contra vírus);
- Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
- Antivírus de Mensagens Instantâneas (módulo para verificação de mensagens como ICQ, MSN, IRC, etc);
- Firewall com IDS;
- Autoproteção contra ataques aos serviços/processos do antivírus;
- Controle de dispositivos externos, com capacidade de bloqueio de dispositivos USB, FireWire, bluetooth e outros;
- Controle de acesso a sites por categoria;

- Controle de execução de aplicativos, com capacidade de criação de regras definindo quais aplicativos podem ou não podem ser executados pelos usuários;
- Controle de vulnerabilidades do Windows e dos aplicativos instalados;
- Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
- 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);
- Capacidade de automaticamente desabilitar o Firewall do Windows (caso exista) durante a instalação, para evitar incompatibilidade com o Firewall da solução;
- Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
- 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;
- 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;
- Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
- Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- 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;
- Capacidade de verificar somente arquivos novos e alterados;
- Capacidade de verificar objetos usando heurística;
- Capacidade de agendar uma pausa na verificação;
- Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
- O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve: Perguntar o que fazer, ou, bloquear acesso ao objeto;
- Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré- estabelecida pelo administrador); Caso positivo de desinfecção: Restaurar o objeto para uso; Caso negativo de desinfecção: Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador); Anteriormente a qualquer tentativa

de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

- 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);
- Capacidade de verificar tráfego de ICQ, MSN, AIM e IRC contra vírus e links phishings;
- Capacidade de verificar links inseridos em e-mails contra phishings;
- Capacidade de verificar tráfego SSL nos browsers: Internet Explorer, Firefox e Opera;
- Capacidade de verificação de corpo e anexos de e-mails usando heurística;
- O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve: Perguntar o que fazer, ou Bloquear o e-mail, apagar o objeto ou tentar desinfectá- lo (de acordo com a configuração pré-estabelecida pelo administrador); Caso positivo de desinfecção: Restaurar o e-mail para o usuário;Caso negativo de desinfecção: Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);
- Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;
- Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;
- Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;
- Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (Java Script, Visual Basic Script, etc), usando heurísticas;
- Deve ter suporte total ao protocolo Ipv6;
- Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;
- Na verificação de tráfego web, caso encontrado código malicioso o programa deve: Perguntar o que fazer, bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio e permitir acesso ao objeto;
- O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador: Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo real, verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação;
- Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;
- 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;

- Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;
- 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;
- Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://www.antiphishing.org/);
- Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;
- 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;
- O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras: Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas; 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;
- Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo: Discos de armazenamento locais, armazenamento removível, impressoras, CD/DVD, drives de disquete, modems, dispositivos de fita, dispositivos multifuncionais, leitores de smart card, dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc), wi-Fi, adaptadores de rede externos, dispositivos MP3 ou smartphones, dispositivos Bluetooth;
- 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;
- Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;
- Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;
- Capacidade de configurar novos dispositivos por Class ID / Hardware ID;
- 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;

- 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);
- Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
- 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;
- 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.
- Estações e Servidores Mac OS X;
- Compatibilidade:
- Mac OS X; Mac OS X Server.
- Características:
- Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
- Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
- 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;
- Deve possuir suportes a notificações utilizando o Growl;
- 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);
- Capacidade de voltar para a base de dados de vacina anterior;
- Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;
- 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;
- Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
- 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;
- Capacidade de verificar somente arquivos novos e alterados;
- Capacidade de verificar objetos usando heurística;

- Capacidade de agendar uma pausa na verificação;
- O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve: Perguntar o que fazer, ou, bloquear acesso ao objeto, apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador); Caso positivo de desinfecção: Restaurar o objeto para uso; Caso negativo de desinfecção: Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
- Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
- Capacidade de verificar arquivos de formato de e-mail;
- 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;
- Capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento.
- Estações de trabalho Linux
- Compatibilidade:
- Plataforma 32-bits: Red Hat Enterprise Linux Desktop; Red Hat Enterprise Linux Desktop; CentOS; Debian GNU/Linux; Ubuntu LTS;
- Plataforma 64-bits: Red Hat Enterprise Linux Desktop; Red Hat Enterprise Linux Desktop; CentOS; Debian GNU/Linux; Ubuntu LTS.
- Características:
- Deve prover as seguintes proteções: Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado; As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
- Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções: Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas); 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; Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena; Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados;
- Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;

- Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- 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;
- Capacidade de verificar objetos usando heurística;
- Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
- Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
- Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).
- Servidores Windows
- Compatibilidade:
- Microsoft Windows Essential Business Server 2008 Std/Premium;
- Microsoft Windows MultiPoint Server 2011 x64;
- Microsoft Windows Small Business Server 2008 Std/Premium x64;
- Microsoft Windows Small Business Server 2011 Essentials/Std x64;
- Microsoft Windows Server 2003 Std/Ent SP2 x86/x64;
- Microsoft Windows Server 2003 R2 Std/Ent SP2 x86/x64;
- Microsoft Windows Server 2008 Core Std/Ent/Dc SP1 x86/x64;
- Microsoft Windows Server 2008 R2 Std/Ent/Dc SP1;
- Microsoft Windows Server 2008 R2 Core Std/Ent/Dc SP1;
- Microsoft Windows Server 2012 Foundation/Essentials/Std x64;
- Microsoft Windows Server 2012 R2 Standard x64;
- Microsoft Windows Hyper-V Server 2008 R2 SP1;
- Microsoft Terminal baseado em Windows Server 2003;
- Microsoft Terminal baseado em Windows Server 2008;
- Microsoft Terminal baseado em Windows Server 2008 R2;
- Microsoft Windows Server edições atualizadas;
- Citrix Presentation Server;
- Citrix XenApp.
- Características:
- Deve prover as seguintes proteções: Antivírus de Arquivos residente (anti spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado; Autoproteção contra ataques aos serviços/processos do antivírus; Firewall com IDS; Controle de vulnerabilidades do Windows e dos aplicativos instalados;
- Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
- As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

- Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções: Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas); Gerenciamento de tarefa (criar ou excluir tarefas de verificação); Leitura de configurações; Modificação de configurações; Gerenciamento de Backup e Quarentena; Visualização de relatórios; Gerenciamento de relatórios; Gerenciamento de chaves de licença; Gerenciamento de permissões (adicionar/excluir permissões acima);
- O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras: Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas; 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.;
- 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;
- Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc);
- Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS);
- Em caso erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;
- Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;
- Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;
- Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;
- Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
- 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;
- Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

- 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;
- Capacidade de verificar somente arquivos novos e alterados;
- Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto-descompressores, PST, arquivos compactados por compactadores binários, etc);
- Capacidade de verificar objetos usando heurística;
- Capacidade de configurar diferentes ações para diferentes tipos de ameaças;
- Capacidade de agendar uma pausa na verificação;
- Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
- O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve: Perguntar o que fazer, ou, bloquear acesso ao objeto; apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador); Caso positivo de desinfecção: Restaurar o objeto para uso; Caso negativo de desinfecção: Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
- Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
- Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
- Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
- Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.
- Servidores Linux
- Compatibilidade:
- Plataforma 32-bits: Red Hat Enterprise Linux Server; CentOS; Ubuntu Server LTS; Debian GNU/Linux;
- Plataforma 64-bits: Red Hat Enterprise Linux Server; CentOS; Ubuntu Server LTS; Debian GNU/Linux;
- Características:
- Deve prover as seguintes proteções: Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado; As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
- Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções: Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas); 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; Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena; Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados;

- Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;
- Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- 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;
- Capacidade de verificar objetos usando heurística;
- Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
- Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
- Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).
- Smartphones e tablets
- Compatibilidade:
- Apple iOS; Symbian OS; Windows Mobile; BlackBerry; Android OS.
- Características:
- Deve prover as seguintes proteções:
- Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de: 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; Arquivos abertos no smartphone; Programas instalados usando a interface do smartphone; Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;
- Deverá isolar em área de quarentena os arquivos infectados;
- Deverá atualizar as bases de vacinas de modo agendado;
- Deverá bloquear spams de SMS através de Blacklists;
- Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado;
- Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;
- Deverá ter firewall pessoal;

- Possibilidade de instalação remota utilizando o Microsoft System Center Mobile Device Manager;
- Possibilidade de instalação remota utilizando o Sybase Afaria;
- Capacidade de detectar Jailbreak em dispositivos iOS;
- Capacidade de bloquear o acesso a site por categoria em dispositivos;
- Capacidade de bloquear o acesso a sites phishing ou malicioso;
- Capacidade de criar containers de aplicativos, separando dados corporativos de dados pessoais;
- Capacidade de configurar White e black list de aplicativos.
- Gerenciamento de dispositivos móveis (MDM):
- Compatibilidade:
- Dispositivos conectados através do Microsoft Exchange ActiveSync: Apple iOS; Symbian OS; Windows Mobile e Windows Phone; Android; Palm WebOS;
- Dispositivos com suporte ao Apple Push Notification (APNs) servisse: Apple iOS 3.0 ou superior.
- Características:
- Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;
- Capacidade de ajustar as configurações de: Sincronização de e-mail; Uso de aplicativos; Senha do usuário; Criptografia de dados; Conexão de mídia removível;
- Capacidade de instalar certificados digitais em dispositivos móveis;
- Capacidade de, remotamente, resetar a senha de dispositivos iOS;
- Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;
- Capacidade de, remotamente, bloquear um dispositivo iOS.

2.2 Identificação dos itens, quantidades e unidades.

DESCRIÇÃO	UNIDADE	QUANTIDADE
LICENÇA PARA USO DE SOFTWARE DE ANTIVÍRUS: Linguagem: português do Brasil; Recursos inclusos: Antimalware; Firewall; Proteção assistida em nuvem; Controle de aplicativos; Lista branca de aplicativos; Monitoramento e controle de acesso à internet (WEB); Gerenciamento e controle de dispositivos móveis para acesso da rede corporativa; Proteção de servidores de arquivos em plataformas Windows, Linux ou FreeBSB; Segurança de endpoints móveis (tablets e smartphones); Dados corporativos e pessoais	UNIDADE	500

separados e armazenados em contêineres criptografados; Centralização do gerenciamento das tarefas a partir de 01 (um) console; Todas as licenças terão validade de 01 (um) ano de atualizações.		

2.3 Informações complementares

O item deve obrigatoriamente possuir as características descritas anteriormente.

2.4 Definição da natureza do serviço

A aquisição atende a classificação de natureza de bem comum, cujos padrões de desempenho e de qualidade serão objetivamente definidos pelo ato convocatório, por meio de especificações usuais do mercado, independentemente de sua complexidade.

3. DESCRIÇÃO DA SOLUÇÃO

3.1 Forma de execução

A forma de pagamento será em uma única parcela a ser paga após aceitação definitiva do bem adquirido. O processo de pagamento obedecerá todos os procedimentos formais existentes no Estado.

O prazo de disponibilização dos produtos e início da prestação dos serviços contratados será de até 30 (trinta) dias úteis, a contar da data da formalização contratual, do recebimento da Nota de Empenho ou da autorização de fornecimento pelos Órgãos Participantes.

A fiscalização da contratação será exercida por um representante da Administração, ao qual competirá dirimir as dúvidas que surgirem no curso da execução do contrato, e de tudo dará ciência à Administração.

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

O fiscal do contrato 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 faltas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis, em conformidade com os termos do art. 67 da Lei nº 8.666, de 1993.

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.

3.2 Duração do contrato

A Contratada deve cumprir todas as obrigações constantes no Termo de Referência/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:

- Efetuar a entrega do objeto/ Realizar a prestação dos serviços em perfeitas condições, conforme especificações, prazo e local constantes no Termo de Referência/Edital, seus anexos, acompanhado da respectiva nota fiscal;
- Entregar, quando for o caso, o manual do usuário, com uma versão em Português e da relação da rede de assistência técnica autorizada;
- 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);
- Substituir, reparar ou repor o objeto ou parte dele considerado defeituoso, ou rejeitado pelo gestor desta contratação e/ou que venha a apresentar defeitos graves de fabricação ou ainda que tenha sido danificado

3.3 Reajuste de preços

O projeto não contempla esta natureza por se tratar de aquisição de bem comum por meio de pregão eletrônico.

3.4 Garantia

A garantia deve contemplar o período da validade das licenças.

3.5 Critérios e práticas de sustentabilidade

Quanto às práticas de sustentabilidade, visto que a contratação se refere apenas a prestação de serviço técnico especializado à mesma não se aplica. Dessa forma, não há necessidade de atender a LEI Nº 12.305, DE 2 DE AGOSTO DE 2010, a qual regula os requisitos de sustentabilidade das compras públicas.

Quanto às práticas de sociabilidade, durante a execução de tarefas no ambiente da Fundação CECIERJ ou das demais instituições públicas envolvidas, os funcionários da empresa fornecedora deverão observar, no trato com os servidores e o público em geral, a urbanidade e os bons costumes de comportamento, tais como: asseio, pontualidade, cooperação, respeito mútuo, discrição e zelo com o patrimônio público. Deverão ainda portar identificação pessoal, de acordo com as normas internas das instituições.

3.6 Possibilidade de subcontratação

Atendendo aos art. 72 e art. 78, inciso VI da Lei Federal 8666/93, os integrantes deste estudo técnico preliminar entendem que não haverá a possibilidade de subcontratação de parte do objeto contratado.

3.7 Possibilidade de participação de Consórcio

Os integrantes deste estudo técnico preliminar não fazem indicações e/ou apontam quaisquer impedimentos quanto a possibilidade de participação de consórcios pois entendem que as variáveis que justificam ou não a possibilidade de participação de consórcio são a complexidade do objeto, abrangência dos serviços, valor final da contratação, necessidade multidisciplinar do objeto não encontrado facilmente no mercado, fomento do mercado e competitividade no certame.

Quanto às questões técnicas do projeto, a equipe técnica responsável pela elaboração deste documento entende que não nos cabe definir a possibilidade. Entendemos que o mesmo deve ser definido pelos departamentos de contratos e jurídico da Fundação CECIERJ de forma conjunta.

3.8 Possibilidade de participação de Cooperativa

Os integrantes deste estudo técnico preliminar não fazem indicações e/ou apontam quaisquer impedimentos quanto à possibilidade de participação de cooperativas pois entendem que, de acordo com a orientação administrativa PGE n.º 08 , as vedações de participação de cooperativas não cabem neste processo.

No entanto, não nos cabe definir o regime. Entendemos que o mesmo deve ser definido pelos departamentos de contratos e jurídico da Fundação CECIERJ de forma conjunta.

3.9 Responsabilidades das partes

3.9.1 Responsabilidades da contratante

Receber o objeto no prazo e condições estabelecidas neste Termo de Referência (ou no Edital e seus anexos) e ainda:

a. Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos/ serviços prestados provisoriamente com as especificações constantes deste Termo de Referência/Edital e da proposta, para fins de aceitação e recebimento definitivo;

b. Comunicar à Contratada, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido/serviço prestado, para que seja substituído, reparado ou corrigido;

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

d. Efetuar o pagamento à Contratada no valor correspondente ao fornecimento do objeto/prestação do serviço, no prazo e forma estabelecidos neste termo de referência.

e. Fornecer à CONTRATADA a relação de servidores e unidades autorizadas a acompanhar e fiscalizar a execução do contrato e atestar os relatórios de visita, quando necessário.

f. A Administração não responderá por quaisquer compromissos assumidos pela Contratada com terceiros, ainda que vinculados à execução do objeto do fornecimento/serviço, bem como por qualquer dano causado a terceiros em decorrência de ato da Contratada, de seus empregados, prepostos ou subordinados.

g. Fornecer à CONTRATADA os documentos, informações e demais elementos que possuir ligados ao presente Contrato.

h. Notificar, por escrito, a CONTRATADA da aplicação de eventuais penalidades, garantindo-lhe o direito ao contraditório e a ampla defesa.

3.9.2 Responsabilidades da contratada

A Contratada deve cumprir todas as obrigações constantes no Termo de Referência/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:

- Efetuar a entrega do objeto/ Realizar a prestação dos serviços em perfeitas condições, conforme especificações, prazo e local constantes no Termo de Referência/Edital, seus anexos, acompanhado da respectiva nota fiscal;
- Entregar, quando for o caso, o manual do usuário, com uma versão em Português e da relação da rede de assistência técnica autorizada;
- 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);
- Substituir, reparar ou repor o objeto ou parte dele considerado defeituoso, ou rejeitado pelo gestor desta contratação e/ou que venha a apresentar defeitos graves de fabricação ou ainda que tenha sido danificado

4. REQUISITOS MÍNIMOS PARA EXECUÇÃO

4.1 Qualificação Técnica

A licitante, juntamente com os documentos de habilitação, deverá apresentar como qualificação técnica, os seguintes documentos:

a. Apresentar comprovação de aptidão para desempenho de atividade pertinente e compatível com as características, quantidades e prazos do objeto da licitação, através da apresentação de no mínimo 01 (um) atestado de desempenho anterior, fornecido por pessoa jurídica de direito público ou privado, comprobatório da capacidade técnica para atendimento ao objeto da presente licitação, com indicação da quantidade fornecida, da qualidade do material, do atendimento, do cumprimento de prazos e demais condições do fornecimento.

b. Para comprovação do quantitativo fornecido, poderão ser apresentados tantos atestados quanto necessários para comprovar que todo o quantitativo indicado na cláusula anterior já tenha sido fornecido pela licitante.

4.2 Autorizações e Licenças Necessárias para a Execução do Objeto

Para aquisições e contratações na área de tecnologia da informação e comunicação, se faz necessário o envio de informações para análise técnica das Subsecretaria de Tecnologia da Informação e Comunicação da Secretaria de Estado da Casa Civil e Governança, conforme decreto nº 46.631/19.

Também se faz necessária a análise de instrução normativa nº 1 de 2019 que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

5. GESTÃO E FISCALIZAÇÃO DO CONTRATO

5.1 Agentes que participarão da gestão do contrato

Os servidores que participarão da fiscalização do contrato a ser celebrado:

Maximiano C Martins – ID 51159546

Bruno Pereira – ID 43361170

5.2 Mecanismos de comunicação a serem estabelecidos

Os mecanismos de comunicação formal a serem estabelecidos entre o Contratante e o Contratado serão por meio de telefone, e-mail, forma escrita e reuniões com realização de ata e assinatura de todos os participantes.

5.3 Critérios de medição por Acordo de Nível de Serviço

É o ato de receber, verificar e confirmar o produto/serviço fornecido pelo contratado. O recebimento do objeto contratual deverá ser feito em duas etapas, Provisória e Definitiva, consistindo da efetiva aceitação do objeto pela administração, conforme art. 73, inciso I da Lei Federal 8.666/93.

O recebimento provisório poderá ser dispensado nos casos previstos no art. 74 da Lei nº 8.666/1993:

“Art. 74. Poderá ser dispensado o recebimento provisório nos seguintes casos:

I - gêneros perecíveis e alimentação preparada;

II - serviços profissionais;

III - obras e serviços de valor até o previsto no art. 23, inciso II, alínea "a", desta Lei, desde que não se componham de aparelhos, equipamentos e instalações sujeitos à verificação de funcionamento e produtividade.

Parágrafo único. Nos casos deste artigo, o recebimento será feito mediante recibo.”

O recebimento provisório ficará a cargo dos Fiscais e o recebimento definitivo, a cargo do servidor ou comissão designada pela autoridade competente.

Definir o método de avaliação da conformidade do objeto entregue com relação às especificações técnicas e com a proposta da contratada, com vistas ao recebimento provisório.

Definir o método de avaliação da conformidade dos produtos e dos serviços entregues com relação aos termos contratuais e com a proposta da contratada, com vistas ao recebimento definitivo;

Definir uma lista de verificação para os recebimentos provisório e definitivo, a serem usadas durante a fiscalização do contrato, se for o caso.

5.4 Pagamento

A forma de pagamento será em uma única parcela a ser paga após aceitação definitiva do bem adquirido. O processo de pagamento obedecerá todos os procedimentos formais existent

6. OBRIGAÇÕES FUTURAS

6.1 Garantia técnica

A garantia técnica tem por finalidade assegurar “a integridade de um produto vendido e/ou a boa qualidade ou durabilidade de um serviço prestado, e que obriga o fabricante a consertar ou substituir a mercadoria com defeito e o prestador de serviço a refazê-lo se insatisfatório”.

Conforme explicado no Acórdão nº. 2406/2015 – 2ª Câmara, do TCU, existem três tipos de garantia técnica:

“3. Em regra existem três tipos de garantia: a legal, a contratual e a estendida. Nesse sentido tem-se que a garantia legal não pode ser modificada nem restringida, é de 90 dias para bens duráveis, e abrange todos os componentes do bem adquirido. Quanto à garantia contratual, entende-se que é ofertada pelo fabricante após o decurso do prazo da garantia legal, é, portanto, um benefício inerente a cada fabricante e pode ser modificado. Sendo assim, exigir que o fabricante do equipamento de informática ofereça a garantia contratual à empresa licitante é, em síntese, condicionar que somente as empresas licitantes capazes de conseguir esse benefício participem do certame, haja vista que não há padronização expressa em normativo legal voltada para os fabricantes de equipamentos de informática, estabelecendo o prazo de cinco anos como garantia contratual. Nesse sentido, tem-se que somente as licitantes que venham a obter a possibilidade de contratar a garantia estendida junto aos fabricantes podem participar do certame, estando excluídas as demais que não lograram êxito junto aos fabricantes, sendo os mesmos ou não. Assim, o prazo mínimo de garantia a ser exigido deve ser o usual dos fabricantes, que geralmente compreende o período de doze meses a partir da data da aquisição. Portanto, a presente análise posiciona-se no sentido de que essa exigência restringe de forma irregular a competição, pois não encontra amparo legal para o objeto em tela”.

As garantias legal e contratual estão expressas, respectivamente, no art. 26 e no art. 50 do Código de Defesa do Consumidor (CDC). A garantia contratual é complementar à legal, sendo facultativa, e conferida mediante termo escrito.

Cabe ressaltar que o prazo de garantia técnica não integra o prazo de vigência do contrato. A vigência contratual extingue-se com a finalização da execução do objeto, ou seja, com o recebimento definitivo e o consequente pagamento. Já a garantia técnica permanece, mesmo com a entrega definitiva do objeto.

Destaca-se que a exigência de garantia maior que a prevista no CDC, provavelmente, terá impacto no preço do bem a ser adquirido.

6.2 Assistência técnica

Recomenda-se que sejam estabelecidos os seguintes parâmetros para a assistência técnica durante a vigência da garantia:

- a assistência técnica será gratuita durante todo o prazo de garantia;

- se as despesas com o envio do equipamento para reparo será custeada pelo contratado durante todo o prazo de garantia; e

- se a reposição de qualquer parte ou peça que apresente defeito durante o prazo de garantia será realizada sem custos para o contratante.

Cabe ressaltar que a exigência de assistência técnica gratuita por prazo superior ao prazo mínimo previsto no CDC provavelmente terá impacto no preço do bem a ser adquirido.

6.3 Rede credenciada de assistência técnica e distribuição de peças

Exige-se uma declaração ou qualquer outro meio de prova do contratado, indicando o nome das empresas - e seus endereços e telefones - que realizem serviços de assistência técnica autorizada pelo fabricante.

7. ASSINATURA DOS RESPONSÁVEIS PELA ELABORAÇÃO

Bruno Pereira – ID 43361170

Marcus V S Anjos – ID 4380097-1

Rio de Janeiro, 07 abril de 2021