TERMO DE REFERÊNCIA

REGISTRO DE PREÇO PARA PRESTAÇÃO DE SERVIÇOS DE ENTREGA, INSTALAÇÃO, CONFIGURAÇÃO, MIGRAÇÃO DE SOLUÇÃO CORPORATIVA DE SEGURANÇA PARA PROTEÇÃO DE ESTAÇOES DE TRABALHO, SERVIDORES, COM GERÊNCIA CENTRALIZADA E GARANTIA TÉCNICA, DE 24 (VINTE E QUATRO) MESES E TREINAMENTO.

Outubro de 2019

1. OBJETO

Registro de Preços para prestação de serviços de Entrega, Instalação, Configuração, Migração de solução corporativa de segurança para proteção de Estações de Trabalho e Servidores com Gerência Centralizada, com Garantia Técnica de 24 (vinte e quatro) meses e Treinamento, conforme descritos, caracterizados e especificados neste Termo de Referência.

2. DEFINIÇÕES

2.1. CONTRATANTE é a Empresa Municipal de Informática S.A. – IPLANRIO, solicitante do serviço e responsável pela efetivação da contratação.

2.2. CONTRATADA é a empresa executante dos serviços a serem contratados.

3. DESCRIÇÃO DOS PRODUTOS E SERVIÇOS

ITEM	DESCRIÇÃO	UNIDADE	QTD	
1	(1) Solução de Proteção para Estações de Trabalho e (2) Segurança para Proteção da camada de Servidores Virtuais e Físicos).	Cliente	31.000 (1)	380 (2)
2	Serviço de Instalação, Configuração e Migração (Proteção para Estações de Trabalho e Proteção da camada de Servidores Virtuais e Físicos).	Unidade	2	
3	Treinamento (Proteção para Estações de Trabalho e Proteção da camada de Servidores Virtuais e Físicos).	Unidade	2	

3.1. SOLUÇÃO DE PROTEÇÃO PARA ESTAÇÕES DE TRABALHO (ITEM 1)

A solução de proteção para as estações de trabalho deverá ser licenciada para **31.000 (trinta e um mil)** clientes e possuir as seguintes funcionalidades:

a) Proteção Anti-malware para Estações de Trabalho;

b) Proteção de rootkits e Ransomware;

c) Proteção de HIPS (Host IPS) e Host Firewall;

d) Controle de Aplicações;

3.1.1. Proteção Anti-malware para Estações de Trabalho Windows

3.1.1.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

- Windows 7 (x86/x64);
- Windows 8 e 8.1 (x86/x64);
- Windows 10 (x86/x64);

3.1.1.2. Deve disponibilizar evidências de varredura em todas as estações de trabalho, identificando as atualizações de sucesso e as ações de insucesso. Para garantir que os casos de insucesso sejam monitorados para tomada de ações pontuais;

3.1.1.3. Deve ser integrada ao Windows Security Center, quando utilizado plataforma Microsoft;

3.1.1.4. Deve possuir tecnologia de Machine Learning sendo capaz de detectar variantes de malwares desconhecidos por similaridade de código;

3.1.1.5. Deverá incluir módulo de monitoração de comportamento malicioso de aplicações de forma a bloqueá-las mesmo quando a assinatura não for reconhecida;

3.1.1.6. Deverá incluir regras específicas para detecção de Ransomware;

3.1.1.7. Deverá ter capacidade de detecção e remoção de todos os tipos de malwares, incluindo spyware, adware, grayware, cavalos de Tróia, fileless, dentre outros;

3.1.1.8. Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em:

3.1.1.9. Processos em execução em memória principal (RAM);

3.1.1.10. Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);

3.1.1.11. Arquivos compactados automaticamente em, pelo menos, nos seguintes formatos: zip, exe e Microsoft cab;

3.1.1.12. Arquivos recebidos por meio de programas de comunicação instantânea (MSN Messenger, Yahoo Messenger, Google talk, dentre outros).

3.1.1.13. Deve detectar e proteger em tempo real a estação de trabalho contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em linguagens tais como Javascript, vbscript/Activex;

3.1.1.14. Deve possuir detecção heurística de vírus desconhecidos;

3.1.1.15. Deve permitir configurações customizadas de proteção que permitam reduzir impactos no desempenho dos “scans”.

3.1.1.16. Deve permitir diferentes configurações de detecção (varredura ou rastreamento):

a) Em tempo real de arquivos acessados pelo usuário;

b) Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a necessidade de escrita de arquivo;

c) Manual, imediato ou programável, com interface gráfica em janelas, personalizável, com opção de limpeza;

d) Por linha-de-comando e parametrizável;

e) Automáticos do sistema com as seguintes opções:

f) Escopo: todos os discos locais, discos específicos, pastas específicas ou arquivos específicos;

g) Ação: somente alertas, limpar automaticamente, apagar automaticamente ou prover ação de quarentena;

h) Frequência: horária, diária, semanal e mensal;

i) Exclusões: pastas ou arquivos (por nome e/ou extensão) que não devem ser rastreados;

3.1.1.17. Deve possuir mecanismo de cache de informações dos arquivos já “escaneados”;

3.1.1.18. Deve possuir cache persistente dos arquivos já “escaneados” para que nos eventos de desligamento e reinicialização das estações de trabalho e notebooks, a cache não seja descartada;

3.1.1.19. Deve possibilitar alterações nos parâmetros de comunicação entre o cliente antivírus e o servidor de gerenciamento da solução de antivírus;

3.1.1.20. Deve ser capaz de detectar variantes de malwares que possam ser geradas em tempo real na memória da estação de trabalho ou notebook, permitindo que seja tomada ação de submetê-la para o analisador de sandbox para análise e remediação;

3.1.1.21. Deve permitir a restauração de maneira granular de arquivos em quarentena sob suspeita de representarem risco de segurança;

3.1.1.22. Deve permitir a restauração dos arquivos em quarentena;

3.1.2. **Proteção Anti-malware para Estações Linux**

3.1.2.1. Varredura manual com interface gráfica, personalizável, com opção de limpeza dos malwares encontrados;

3.1.2.2. Varredura manual por linha de comando, parametrizável e com opção de limpeza automática em todos os sistemas operacionais;

3.1.2.3. Capacidade de detecção e remoção de todos os tipos de malwares, incluindo spyware, adware, grayware, cavalos de Tróia, rootkits, e outros;

3.1.2.4. O cliente da solução deve armazenar localmente, e enviar para o servidor (para fins de armazenamento) logs de ocorrência de ameaças, contendo no mínimo os seguintes dados: nome da ameaça, caminho do arquivo comprometido (quando disponível), data e hora da detecção, endereço IP do cliente e ação realizada;

3.1.2.5. A desinstalação do cliente nas estações de trabalho deverá ser completa, removendo arquivos, entradas de registro e configurações, logs diversos, serviços do sistema operacional e quaisquer outros mecanismos instalados;

3.1.2.6. Possibilidade de rastrear ameaças em arquivos compactados em, no mínimo, 6 níveis recursivos de compactação e 10 níveis para OLE.

3.1.2.7. As mensagens exibidas aos usuários devem ser traduzidas para o português do Brasil;

3.1.3. Proteção Anti-malware para estações Mac-OS

3.1.3.1. O cliente para instalação deverá possuir compatibilidade com os sistemas operacionais:

3.1.3.2. Mac os x 10.9 e 10.10 em processadores 64 bits;

3.1.3.3. Gerenciamento integrado a console de gerência central da solução.

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

3.1.3.5. Permitir a verificação das ameaças da maneira manual e agendada;

3.1.3.6. Permitir a criação de listas de exclusões para pastas e arquivos que não serão verificados pelo antivírus;

3.1.3.7. Permitir a ações de reparar arquivo ou colocar em quarentena em caso de infeções a arquivos;

3.1.4. Funcionalidade de Atualização

3.1.4.1. Deve permitir a programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência configuráveis (no mínimo diária) e horários definidos pelo administrador da solução;

3.1.4.2. Deve permitir atualização incremental da lista de definições de vírus;

3.1.4.3. Deve permitir a atualização automática das vacinas a partir de localização na rede local ou na internet, a partir de fonte autenticável;

3.1.4.4. Deve permitir o rollback das atualizações das listas de definições de vírus e engines;

3.1.4.5. Deve permitir a indicação de agentes para efetuar a função de replicador de atualizações, de forma que outros agentes possam utiliza-los como fonte de atualizações, não sendo necessária a comunicação direta com o servidor de Anti-malware para essas tarefas;

3.1.4.6. Deve permitir que os agentes de atualização possam replicar os componentes de vacinas;

3.1.4.7. O servidor da solução de Anti-malware, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os agentes replicadores de atualizações, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização;

3.1.5. **Funcionalidade de Administração**

3.1.5.1. Deve permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pela console de administração da solução completa;

3.1.5.2. Deve possibilitar instalação "silenciosa";

3.1.5.3. Deve permitir o bloqueio por nome de arquivo;

3.1.5.4. Deve permitir o rastreamento e bloqueio de infecções;

3.1.5.5. Deve possuir mecanismo de detecção de ameaças baseado em comportamento de processos que estão sendo executados nas estações de trabalho e notebooks;

3.1.5.6. Deve efetuar a instalação remota nas estações de trabalho, sem requerer outro software ou agente adicional, previamente instalado e sem necessidade de reiniciar a estação de trabalho;

3.1.5.7. Deve desinstalar automática e remotamente a solução de antivírus atual, sem requerer outro software ou agente;

3.1.5.8. Deve permitir a desinstalação através da console de gerenciamento da solução;

3.1.5.9. Deve ter a possibilidade de designação do local onde o backup automático será realizado;

3.1.5.10. Deve ter a possibilidade de determinar a capacidade ou tempo de armazenamento da área de quarentena;

3.1.5.11. Deve possibilitar ao administrador a execução de tarefas para a deleção de arquivos armazenados na área de quarentena na estação de trabalho.

3.1.5.12. Deve permitir remoção automática de clientes inativos por determinado período de tempo;

3.1.5.13. Deve permitir integração com Active Directory para acesso a console de administração;

3.1.5.14. Identificar através da integração com o Active Directory, quais máquinas estão sem a solução de Anti-malware instalada;

3.1.5.15. Deve permitir criação de diversos perfis e usuários para acesso a console de administração;

3.1.5.16. Deve possuir solução de consulta do hash dos arquivos integrada e gerenciada através da solução de antivírus, cancelando o download ou execução do arquivo, de forma automática, baseado na resposta à consulta da base do fabricante;

3.1.5.17. Deve permitir agrupamento automático de estações de trabalho e notebooks da console de gerenciamento baseando-se no escopo do Active Directory ou IP;

3.1.5.18. Deve registrar no sistema de monitoração de eventos da console de Anti-malware informações relativas ao usuário “logado” no sistema operacional;

3.1.5.19. Devem prover ao administrador relatório de conformidade do status dos componentes, serviços, configurações das estações de trabalho e notebooks que fazem parte do escopo de gerenciamento da console de antivírus;

3.1.5.20. Deve prover ao administrador informações sobre quais estações de trabalho e notebooks fazem parte do escopo de gerenciamento da console de Anti-malware não realizaram o escaneamento agendado ou o escaneamento demandado pelo administrador no período determinado de dias;

3.1.5.21. Deve prover segurança através de SSL para as comunicações entre o servidor e a console de gerenciamento web;

3.1.5.22. Deve prover segurança através de SSL para as comunicações entre o servidor e os agentes de proteção;

3.1.5.23. Deve suportar a comunicação por meio de canal seguro (LDAPS) entre o servidor de Gerência e o Active Directory;

3.1.5.24. Deve permitir a criação de usuários locais de administração da console de Anti-malware;

3.1.5.25. Deve possuir a integração com o Active Directory para utilização de seus usuários para administração da console de Anti-malware;

3.1.5.26. Deve permitir criação de diversos perfis de usuários que permitam acessos diferenciados e customizados a diferentes partes da console de gerenciamento;

3.1.5.27. Deve bloquear acessos indevidos a área de administração do agente que não estejam na tabela de políticas definidas pelo administrador;

3.1.5.28. Deve se utilizar de mecanismo de comunicação segura entre o servidor de administração e os agentes de proteção distribuídos nas estações de trabalho e notebooks;

3.1.5.29. Deve permitir a gerência de domínios separados para usuários previamente definidos;

3.1.5.30. Deve ser capaz de enviar notificações específicas aos respectivos administradores de cada domínio definido na console de administração;

3.1.6. **Funcionalidade de Controle de Dispositivos**

3.1.6.1. Deve possuir controle de acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes opções: acesso total, apenas leitura, e bloqueio total;

3.1.6.2. Deve possuir controle de acesso a drivers de mídias de armazenamento como CD-ROM e DVD, com as seguintes opções: acesso total, apenas leitura, e bloqueio total;

3.1.7. **Funcionalidade de Autoproteção**

3.1.7.1. Deve possuir mecanismo de proteção contra uso não autorizado no qual o agente do antivírus deve ser protegido contra mudança do seu estado (não possibilitar que um administrador da estação de trabalho e notebook possa parar o serviço do antivírus) bem como mecanismo para restaurar seu estado normal;

3.1.7.2. Deve possuir no mecanismo de autoproteção as seguintes proteções:

a) Proteção e verificação dos arquivos de assinatura;

b) Proteção dos processos do agente de segurança;

c) Proteção das chaves de registro do agente de segurança;

d) Proteção do diretório de instalação do agente de segurança.

3.1.8. **Funcionalidade de HIPS – Host IPS e Host Firewall**

3.1.8.1. Deve ser capaz de realizar a proteção contra ataques nos seguintes sistemas operacionais:

a) Windows Server 2008 R2 e 2012 (32/64-bit);
b) Windows 7 (x86/x64);
c) Windows 8 e 8.1 (x86/x64);
d) Windows 10.

3.1.8.2. Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host ips e host firewall;

3.1.8.3. Todas as regras das funcionalidades de firewall e ips de host devem permitir apenas detecção (log) ou prevenção (bloqueio);

3.1.8.4. Deve permitir ativar e desativar o produto sem a necessidade de remoção;

3.1.8.5. A funcionalidade de host ips deve possuir regras para controle do tráfego de pacotes de determinadas aplicações;

3.1.8.6. Deve prover proteção contra as vulnerabilidades do sistema operacional Windows Vista ou superior por meio de regras de host IPs;

3.1.8.7. Deve prover proteção nativa ou por meio de customização contra as vulnerabilidades de aplicações terceiras, por meio de regras de host ips, tais como Oracle Java, abobe pdf reader, adobe flash player, realnetworks real player, Microsoft Office, Apple itunes, Apple quick time, Apple safari, Google chrome, Mozilla Firefox, opera browser, MS internet Explorer, entre outras

3.1.8.8. Deve permitir a criação de políticas de segurança personalizadas;

3.1.8.9. Deve permitir a emissão de alertas via SMTP ou SNMP;

3.1.8.10. Deve permitir configuração e manipulação de políticas de firewall através de prioridades;

3.1.8.11. Deve permitir criação de regras de firewall utilizando os seguintes protocolos: Icmp, icmpv6, tcp, udp, tcp+udp.

3.1.8.12. Deve permitir criação de regras de firewall por origem de ip ou Mac ou porta e destino de ip ou Mac ou porta;

3.1.8.13. Deve permitir a criação de regras de firewall pelos seguintes frames types: Ip, ipv4 e ipv6,

3.1.8.14. Deve permitir a criação de contextos para a aplicação para criação de regras de firewall;

3.1.8.15. Deve permitir o isolamento de interfaces de rede, possibilitando o funcionamento de uma interface por vez;

3.1.8.16. Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;

3.1.8.17. Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar a visualização e gerenciamentos;

3.1.8.18. A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação;

3.1.9. Controle de aplicações

3.1.9.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

a) Windows Server 2008 R2 e 2012 (32/64-bit);
b) Windows 7 (x86/x64);
c) Windows 8 e 8.1 (x86/x64);
d) Windows 10;

3.1.9.2. Deve permitir a criação de políticas de segurança personalizadas;

3.1.9.3. As políticas de segurança devem permitir a seleção dos alvos baseados nos seguintes critérios:

3.1.9.4. Grupos de máquinas espelhados do Active Directory;

3.1.9.5. Usuários ou grupos do Active Directory;

3.1.9.6. As políticas de segurança devem permitir o controle do intervalo para envio de atualização de cada política;

3.1.9.7. As políticas de segurança devem permitir a definição de qual servidor de gerenciamento o agente de segurança deverá comunicar-se;

3.1.9.8. As políticas de segurança devem permitir a ocultação do ícone do agente, que reside da barra de tarefas, e de notificações ao usuário;

3.1.9.9. As políticas de segurança devem permitir o controle através de regras de aplicação;

3.1.9.10. As regras de controle de aplicação devem permitir as seguintes ações:

a) Permissão de execução;

b) Bloqueio de execução;

3.1.9.11. As regras de controle de aplicação devem permitir o modo de apenas coleta de eventos (logs), sem a efetivação da ação regra;

3.1.9.12. As regras de controle de aplicação devem permitir os seguintes métodos para identificação das aplicações:

a) Assinatura sha-1, sha256 ou md5 do executável;

b) Caminho lógico do executável;

c) Base de assinaturas de certificados digitais válidos e seguros;

3.1.9.13. As políticas de segurança devem permitir a utilização de múltiplas regras de controle de aplicações.

3.1.9.14. Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;

3.1.9.15. Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar na visualização e gerenciamentos;

3.1.9.16. A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação;

3.2. SOLUÇÃO DE SEGURANÇA PARA PROTEÇÃO DA CAMADA DE SERVIDORES FÍSICOS E VIRTUAIS

3.2.1. A solução deverá ser licenciada para 380 (trezentos e oitenta) ativos;

3.2.2. As licenças devem ser fornecidas com os módulos de Firewall, Inspeção de Pacotes, Anti-malware, Controle de Aplicações, HIPS e Inspeção Avançada de Tráfego, sem a necessidade de instalação de agente para ambiente VMWare v6 ou ambiente com NSX;

3.2.3. Deverá suportar, no mínimo, as seguintes Distribuições: Suse Linux enterprise 11; Red Hat enterprise Linux 6.0 e 7.0; CentOS 6.0 e 7.0;

3.2.4. Todos componentes que fazem parte da solução devem ser do mesmo fabricante;

3.2.5. **Características Gerais;**

3.2.5.1. Precisa ter a capacidade de controlar e gerenciar a segurança de múltiplas plataformas e sistemas operacionais a partir de uma console única e centralizada do próprio fabricante;

3.2.5.2. A solução deverá ser gerenciada por console Web. Deve suportar certificado digital para gerenciamento;

3.2.5.3. O console de administração deverá permitir o envio de notificações via SMTP;

3.2.5.4. A solução deve poder enviar os logs para um dispositivo SIEM (Security Information and Event Management);

3.2.5.5. Todos os eventos e ações realizadas na console de gerenciamento precisam ser gravados para fins de auditoria;

3.2.5.6. A solução deverá permitir que a distribuição de patterns e novos componentes possa ser efetuados automaticamente em diversos pontos do ambiente;

3.2.5.7. A solução deverá permitir a criação de múltiplos perfis de segurança, que serão vinculados aos diferentes tipos de servidores do ambiente;

3.2.5.8. A solução precisa permitir a criação de relatórios. A criação e envio destes relatórios deverá ocorrer sob demanda, ou agendado com o envio automático do relatório via e-mail;

3.2.5.9. A solução deverá a criação de criação de relatórios no formato PDF.

3.2.5.10. O console de gerenciamento deve apresentar alta disponibilidade em nível de aplicação, através da criação de várias gerências, de modo que na ausência da principal, os clientes automaticamente se comuniquem com a secundária e com todas as configurações preservadas;

3.2.5.11. O console de gerenciamento deve armazenar políticas e logs em base de dados. A escolha da base de dados pode ser facultativa entre Oracle ou MSSQL;

3.2.5.12. Quando operadas em modo alta disponibilidade, as consoles devem compartilhar o mesmo database;

3.2.5.13. O console deve se integrar com o Active Directory para que os usuários do Active Directory possam administrar a solução, com permissões customizadas pela própria solução;

3.2.5.14. Os usuários devem ter a capacidade de receber determinados papéis para administração como "acesso total" e "acesso parcial", podendo ser customizado o que compõe o "acesso parcial";

3.2.5.15. Quando configurado o acesso parcial, este deve permitir que um usuário possa gerenciar a segurança de um único computador, podendo ainda definir em quais módulos de proteção será possível editar ou criar novas políticas de segurança;

3.2.5.16. O console deve se integrar com o Active Directory para que possa ser efetuado o controle das máquinas no Active Directory;

3.2.5.17. A comunicação entre a console de gerenciamento e componentes de proteção deverá ser criptografada;

3.2.5.18. O console de gerenciamento deverá ter dashboards para facilidade de monitoração, as quais deverão ser customizadas pelo administrador em quantidade e período de monitoração;

3.2.5.19. Os componentes de atualização deverão buscar os updates das assinaturas e distribuí-las.

3.2.5.20. O console de gerenciamento deverá ser gerenciado por Internet Explorer, Chrome e Firefox;

3.2.5.21. A solução deve possuir a capacidade de criar políticas de forma global para todas as máquinas, por perfis e individualmente para cada host;

3.2.5.22. Cada perfil poderá ser atribuído para um host ou um conjunto de hosts;

3.2.5.23. A solução deverá vir com perfis padrão pré-definidos;

3.2.5.24. A solução deve possuir a capacidade de isolamento de placa de rede, de forma que impeça a comunicação entre placas de rede do mesmo host, de acordo com definição do administrador;

3.2.5.25. A solução deverá ser capaz de aplicar políticas de firewall diferentes para placas de redes diferentes em um mesmo host;

3.2.5.26. A solução deverá ser capaz de executar by-pass completo de rastreamento de tráfego de forma que os módulos não atuem em determinado tipo de conexão ou pacote;

3.2.5.27. A solução deverá ser capaz de reconhecer e bloquear endereços IP que estejam realizando Network Scan, Port Scan, TCP Null Scan, TCP SYNFIN Scan, TCP Xmas Scan e Computer OS Fingerprint;

3.2.5.28. A solução deverá ter a possibilidade de enviar logs para SYSLOGS;

3.2.5.29. A solução deverá ter a possibilidade de enviar eventos da console via SNMP;

3.2.5.30. Solução deverá apresentar relatórios customizados de todas as suas funcionalidades;

3.2.5.31. Os relatórios deverão poder ser exportados nos formatos PDF;

3.2.5.32. Deve permitir enviar os relatórios para uma lista de contatos independente de login na console de administração;

3.2.5.33. As atualizações de assinaturas deverão ocorrer de forma agendada e automática;

3.2.5.34. Deve ser possível baixar as assinaturas na console de gerenciamento, mas não distribuí-las aos componentes de proteção;

3.2.5.35. A solução deverá ter capacidade de gerar pacote de auto diagnóstico de modo a coletar arquivos relevantes para envio ao suporte do produto;

3.2.5.36. No gerenciamento das licenças, deve ser informada a quantidade contratada, assim como, a quantidade em utilização de componentes de proteção;

3.2.5.37. Solução deverá ter mecanismo de procura em sua console de gerenciamento de modo que seja facilitada a busca de regras;

3.2.5.38. Possibilidade de identificação dos IPs que estejam realizando ataques;

3.2.5.39. O fabricante deverá participar do programa “Microsoft Active Protection Program” para obtenção de informações de modo a permitir a criação de regras de proteção antes mesmo dos patches serem publicados pelo fabricante;

3.2.5.40. O console de gerenciamento deve se integrar com o VMware vCenter 5.1 ou Superior, de modo a importar e sincronizar os objetos (hosts VMware e guests vm) para o console de gerenciamento da solução;

3.2.5.41. A partir desta integração, deverá ser possível gerir a segurança dos guests vm, podendo ser atribuídos perfis de segurança, regras únicas para cada host, além de possibilitar a coleta dos logs gerados para cada módulo habilitado;

3.2.5.42. Esta integração deve possibilitar que, a partir da instalação e integração de um virtual appliance do fabricante da solução de segurança com o ambiente Vmware e suas APIs, seja possível proteger as guests vms sem a necessidade de instalação de agentes de segurança do fabricante da solução nas guests vms;

3.2.5.43. Este virtual appliance deverá integrar-se com o VMware NSX, possibilitando que no mínimo 3 funcionalidades possam ser efetuadas diretamente via hypervisor e virtual appliance em conjunto, não necessitando a instalação de agentes adicionais de segurança do fabricante nos guests VMs protegidos. Dentre as funcionalidades, estão incluídas apenas:

- Firewall
- Anti-malware
- Controle de Acesso a Sites Maliciosos
- Controle de Aplicações
- Monitoramento de Integridade
- IDS/IPS

3.2.5.44. Precisa ter a capacidade de detectar e aplicar as regras necessárias do módulo de IDS/IPS, para cada servidor através da console de administração;

3.2.5.45. O console de gerenciamento deve permitir a utilização do mesmo perfil de segurança para servidores virtuais, físicos e desktops virtuais;

3.2.5.46. A solução deverá ter a capacidade de proteger automaticamente os servidores que são adicionados ao ambiente com perfil de segurança pré-definido pelo administrador;

3.2.5.47. Para virtualização em ambiente Hyper-V (Microsoft Windows Server 2008 R2 com Hyper-V e/ou Microsoft Windows Server 2012 com Hyper-V), a solução deverá integrar-se com a utilização de agente, possibilitando a execução das funcionalidades de Anti-malware, Firewall, IDS/IPS e Controle de Aplicações;

3.2.6. **Características para Firewall**

3.2.6.1. Operar como firewall de host para proteção dos servidores virtualizados;

3.2.6.2. Precisa ter a capacidade de controlar o tráfego baseado no Endereço IP, Tipos de Protocolos e intervalo de portas;

3.2.6.3. Precisa ter a capacidade de definir regras distintas para interfaces de rede distintas;

3.2.6.4. A solução deverá ser capaz de reconhecer e possibilitar o bloqueio endereços IP que estejam realizando Network Scan, Port Scan, TCP Null Scan, TCP SYNFIN Scan, TCP Xmas Scan e Computer OS Fingerprint;

3.2.6.5. Precisa ter a capacidade de implementação de regras em determinados horários que podem ser customizados pelo administrador;

3.2.6.6. Precisa ter a capacidade de definição de regras para contextos específicos;

3.2.6.7. Para facilitar a criação e administração de regras de firewall, as mesmas poderão ser baseadas em objetos que podem ser lista de IPs e lista de portas;

3.2.6.8. Regras de firewall poderão ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo se está no domínio ou não);

3.2.6.9. Regras de firewall poderão ser válidas de acordo com agendamento por horário ou dia da semana;

3.2.6.10. O firewall deverá ser stateful bidirecional;

3.2.6.11. As regras de Firewall deverão permitir, minimamente as ações de bloqueio, permissão e registro do tráfego;

3.2.6.12. O firewall deverá permitir a criação de regras através do protocolo, origem do tráfego, destino e direção;

3.2.6.13. As regras de Firewall deverão permitir, minimamente as ações de bloqueio, permissão e registro do tráfego;

3.2.6.14. A solução deverá utilizar o conceito de regras implícitas para a regra ALLOW, negando o tráfego para todo o restante que não estiver liberado;

3.2.6.15. A solução deve permitir a utilização de atribuição de prioridades diferentes as regras de firewall;

3.2.6.16. Deverá logar a atividade stateful;

3.2.6.17. Deverá prevenir ack storm;

3.2.6.18. Deverão existir regras padrão que facilitem a criação e adição de novas regras;

3.2.7. **Características para Inspeção de Pacotes**

3.2.7.1. Precisa ter a capacidade de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do S.O. e demais aplicações;

3.2.7.2. Precisa ter a capacidade de varrer o servidor protegido detectando o tipo e versão do S.O., detectando também as demais aplicações, recomendando e aplicando automaticamente regras IDS/IPS que blindem vulnerabilidades existentes no S.O. e aplicações. Esta varredura deverá poder ser executada sob demanda ou agendada;

3.2.7.3. Precisa ter a capacidade de detectar uma conexão maliciosa, com a possibilidade de bloquear esta conexão. A opção de detecção e bloqueio deverá possibilitar a implementação de forma global (todas as regras) e apenas para uma regra ou grupos de regras;

3.2.7.4. Precisa conter ou permitir a customização de regras de defesa para blindagem de vulnerabilidades e ataques que explorem Windows 2003, 2008, 2012 e mais de 100 tipos de aplicações padrão de mercado, incluindo Microsoft IIS, SQL Server, Microsoft Exchange, Oracle Database, Adobe Acrobat, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome e Web Server Apache;

3.2.7.5. Precisa ter a capacidade de armazenamento do pacote capturado quando detectado um ataque;

3.2.7.6. Deverá possibilitar a criação de regras de IPS customizadas, para proteger aplicações desenvolvidas pelo cliente;

3.2.7.7. Precisa possuir a capacidade de detectar e controlar conexões de aplicações específicas incluindo Team Viewer, programas P2P e instant messaging;

3.2.7.8. Precisa ter a capacidade de detectar e bloquear ataques em aplicações Web tais como SQL Injections e Cross Site Scriptings. Deverá ainda existir a possibilidade de captura do pacote relacionado ao ataque para fins de investigação do incidente;

3.2.7.9. Deverá bloquear tráfego por aplicação independente da porta que a aplicação utilize, de modo que a aplicação não consiga comunicar na rede, como por exemplo: bloqueio de tráfego de um determinado web browser ou aplicação de backup;

3.2.7.10. Solução deve ser capaz de habilitar modo debug na coleta dos pacotes de forma a capturar o tráfego anterior e posterior ao que foi bloqueado para facilidade de análise;

3.2.7.11. As regras de IPS deverão obrigatoriamente ter descrições de seu propósito;

3.2.7.12. As regras de IPS poderão atuar detectando ou bloqueando os eventos que as violem de modo que o administrador possa optar por qual ação tomar;

3.2.7.13. As regras de IPS de vulnerabilidade deverão apresentar severidade baseada em CVSS;

3.2.7.14. As regras de IPS quando disparadas poderão ter a possibilidade de emitir um alerta;

3.2.7.15. As regras devem ser atualizadas automaticamente pelo fabricante;

3.2.7.16. Poderá atuar no modo em linha para proteção contra ataques ou modo escuta para monitoração e alertas;

3.2.8. **Características para Anti-malware**

3.2.8.1. A solução deve permitir a proteção contra códigos maliciosos sem a necessidade da instalação de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e conforme agendamento, possibilitando a tomada de ações distintas para cada tipo de ameaça;

3.2.8.2. A solução deve possibilitar a criação de listas de exclusão, para que o processo do antivírus não execute a varredura de determinados diretórios ou arquivos do S.O.;

3.2.8.3. A solução deve possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção;

3.2.8.4. A solução deve possuir uma cache dos arquivos verificados de modo a evitar a redundância da varredura;

3.2.8.5. A cache de arquivos verificados deverá estar disponível para varredura sob demanda e varredura em tempo real;

3.2.8.6. Em ambientes Windows, deve ter capacidade de realizar inspeção e detecção sem vacina, especialmente para Ransomware e ataques de dia zero;

3.2.8.7. A solução deve ter capacidade de monitorar arquivos do sistema e softwares instalados contra mudanças não autorizadas, a fim de detectar e bloquear ameaças;

3.2.8.8. A solução deve ter capacidade de monitorar processos legítimos contra realizações de ações que não são tipicamente realizada pelos mesmos, a fim de detectar e bloquear ameaças;

3.2.8.9. A solução deve ter capacidade de monitorar documentos contra a criptografia

3.2.8.10. A solução deve proteger Docker hosts;

3.2.9. **Características para Monitoramento de Integridade**

3.2.9.1. A solução deve permitir o monitoramento de integridade de arquivos na máquina virtual (VMWARE) a ser monitorada;

3.2.9.2. Precisa ter a capacidade de detectar mudanças de integridade em arquivos e diretórios do S.O. e aplicações terceiras;

3.2.9.3. Precisa ter a capacidade de monitorar o status de serviços e processos do sistema operacional;

3.2.9.4. Precisa ter a capacidade de monitorar mudanças efetuadas no registro do Windows;

3.2.9.5. Precisa ter a capacidade de criação de regras de monitoramento em chaves de registro, diretórios e subdiretórios e para criação de regras avançadas;

3.2.9.6. Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de monitoramento de acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada;

3.2.9.7. O monitoramento poderá ser realizado em Real-time ou utilizando de scans periódicos para detectar mudanças de integridade;

3.2.9.8. A solução deverá monitorar modificações em arquivos, pastas, registros, processos, serviços e portas.

3.2.9.9. Referente à integridade dos arquivos deverá rastrear por criação, última modificação, último acesso, permissões, owner, grupo, tamanho, Sha1, Sha256 e Flags.

3.2.9.10. Deverá alertar toda vez que uma modificação ocorrer;

3.2.9.11. Deverá logar e colocar em relatório todas as modificações que ocorram;

3.2.9.12. As regras de monitoramento de integridade deverão ser atualizadas pelo fabricante ou melhoradas de forma automática;

3.2.9.13. O monitoramento deverá ocorrer em real time;

3.2.9.14. Deverá poder classificar as regras de acordo com severidade para melhor verificação nos logs e recebimento de alertas;

3.2.9.15. Deverá possibilitar escolher o diretório onde o arquivo será monitorado e incluir ou não incluir determinados tipos de arquivos dentro desse mesmo diretório;

3.2.9.16. Algumas regras podem ser modificadas pelo administrador para adequação ao seu ambiente;

3.2.10. **Características para Controle de Aplicação**

3.2.10.1. A solução deve permitir o controle de aplicações ao menos para Sistemas Operacionais Red Hat 6 e 7;

3.2.10.2. Um scan deve ser rodado na máquina e todas as aplicações inicialmente instaladas devem ser consideradas seguras para uso, o chamado baseline.

3.2.11. **Funcionalidade de HIPS – Host IPS e Host Firewall**

3.2.11.1. Deve ser capaz de realizar a proteção contra ataques nos seguintes sistemas operacionais:

a) Windows Server 2008 R2 e 2012 (32/64-bit);

3.2.11.2. Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host ips e host firewall;

3.2.11.3. Todas as regras das funcionalidades de firewall e ips de host devem permitir apenas detecção (log) ou prevenção (bloqueio);

3.2.11.4. Deve permitir ativar e desativar o produto sem a necessidade de remoção;

3.2.11.5. A funcionalidade de host ips deve possuir regras para controle do tráfego de pacotes de determinadas aplicações;

3.2.11.6. Precisa conter ou permitir a customização de regras de defesa para blindagem de vulnerabilidades e ataques que explorem Windows 2012 e mais de 100 tipos de aplicações padrão de mercado, incluindo Microsoft IIS, SQL Server, Oracle Database, Adobe Acrobat, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome e Web Server Apache.;

3.2.11.7. Deve permitir a emissão de alertas via SMTP ou SNMP;

3.2.11.8. Deve permitir configuração e manipulação de políticas de firewall através de prioridades;

3.2.11.9. Deve permitir criação de regras de firewall utilizando os seguintes protocolos: Icmp, icmpv6, tcp, udp, tcp+udp.

3.2.11.10. Deve permitir criação de regras de firewall por origem de ip ou mac ou porta e destino de ip ou mac ou porta;

3.2.11.11. Deve permitir a criação de regras de firewall pelos seguintes frames types: Ip, ipv4 e ipv6,

3.2.11.12. Deve permitir a criação de contextos para a aplicação para criação de regras de firewall;

3.2.11.13. Deve permitir o isolamento de interfaces de rede, possibilitando o funcionamento de uma interface por vez;

3.2.11.14. Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;

3.2.11.15. Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar a visualização e gerenciamentos;

3.2.11.16. A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação;

4. SERVIÇOS DE INSTALAÇÃO, CONFIGURAÇÃO E MIGRAÇÃO (ITEM 2)

4.1. Os Serviços de Instalação, Configuração e Migração compreendem o planejamento, desenvolvimento, implantação, parametrização, migração e garantia técnica;

4.2. Os Serviços de Instalação e Configuração consistem em realizar todos os procedimentos necessários para que os softwares, ao final destas etapas, estejam todos instalados e configurados.

4.3. O Serviço de Migração consiste em realizar todos os procedimentos necessários para a instalação e configuração de 50% das licenças de Proteção para Estações de Trabalho e Servidores estejam instalada nos respectivos ativos.

4.4. Instalação da Solução

4.4.1. Todas as configurações serão definidas entre a CONTRATADA e a CONTRATANTE através do Plano de Instalação a ser elaborado pela CONTRATADA;

4.5. Validação do Ambiente

4.5.1. Consiste realizar todos os procedimentos necessários para que ao final desta etapa o ambiente esteja em produção. Nesta etapa não havendo nenhuma pendência, será dado o termo de aceite dos serviços em até 05 (cinco) dias úteis;

4.5.2. Em até 05 (cinco) dias, após a conclusão de cada fase, deverá ser entregue em papel e em meio digital a documentação formal dos procedimentos realizados e instruções de trabalho. Esse conjunto de documentos deverão pautar os serviços futuros, e atender as necessidades de auditoria do CONTRATANTE.

4.6. Observações Gerais

4.6.1. Os itens ofertados deverão ser fornecidos sem restrição de uso e sem perda de qualquer funcionalidade.

4.6.2. Toda a solução a ser implementada terá que, obrigatoriamente ser validada pelo próprio fabricante do software CONTRATADO, através de certificação/documento do tipo “Quality Assurance”.

4.6.3. Para a realização dos Serviços de “Quality Assurance”, a empresa CONTRATADA deverá especificar e contratar direto com o fabricante da Solução Contratada a certificação do ambiente. Caberá unicamente à empresa CONTRATADA a alocação dos recursos do fabricante da Solução Ofertada para a realização dos Serviços de Quality Assurance na CONTRATANTE.

5. TREINAMENTO (ITEM 3)

5.1. Oferecer 6 (seis) vagas para treinamento nas soluções propostas, com carga horária mínima de 40 (quarenta) horas.

5.2. O treinamento deverá contemplar a instalação, configuração e utilização de todas as funcionalidades da solução ofertada e fazer parte da grade de treinamento oficiais da Fabricante.

5.3. O treinamento deverá ser ministrado por profissional certificado pela fabricante.

5.4. O treinamento deverá ser ministrado nas instalações da IPLANRIO em horário comercial.

5.5. A CONTRATADA será responsável pelo fornecimento do material didático para o treinamento, com o conteúdo programático que abranja a totalidade dos componentes.

5.6. Os servidores participantes farão avaliação do curso com atribuição de grau, conforme indicado abaixo:

- I (Insuficiente) – 0 a 25%
- R (Regular) – 26 a 50%
- B (Bom) – 51 a 75%
- O (Ótimo) – 76 a 100%

5.7. Se o treinamento for contratado de forma isolada e o prazo para sua realização não ultrapassar 30 (trinta dias) e o valor estiver dentro do limite legal (art. 62 c/c art. 23 da Lei 8.666/93), poderá ser dispensada a assinatura do termo contratual, que será substituído pela Nota de empenho.

5.8. A CONTRATANTE será responsável por disponibilizar infraestrutura mínima para a realização do treinamento;

6. PRAZOS

6.1. O Contrato vigorará a partir da data da sua assinatura até 24 (vinte e quatro) meses contados desta.

6.2. O prazo para entrega das licenças será de 15 (quinze) dias corridos contados da assinatura do contrato;

6.3. O prazo de instalação e configuração das soluções será de 120 (cento e vinte) dias corridos contados da assinatura do contrato;

6.4. O prazo de garantia técnica será de 24 (vinte e quatro) meses contados da instalação e configuração das licenças;

6.5. O treinamento de cada produto da solução deverá ser ministrado em até 60 (sessenta) dias após o processo de instalação e configuração de toda a solução.

6.6. O prazo de execução dos serviços poderá ser prorrogado ou alterado nos termos do Decreto Municipal 44.698/18 e do Regulamento de Licitações e Contratos da IplanRio;

6.7. No caso de serviços continuados, o contrato poderá ser prorrogado por até 5 (cinco) anos, na forma do Decreto Municipal nº 44.698/18 e do Regulamento de Licitações e Contratos da IplanRio;

6.8. Somente ocorrerá reajustamento do Contrato decorrido o prazo de 24 (vinte e quatro) meses contados da data da sua assinatura.

7. GARANTIA TÉCNICA

7.1. A Garantia Técnica deverá ser prestada para cada solução fornecida e deverá ser acionada em caso de qualquer indisponibilidade da solução, conforme os índices de criticidade abaixo:

Criticidade	Descrição	Prazo Máximo de Atendimento	Objetivo de Restauração de Serviço
Severidade 1 (Alta)	Sistema parado ou produto inoperante com impacto nas operações críticas de negócio. Exemplos: Servidor de produção ou outro sistema inicial está inativo. Parte substancial dos dados essenciais corre risco de perda ou corrupção. Operações relacionadas ao negócio foram afetadas, falha que compromete a integridade geral do sistema ou dos dados.	Em até 30 min. Deve ser iniciado o atendimento através de transferência ao telefone.	Restauração do serviço referente à solução contratada em até 6 dias.
Severidade 2 (Média/Alta)	Alto impacto no ambiente de produção ou grande restrição de funcionalidade. Exemplo: Ocorreu um problema no qual um recurso importante foi gravemente danificado. As operações podem continuar de forma limitada, embora a produtividade em longo prazo possa ser afetada negativamente.	Em até 2 horas deve ser iniciado o atendimento através de transferência ao telefone ou retorno de chamada.	Restauração do serviço referente à solução contratada em até 10 dias.

Severidade 3 (Média/Baixa)	O defeito não gera impacto ao negócio. Exemplo: Ocorreu um erro que causou impacto negativo limitado nas operações.	Em até 6 horas deve ser iniciado o atendimento através de transferência ao telefone ou retorno de chamada.	Restauração do serviço referente à solução contratada ou na próxima atualização do Software
Severidade 4 (Baixa)	O problema é pequeno, ou de documentação. Exemplos: O problema não afetou as operações da contratante negativamente; Encaminhamento de solicitações e ou sugestões para novos recursos ou aprimoramento do software licenciado	No mesmo dia ou no próximo dia útil comercial	Restauração do serviço referente à solução contratada em até 20 dias ou considerado para as próximas atualizações do Software

7.2. O atendimento deve estar disponível para os produtos objetos do presente certame;

7.3. A Garantia Técnica relativo às subscrições adquiridas deverá contemplar a atualização de versão (upgrades) para novas versões ou patches e publicadas durante o período de vigência do contrato, sem ônus para a CONTRATANTE.

7.4. Para eventos caracterizados como Severidade 1 e/ou Severidade 2, conforme descritos na tabela acima, deverão ser disponibilizadas até 4 visitas presenciais solicitadas sob demanda, para cada período de 12 (doze) meses, em regime 24 x 7 x 120 para resolução dos chamados, atividades proativas com acesso as ferramentas de propriedade exclusivas do fabricante para análise de capacidade e reparos;

7.5. Para a abertura de chamados, a CONTRATADA deverá disponibilizar canais de acesso 24 (vinte e quatro) horas por dia e 7(sete) dias por semana, através de número de telefone de discagem gratuita e internet para abertura de chamados técnicos objetivando a resolução de problemas e dúvidas quanto ao funcionamento dos softwares.

7.6. Todos os chamados, independente de sua criticidade, deverão ser abertos em um único número telefônico.

7.7. Todos os prazos para atendimento da garantia começarão a ser contados a partir da abertura do chamado independentemente deste ter sido feito via telefone, e-mail, Website do fabricante;

7.8. Dentro do prazo máximo de solução está compreendido o prazo de atendimento;

7.9. Considera-se plenamente solucionado o problema quando restabelecidos os sistemas/serviços sem restrições, ou seja, quando não se tratar de uma solução paliativa;

7.10. Os serviços de atendimento de garantia para chamados de severidades 1 e 2 não podem ser interrompidos até o completo restabelecimento de todas as funções do sistema paralisado (indisponível), mesmo que para isso tenham que se estender por períodos noturnos e dias não úteis (sábados, domingos e feriados);

7.11. Nos casos em que as manutenções necessitarem de paradas da solução, o CONTRATANTE deverá ser imediatamente notificado para que se proceda à aprovação da manutenção, ou para que seja agendada nova data, a ser definida pelo CONTRATANTE, para execução das atividades de manutenção;

7.12. A CONTRATADA deve emitir relatórios de todas as intervenções realizadas, preventivas e corretivas, programadas ou de emergência, ressaltando os fatos importantes e detalhando os pormenores das intervenções, de forma a manter registros completos das ocorrências e subsidiar as decisões da administração do Complexo Central de Tecnologia do CONTRATANTE;

7.13. O relatório deve ser assinado por representante do CONTRATANTE, responsável pelo acompanhamento do serviço, que se obriga a acompanhar a execução das manutenções;

7.14. Não haverá custos adicionais para a CONTRATANTE, quando da abertura dos chamados técnicos.

7.15. Em caso de descumprimento dos prazos descrito na tabela do item 7.1, a Contratada se sujeitará às penalidades previstas no Edital e no Contrato.

8. DA FISCALIZAÇÃO

8.1. A CONTRATADA submeter-se-á a todas as medidas e procedimentos de Fiscalização. Os atos de fiscalização, inclusive inspeções e testes, executados pelo CONTRATANTE e/ou por seus prepostos, não eximem a CONTRATADA de suas obrigações no que se refere ao cumprimento das normas, especificações e projetos, nem de qualquer de suas responsabilidades legais e contratuais.

8.2. A Fiscalização da execução dos serviços caberá à comissão designada por ato da autoridade competente no âmbito do (a) CONTRATANTE. Incumbe à Fiscalização a prática de todos os atos que lhe são próprios nos termos da legislação em vigor, respeitados o contraditório e a ampla defesa.

8.3. A CONTRATADA declara, antecipadamente, aceitar todas as decisões, métodos e processos de inspeção, verificação e controle adotados pelo CONTRATANTE, se obrigando a fornecer os dados, elementos, explicações, esclarecimentos e comunicações de que este necessitar e que forem considerados necessários ao desempenho de suas atividades.

8.4. Compete à CONTRATADA fazer minucioso exame da execução dos serviços, de modo a permitir, a tempo e por escrito, apresentar à Fiscalização, para o devido esclarecimento, todas as divergências ou dúvidas porventura encontradas e que venham a impedir o bom desempenho do Contrato. O silêncio implica total aceitação das condições estabelecidas.

8.5. A atuação fiscalizadora em nada restringirá a responsabilidade única, integral e exclusiva da CONTRATADA no que concerne aos serviços contratados, à sua execução e às consequências e implicações, próximas ou remotas, perante o CONTRATANTE, ou perante terceiros, do mesmo modo que a ocorrência de eventuais irregularidades na execução dos serviços contratados não implicará corresponsabilidade do CONTRATANTE ou de seus prepostos.

8.6. A CONTRATADA se obriga a permitir que o pessoal da fiscalização do CONTRATANTE acesse quaisquer de suas dependências, possibilitando o exame das instalações e também das anotações relativas as pessoas e materiais, fornecendo, quando solicitados, todos os dados e elementos referentes à execução do contrato.

9. ACEITAÇÃO DOS OBJETOS

9.1. A aceitação dos objetos deste TR se dará mediante a avaliação da Comissão de Fiscalização, que constatará se os serviços atendem a todas às especificações contidas neste TR, e na Proposta que ensejou a presente contratação.

9.1.1. Em relação aos serviços de entrega, instalação, migração, configuração da solução, a Comissão de Fiscalização emitirá a Aceitação Provisória após a realização dos mesmos.

9.1.2. Em relação à prestação de serviços de treinamento, somente será emitido o aceite após parecer favorável da Coordenadoria Técnica de Pessoas – CTP, que constatará se o serviço de treinamento atende a todas às especificações contidas neste Termo de Referência.

9.1.3. Os treinamentos somente serão aceitos pela Comissão Fiscalizadora se no mínimo 60% das avaliações do treinamento, preenchidas pelos servidores da IPLANRIO indicarem o conceito “BOM” ou "ÓTIMO".

9.1.3.1. Tal procedimento visa garantir que a Contratada efetivamente transfira para os profissionais da Contratante as informações necessárias para a aplicação do conhecimento.

9.2. Os serviços prestados em desacordo com a especificação deste TR e da Proposta deverão ser recusados pela Comissão responsável pela fiscalização do contrato, que anotará em registro próprio as ocorrências e determinará o que for necessário à regularização das faltas ou defeitos observados. No que exceder à sua competência, comunicará o fato à autoridade superior, em 5 (cinco) dias, para ratificação.

9.3. O objeto do presente contrato será recebido em tantas parcelas quantas forem às relativas ao pagamento.

9.4. Na hipótese da recusa da aceitação, a CONTRATADA deverá reexecutar os serviços não aceitos, em prazo a ser estabelecido pela CONTRATANTE, passando a contar os prazos para pagamento e demais compromissos do CONTRATANTE da data da efetiva aceitação. Caso a CONTRATADA não reexecute os serviços não aceitos no prazo assinado, a CONTRATNTE se reserva o direito de providenciar a sua execução a expensas da CONTRATADA, sem prejuízo das penalidades cabíveis.

10. QUALIFICAÇÃO TÉCNICA

10.1. A Licitante deverá comprovar aptidão para desempenho de atividade pertinente e compatível em características e prazos com os objetos da licitação, mediante apresentação de certidão(ões) ou atestado(s) fornecido(s) por pessoa jurídica de direito público ou privado.

10.1.1. Considera-se compatível com objeto da licitação, em relação ao item 1, atestado ou certidão que demonstre que a Licitante prestou 10% das quantidades dos itens descritas na tabela do item 3 deste TR.

10.1.2. Considera-se compatível com objeto da licitação, em relação aos itens 2 e 3, atestado ou certidão que demonstre que a Licitante prestou 50% das quantidades dos itens descritas na tabela do item 3 deste TR.

10.2. A licitante deverá apresentar declaração de que, à época da assinatura do contrato, alocará na prestação dos serviços de instalação, configuração e operação assistida profissionais que possuam certificação na solução ofertada.

10.3. Declaração da licitante de que, à época da assinatura da contratação, alocará na prestação de serviços de treinamento profissionais certificados na solução ofertada, referente ao curso que for ministrar.

10.4. Será admitida a soma dos atestados ou certidões apresentados pelas licitantes, desde que os mesmos sejam tecnicamente pertinentes e compatíveis em características e prazos com o objeto da licitação e descritos na tabela do item 3 deste TR.

11. HOMOLOGAÇÃO TÉCNICA

11.1. A homologação será realizada em uma única etapa. No momento da homologação será efetuada a verificação dos catálogos/manuais oficiais dos produtos ofertados. As características dos produtos oferecidos deverão estar em conformidade com a especificação técnica descrita neste documento.

11.2. A CONTRATANTE, em qualquer momento ou fase do processo de homologação, poderá requisitar que as Licitantes comprovem as especificações exigidas neste termo de referência, em função de divergências ocorridas. As Licitantes deverão fazê-lo através de testes comprobatórios de conformidade perante a equipe técnica da Contratante.

11.3. A Licitante deverá apresentar documentação técnica oficial e original (ex: especificações, catálogos, prospectos e folders) de toda a solução ofertada que serão instalados na Contratante, junto da proposta.

11.4. Estes documentos serão utilizados pela Diretoria de Operações da RESPONSÁVEL TÉCNICA, para comprovação técnica do conteúdo especificado e requisitado no edital, referente à solução, devendo e atender as recomendações abaixo:

I. A documentação técnica oficial e original deverá ser apresentada de forma única;

II. Os referidos documentos deverão estar atualizados em sua última versão, de impressão e de conteúdo, de forma a não causar divergências de informações entre as diversas fontes oficiais disponibilizadas pelo fabricante da solução, incluindo-se os “sites” oficiais dos fabricantes na Internet.

III. Não serão aceitas declarações ou cartas de conformidade ou adequação ao solicitado e especificado neste Termo de Referência em substituição ou complementação da documentação técnica oficial e original.

12. OBRIGAÇÕES DA CONTRATADA

12.1. Prestar os serviços de acordo com todas as exigências contidas no Termo de Referência e na Proposta;

12.2. Tomar as medidas preventivas necessárias para evitar danos a terceiros, em consequência da execução dos serviços.

12.3. Responsabilizar-se integralmente pelo ressarcimento de quaisquer danos e prejuízos, de qualquer natureza, que causar à CONTRATANTE ou a terceiros, decorrentes da execução do objeto desta contratação, respondendo por si, seus empregados, prepostos e sucessores, independentemente das medidas preventivas adotadas e da comprovação de sua culpa ou dolo na execução do contrato.

12.4. Atender às determinações e exigências formuladas pela CONTRATANTE;

12.5. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados, no prazo determinado pela Fiscalização;

12.6. Responsabilizar-se, na forma do Contrato, por todos os ônus, encargos e obrigações comerciais, sociais, tributárias, trabalhistas e previdenciárias, ou quaisquer outras previstas na legislação em vigor, bem como por todos os gastos e encargos com material e mão de obra necessária à completa realização dos serviços até o seu término:

a) em caso de ajuizamento de ações trabalhistas contra a CONTRATADA, decorrentes da execução do presente Contrato, com a inclusão do Município do Rio de Janeiro ou de entidade da Administração Pública indireta como responsável subsidiário ou solidário, o CONTRATANTE poderá reter, das parcelas vincendas, o montante dos valores cobrados, que serão complementados a qualquer tempo com nova retenção em caso de insuficiência;

b) no caso da existência de débitos tributários ou previdenciários, decorrentes da execução do presente Contrato, que possam ensejar responsabilidade subsidiária ou solidária do CONTRATANTE, as parcelas vincendas poderão ser retidas até o montante dos valores cobrados, que serão complementados a qualquer tempo com nova retenção em caso de insuficiência;

c) as retenções previstas nas alíneas “a” e “b” poderão ser realizadas tão logo tenha ciência o Município do Rio de Janeiro ou o CONTRATANTE da existência de ação trabalhista ou de débitos tributários e previdenciários e serão destinadas ao pagamento das respectivas obrigações caso o Município do Rio de Janeiro ou entidade da Administração Pública indireta sejam compelidos a tanto, administrativa ou judicialmente, não cabendo, em nenhuma hipótese, ressarcimento à CONTRATADA;

d) eventuais retenções previstas nas alíneas “a” e “b” somente serão liberadas pelo CONTRATANTE se houver justa causa devidamente fundamentada.

12.7. Manter as condições de habilitação e qualificação exigidas no Edital durante todo prazo de execução contratual;

12.8. Responsabilizar-se inteira e exclusivamente pelo uso regular de marcas, patentes, registros, processos e licenças relativas à execução desta contratação, eximindo a CONTRATANTE das consequências de qualquer utilização indevida;

12.9. Indicar nas notas fiscais emitidas, quando o objeto envolver prestação de serviços, o efetivo período do mês que está sendo faturado.

12.10. Ministrar sem ônus para a contratante, no mínimo, 01 (uma) palestra no primeiro mês de vigência do Contrato, nas dependências da Empresa Municipal de Informática S.A. – IPLANRIO, visando explicar os procedimentos para o licenciamento da solução ofertada. Todas as despesas de hospedagem, transporte e alimentação serão de responsabilidade da Contratada.

12.11. Garantir que a distribuição dos produtos esteja livre de defeitos, sob uso normal, e de qualquer rotina alienígena (vírus), voltada para a danificação ou degradação, tanto de dados, quanto de hardware ou de software, ou outro defeito similar.

12.12. Responder, formalmente, dentro de 03 (três) dias úteis, a todas as correspondências emitidas pela contratante (Empresa Municipal de Informática S.A. – IPLANRIO), prestando todos os esclarecimentos solicitados.

12.13. Comprovar, no ato da assinatura do contrato, que os profissionais alocados na prestação de serviços de instalação, configuração e Operação Assistida possuem certificação na solução ofertada.

12.14. Comprovar, no ato da assinatura do contrato, que os instrutores possuem certificação na solução ofertada referente ao curso que forem ministrar.

12.15. Disponibilizar, no ato da contratação, instrutor(es) ou monitor(es) alocado(s) aos serviços de treinamento objeto deste Termo de Referencia.

12.16. Fornecer material didático oficial aos alunos, incluindo: apostilas, apresentações, indicação de bibliografia sobre o assunto. Este material deverá ser entregue no formato impresso, em língua portuguesa.

12.17. Informar à Contratante, por e-mail, no dia útil seguinte a realização do treinamento, sobre ausência e atraso dos servidores da Contratante;

12.18. Emitir certificados de conclusão para cada servidor participante no final de cada curso;

12.19. Enviar para a Contratante cópia dos certificados nominais de conclusão, lista de presença e as avaliações do treinamento preenchidas pelos servidores participantes da Contratante, em até 05(cinco) dias úteis após o término do treinamento descrito no item 03 – Descrição dos Serviços deste Termo de Referência. Este procedimento é condição para atestação da nota fiscal;

12.20. Em relação à prestação de serviços que demandam a entrada dos prestadores de serviços nas instalações da Iplanrio e, por consequência, o fornecimento de crachá para acesso ao Teleporto, é obrigado a devolver o referido crachá ao final da prestação do serviço ou caso o prestador seja substituído e, na hipótese do crachá não ser devolvido, deverá reembolsar a Iplanrio pelo custo do crachá.

13. SANÇÕES ADMINISTRATIVAS

Sem prejuízo de indenização por perdas e danos, a CONTRATANTE poderá impor ao licitante, adjudicatário ou contratado, pelo descumprimento total ou parcial das obrigações a que esteja sujeito, as sanções descritas no Edital e na Minuta de Contrato, observado o Regulamento Geral do Código de Administração Financeira e Contabilidade Pública do Município do Rio de Janeiro – RGCAF, garantida a defesa prévia à CONTRATADA.

14. DA GARANTIA CONTRATUAL

14.1 A empresa beneficiária prestará garantia de 2% (dois por cento) do valor total do Contrato, até o momento da sua assinatura ou da retirada do instrumento equivalente, em uma das modalidades previstas no art. 81 do Decreto Municipal 44.698/18.

14.1.1 No caso de seguro-garantia, o instrumento deverá contemplar a possibilidade de sua renovação no período compreendido entre a data de assinatura do Contrato e a data de encerramento da sua execução e incluir a cobertura dos valores relativos a multas eventualmente aplicadas.

14.1.2 No caso de fiança bancária, deverá ser observado o padrão estabelecido pelo Decreto Municipal nº 26.244/06 ou pela Portaria IPLANRIO "N" N.º 153, de 09 de fevereiro de 2011.

14.1.3 A licitante vencedora deverá apresentar garantia no prazo de até 05 (cinco) dias úteis, contados da convocação por meio de comunicação formal.

14.2 A não-observância do prazo estabelecido no subitem 14.1.3 caracteriza o descumprimento total da obrigação assumida, sujeitando a licitante vencedora às penalidades legalmente estabelecidas.

14.3 A CONTRATANTE utilizará a garantia para assegurar as obrigações associadas ao Contrato, podendo recorrer a esta inclusive para cobrar valores de multas eventualmente aplicadas e ressarcir-se dos prejuízos que lhe forem causados em virtude do descumprimento das referidas obrigações.

14.4 Os valores das multas impostas por descumprimento das obrigações assumidas no Contrato serão descontados da garantia caso não venham a ser quitados no prazo de 03 (três) dias úteis, contados da ciência da aplicação da penalidade. Se a multa aplicada for de valor superior ao valor da garantia prestada, além da perda desta, responderá a CONTRATADA pela diferença, que será descontada dos pagamentos eventualmente devidos pela Administração ou cobrada judicialmente.

14.5 Em caso de rescisão decorrente de falta imputável à CONTRATADA, a garantia reverterá integralmente ao CONTRATANTE, que promoverá a cobrança de eventual diferença que venha a ser apurada entre o importe da garantia prestada e o débito verificado.

14.6 Na hipótese de descontos da garantia a qualquer título, seu valor original deverá ser integralmente recomposto no prazo de 7 (sete) dias úteis, exceto no caso da cobrança de valores de multas aplicadas, em que esse será de 48 (quarenta e oito) horas, sempre contados da utilização ou da notificação pelo(a) CONTRATANTE, o que ocorrer por último, sob pena de rescisão administrativa do Contrato.

14.7 Caso o valor do Contrato seja alterado, de acordo com o art. 92 do Decreto Municipal n.º 44.698/18, a CONTRATADA deverá complementar o valor da garantia para que seja mantido o percentual de 2% (dois por cento) do valor do Contrato.

14.8 Sempre que houver reajuste ou alteração do valor do Contrato, a garantia será complementada no prazo de 7 (sete) dias úteis do recebimento, pela CONTRATADA, do correspondente aviso, sob pena de aplicação das sanções previstas no RGCAF.

14.9 Os reforços do valor da garantia poderão ser igualmente prestados em uma das modalidades previstas no art. 81 do Decreto Municipal 44.698/18.

14.10 A garantia contratual somente será restituída após o integral cumprimento do Contrato, mediante ato liberatório da autoridade contratante, nos termos do artigo 465, do RGCAF, podendo ser retida, se necessário, para quitar eventuais obrigações da CONTRATADA.

15. DA PROPOSTA DE PREÇOS

15.1 Os preços propostos deverão estar de acordo com os praticados no mercado, e neles deverão estar inclusos todos os impostos, taxas, fretes, material, mão de obra, instalações e quaisquer outras despesas necessárias e não especificadas neste Termo de Referência, mas julgadas essenciais ao cumprimento do objeto desta contratação.

15.2 A proposta de preços deve ser apresentada de acordo com as especificações deste Termo de Referência e nos moldes praticados pelo Município do Rio de Janeiro.

16. LOCAL DE EXECUÇÃO DOS SEVIÇOS

16.1 O local de entrega dos produtos e das respectivas subscrições será o setor de informática da Empresa Municipal de Informática S.A. – IPLANRIO ou de modo eletrônico.

16.2 O local de execução dos serviços será definido nos seguintes termos:

a) Os serviços de instalação, configuração, e garantia técnica e operação assistida serão executados nas dependências da IplanRio, devendo as licenças serem entregues/disponibilizadas no seu respectivo setor de informática ou por meio eletrônico.

b) Os serviços de treinamento serão executados em local a ser disponibilizado pela CONTRATANTE com observância do item 6.

17. CONDIÇÕES DE PAGAMENTO

17.1 Em relação aos itens 1 e 2, os pagamentos serão efetuados à CONTRATADA, por demanda conforme Cronograma Físico Financeiro descrito no item 21 deste Termo de Referência, após a regular liquidação da despesa, nos termos do art. 63 da Lei Federal nº 4.320/64, observadas as disposições referentes ao recebimento do objeto contidas no Termo de Referência, no Edital e no contrato. O prazo para pagamento será de 30 (trinta) dias, contados da data do protocolo do documento de cobrança no setor pertinente do(a) CONTRATANTE e obedecido o disposto na legislação.

17.2 Em relação ao item 3, o pagamento serão efetuado depois da conclusão do treinamento e a aceitação pela CONTRATANTE, conforme Cronograma Físico Financeiro descrito no item 21 deste Termo de Referência, bem como, após a regular liquidação da despesa, nos termos do art. 63 da Lei Federal nº 4.320/64, observadas as disposições referentes ao recebimento do objeto contidas no Termo de Referência, no Edital e no contrato.

17.3 Para fins de medição, se for o caso, e faturamento, o período-base de medição do serviço prestado será de um mês, considerando-se o mês civil, podendo no primeiro mês e no último, para fins de acerto de contas, o período se constituir em fração do mês, considerado para esse fim o mês com 30 (trinta) dias.

17.4 O pagamento à CONTRATADA será realizado em razão dos serviços efetivamente prestados e aceitos no período-base mencionado no item anterior sem que o(a) CONTRATANTE esteja obrigado(a) a pagar o valor total do contrato.

17.5 A CONTRATADA deverá apresentar juntamente com o documento de cobrança, os comprovantes de recolhimento do FGTS e INSS de todos os empregados atuantes no contrato, assim como Certidão Negativa de Débitos Trabalhistas – CNDT ou Certidão Positiva de Débitos Trabalhistas com efeito negativo válida, declaração de regularidade trabalhista, e documentos exigidos pelas normas de liquidação das despesas aplicáveis.

17.6 O valor dos pagamentos eventualmente efetuados com atraso, desde que não decorra de fato ou ato imputável à CONTRATADA, sofrerá a incidência de juros de 1% (um por cento) ao mês, calculados pro rata die entre o 31º (trigésimo primeiro) dia da data do protocolo do documento de cobrança na tesouraria da CONTRATANTE e a data do efetivo pagamento.

17.7 O valor dos pagamentos eventualmente antecipados será descontado à taxa de 1% (um por cento) ao mês, calculada pro rata die, entre o dia do pagamento e o 30º (trigésimo) dia da data do protocolo do documento de cobrança na Tesouraria da CONTRATANTE.

17.8 O pagamento será efetuado à CONTRATADA através de crédito em conta corrente aberta em banco a ser indicado pelo CONTRATANTE, a qual deverá ser cadastrada junto à Coordenação do Tesouro Municipal.

18. PROPRIEDADE, SIGILO E RESTRIÇÕES

18.1 Todos os produtos resultantes dos serviços desenvolvidos pela CONTRATADA deverão ser entregues a CONTRATANTE, que terá direito de propriedade sobre os mesmos, inclusive códigos fonte, documentação, componentes básicos e bibliotecas, utilizados no desenvolvimento do software;

18.2 O direito patrimonial e a propriedade intelectual dos Produtos/Serviços contratados são exclusivos da CONTRATANTE;

18.3 A CONTRATADA obriga-se a tratar como "segredos comerciais e confidenciais", quaisquer informações, dados, processos, fórmulas, códigos, fluxogramas, diagramas lógicos, dispositivos e modelos relativos aos serviços ora contratados, utilizando-os apenas para as finalidades previstas neste ajuste, não podendo revelá-los ou facilitar a sua revelação a terceiros;

18.4 A CONTRATADA obriga-se a manter o Serviço Contratado em completo sigilo e a não retirar ou destruir qualquer indicação dele constante, referente à propriedade da CONTRATANTE.

18.5 Compromete-se ainda a tomar todas as medidas cabíveis para que seus empregados cumpram estritamente a obrigação por ela assumida. Salvo para fins de segurança back-up a CONTRATADA não extrairá cópias, não permitindo que o façam, nem reproduzirá qualquer parte do Serviço Contratado, sob qualquer forma, sem o prévio consentimento, por escrito, da CONTRATANTE.

19. MODALIDADE E TIPO DE LICITAÇÃO

A licitação se dará na modalidade de pregão eletrônico do tipo menor preço global com desconto linear entre os item, pois trata-se de uma aquisição de bens comuns de Tecnologia da Informação, nos ditames da Lei Federal nº 10.520/2002. Conforme item 3 das Especificações Técnicas, devendo estar incluídos nos preços ofertados todos os custos relativos a tributos, entrega e demais despesas diretas e indiretas, nas condições descritas e especificadas no Edital e em seus Anexos

20. DA SUBCONTRATAÇÃO

20.1 Na hipótese descrita no caput, a CONTRATADA não poderá efetivamente subcontratar, nem ceder, sem a prévia e expressa anuência da CONTRATANTE e sempre mediante instrumento próprio, a ser publicado na imprensa oficial.

20.2 A CONTRATADA, na execução do contrato, sem prejuízo das responsabilidades contratuais e legais, poderá subcontratar partes do serviço ou fornecimento, no limite de 20% (vinte por cento) do objeto da licitação e abaixo indicados:

a) Serviços de instalação, configuração e Migração.

b) Treinamento

20.3 A SUBCONTRATADA deverá atender, em relação ao objeto da subcontratação, as exigências de qualificação técnica impostas ao licitante vencedor.

20.4 A SUBCONTRATADA será solidariamente responsável com a CONTRATADA por todas as obrigações legais e contratuais decorrentes do objeto do Contrato, nos limites da subcontratação, inclusive as de natureza trabalhista e previdenciária.

20.5 É vedada a subcontratação de empresa ou consórcio que tenha participado:

a) do procedimento licitatório do qual se originou a contratação;

b) direta ou indiretamente, da elaboração de projeto básico ou executivo.

21. CRONOGRAMA DE DESEMBOLSO FÍSICO-FINANCEIRO

Etapa	Descrição	Prazo	Percentual de pagamento referente ao valor total do contrato
1	Entrega das Licenças (Item 1)	1º Parcela até 30 dias após a entrega das licenças para a CONTRATANTE, contados da data do protocolo do documento de cobrança no setor pertinente da CONTRATANTE, após a devida atestação.	40%
		2º Parcela até 12 (doze) meses após a entrega das licenças para a CONTRATANTE, contados da data do protocolo do documento de cobrança no setor pertinente da CONTRATANTE, após a devida atestação.	50%

2	Serviços de instalação, configuração e Migração (Item 2)	Uma parcela até 30 dias após a execução dos serviços, contados da data do protocolo do documento de cobrança no setor pertinente do (a) CONTRATANTE, após a devida atestação**.**	7%
3	Serviço de Treinamento (Item 3)	Uma parcela até 30 dias após a execução dos serviços, contados da data do protocolo do documento de cobrança no setor pertinente do (a) CONTRATANTE, após a devida atestação**.**	3%

Rio de Janeiro, 25 Outubro de 2019.

Jorge Francisco Antunes
Assessor Técnico
Diretoria de Operações
IPLANRIO

João Cypriano
Diretor de Operações
IPLANRIO