PREFEITURA DA CIDADE DO RIO DE JANEIRO

Secretaria Municipal da Casa Civil

Empresa Municipal de Informática - IPLANRIO

TERMO DE REFERÊNCIA

SELEÇÃO DE EMPRESA PARA FORNECIMENTO DE SOLUÇÃO CORPORATIVA DE SEGURANÇA PARA PROTEÇÃO DE ESTAÇOES DE TRABALHO, SERVIDORES E REDE.

Outubro de 2017

1. OBJETO

Aquisição de solução corporativa de segurança para proteção de Estações de Trabalho, Servidores e Rede com Gerência Centralizada, Serviço de Instalação, Configuração, Suporte Técnico, Operação Assistida por 45 (quarenta e cinco) dias, e treinamento, conforme descritos, caracterizados e especificados neste Termo de Referência.

2. DEFINIÇÕES

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

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

III. GESTOR DO PROCESSO é a pessoa com atribuições gerenciais, técnicas e operacionais relacionadas ao processo de gestão do contrato, indicado pela Empresa Municipal de Informática S.A. – IPLANRIO CONTRATANTE.

IV. REPRESENTANTE DA CONTRATADA é o funcionário preposto da contratada, responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto a contratante, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual.

3. DESCRIÇÃO DOS PRODUTOS E SERVIÇOS

3.1. **Especificação da Solução de Proteção para Estações de Trabalho**

A solução de segurança de Endpoint deverá ser licenciada para **28.650 (vinte e oito mil e seiscentos e cinquenta)** 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) Solução de Segurança para Proteção da camada de Servidores Físicos e Virtuais;

3.1.1. **Módulo de proteção Anti-malware**

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

- Windows Server 2008, 2008 R2 e 2012 (32/64-bit);
- Windows vista (x86/x64);
- Windows 7 (x86/x64);
- Windows 8 e 8.1 (x86/x64);
- Windows 10

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 capacidade nativa de integração com modulo da análise virtual para ameaças desconhecidas com suporte a sandbox do mesmo fabricante da solução ofertada

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

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

3.1.1.7. Deverá incluir regras específicas para detecção de Ransomware;

3.1.1.8. Deve detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, key loggers, programas de propaganda, rootkits, phishing, dentre outros;

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

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

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

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

3.1.1.13. Arquivos recebidos por meio de programas de comunicação instantânea (msn messenger, yahoo messenger, google talk, dentre outros).

3.1.1.14. 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;

3.1.1.15. Deve possuir detecção heurística de vírus desconhecidos;

3.1.1.16. Deve permitir configurar a prioridade do uso de CPU que será utilizada para uma varredura manual ou agendada;

3.1.1.17. 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, parametrizável, com opção de limpeza;

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 mover automaticamente para área de segurança (quarentena);

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

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

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

3.1.1.19. 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;

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

3.1.1.21. Deve ser capaz de aferir a reputação das URL’s acessadas pelas estações de trabalho e notebooks, sem a necessidade de utilização de qualquer tipo de programa adicional ou plug-in ao navegador web, de forma a proteger o usuário independente da maneira de como a URL está sendo acessada;

3.1.1.22. 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 colocar a ameaça em quarentena;

3.1.1.23. Deve ser capaz de bloquear o acesso a qualquer site não previamente analisado pelo fabricante;

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

3.1.1.25. Deve permitir em conjunto com a restauração dos arquivos em quarentena a adição automática as listas de exclusão de modo a evitar novas detecções dos arquivos;

3.1.1.26. A solução de antivírus deverá ser capaz de submeter automaticamente arquivos suspeitos a uma solução de análise de ameaças direcionadas/desconhecidas locais, não sendo realizada de maneira externa ao ambiente, apresentado como resultado da análise, no mínimo, as seguintes informações;

a) Processos de Auto Start;
b) Modificações de Arquivos de Sistema;
c) Serviços criados e modificados;
d) Atividade de Rede Suspeita;
e) Modificações de Registros;

3.1.1.27. A análise de ameaças direcionadas/desconhecidas locais deverá detectar objetos maliciosos que explorem vulnerabilidades específicas dos seguintes sistemas operacionais e aplicativos apresentando relatório detalhado da ameaça;

a) Microsoft Windows 7, 8 e 10 em Português;
b) Microsoft Office: 2007, 2010 e 2013;
c) Adobe Reader: 9, X e XI;
d) Java;
e) Firefox;
f) Adobe Flash Player;

3.1.1.28. A solução de análise de ameaças direcionadas/desconhecidas deverá realizar automaticamente o bloqueio em ações suspeitas nos Desktops infectados com aquela ameaça analisada em sandbox.

3.1.2. **Funcionalidade de Atualização**

3.1.2.1. 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;

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

3.1.2.3. Deve permitir a atualização automática do "*engine"* do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável;

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

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

3.1.2.6. Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, versão de programas, hotfix e configurações específicas de domínios da árvore de gerenciamento;

3.1.2.7. 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 e configurações, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização;

3.1.2.8. O agente replicador de atualizações e configurações, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os demais agentes locais, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização;

3.1.3. **Funcionalidade de administração**

3.1.3.1. 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;

3.1.3.2. Deve possibilitar instalação "silenciosa";

3.1.3.3. Deve permitir o bloqueio por nome de arquivo;

3.1.3.4. Deve permitir o travamento de pastas/diretórios e de compartilhamentos;

3.1.3.5. Deve permitir o rastreamento e bloqueio de infecções;

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

3.1.3.7. 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;

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

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

3.1.3.10. Deve ter a possibilidade de backup da base de dados da solução através da console de gerenciamento;

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

3.1.3.12. Deve ter a possibilidade de determinar a capacidade de armazenamento da área de quarentena;

3.1.3.13. Deve permitir a deleção dos arquivos que se encontram em quarentena.

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

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

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

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

3.1.3.18. Deve permitir que a solução utilize consulta externa à base de reputação de sites integrada e gerenciada através da solução de Anti-malware, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

3.1.3.19. 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;

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

3.1.3.21. Deve permitir criação de subdomínios consecutivos dentro da árvore de gerenciamento;

3.1.3.22. Deve possuir solução de reputação de sites local para sites já conhecidos como maliciosos integrados e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

3.1.3.23. Deve registrar no sistema de monitoração de eventos da console de Anti-malware informações relativas ao usuário logado no sistema operacional

3.1.3.24. Deve 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;

3.1.3.25. 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;

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

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

3.1.3.28. Deve utilizar de chave de criptografia que seja/esteja em conformidade com o Active Directory para realizar uma conexão segura entre servidor de antivírus e o controlador de domínio;

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

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

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

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

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

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

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

3.1.3.36. Deve permitir configuração do serviço de reputação de sites da web em níveis: baixo, médio e alto.

3.1.4. Funcionalidade de controle de dispositivos

3.1.4.1. 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, leitura e escrita, leitura e execução, apenas leitura, e bloqueio total;

3.1.4.2. Deve possuir o controle de acesso a drives de mídias de armazenamento como cdrom, dvd, com as opções de acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

3.1.4.3. Deve possuir o controle a drives mapeados com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

3.1.4.4. Deve permitir escaneamento dos dispositivos removíveis e periféricos (USB, disquete, cdrom) mesmo com a política de bloqueio total ativa.

3.1.5. Funcionalidade de autoproteção

3.1.5.1. 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;

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

3.1.5.3. Autenticação de comandos ipc;

3.1.5.4. Proteção e verificação dos arquivos de assinatura;

3.1.5.5. Proteção dos processos do agente de segurança;

3.1.5.6. Proteção das chaves de registro do agente de segurança;

3.1.5.7. Proteção do diretório de instalação do agente de segurança.

3.1.6. Módulo de proteção Anti-malware para estações Linux

3.1.6.1. Deverá suportar, no mínimo, as seguintes Distribuições: Suse linux enterprise 10 e 11; Red Hat enterprise linux 6.0 e 7.0; CentOS 6.0 e 7.0;

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

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

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

3.1.6.5. Detecção e remoção de códigos maliciosos de macro do pacote Microsoft office, em tempo real;

3.1.6.6. 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;

3.1.6.7. Geração de cópia de segurança dos arquivos comprometidos antes de realizar o processo de remoção de ameaças. Esta cópia deve ser gravada na máquina local, e o acesso ao arquivo deve ser permitido somente pela solução de segurança ou o administrador;

3.1.6.8. 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;

3.1.6.9. Possibilidade de rastrear ameaças em arquivos compactados em, no mínimo, 15 níveis recursivos de compactação;

3.1.6.10. As mensagens exibidas aos usuários devem ser traduzidas para o português do brasil;

3.1.7. Módulo de proteção Anti-malware para estações mac-os

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

3.1.7.2. Mac os x 10.9 e 10.10 em processadores 32 e 64 bits;

3.1.7.3. Suporte ao apple remote desktop para instalação remota da solução;

3.1.7.4. Gerenciamento integrado à console de gerência central da solução.

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

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

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

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

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

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

a) Windows Server 2008, 2008 R2 e 2012 (32/64-bit);
b) Windows vista (x86/x64);
c) Windows 7 (x86/x64);
d) Windows 8 e 8.1 (x86/x64);
e) 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. Deve permitir a varredura de portas logicas do sistema operacional para identificar quais estejam abertas e possibilitando trafego de entrada ou saída.

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

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

3.1.8.8. Deve efetuar varredura de segurança automática ou sob demanda que aponte vulnerabilidades de sistemas operacionais e aplicações e atribua automaticamente as regras de host ips para proteger a estação de trabalho ou notebook contra a possível exploração da vulnerabilidade;

3.1.8.9. A varredura de segurança deve ser capaz de identificar as regras de host ips que não são mais necessárias e desativá-las automaticamente;

3.1.8.10. Deve prover proteção 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;

3.1.8.11. Deve permitir a criação de políticas diferenciadas em múltiplas placas de rede no mesmo sistema operacional;

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

3.1.8.13. Deve permitir a emissão de alertas via SMTP e snmp;

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

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

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

3.1.8.17. Deve permitir a criação de regras de firewall pelos seguintes frames types: Ip, ipv4, ipv6, arp, revarp.

3.1.8.18. Deve permitir também escolher outros tipos de frame type de 4 dígitos em hex code;

3.1.8.19. Deve permitir a criação de grupos lógicos através de lista de ip, mac ou portas;

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

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

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

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

3.1.8.24. 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. Módulo para 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, 2008 R2 e 2012 (32/64-bit);
b) Windows Vista (x86/x64);
c) Windows 7 (x86/x64);
d) Windows 8 e 8.1 (x86/x64);
e) 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:

a) Nome parcial ou completo das estações de trabalho, permitindo a utilização de caractere coringa para identificação do nome parcial da máquina;
b) Range de endereços IPS;
c) Sistema operacional;

d) Grupos de máquinas espelhados do Active Directory;
e) Usuários ou grupos do Active Directory;

3.1.9.4. As políticas de segurança devem permitir a combinação lógica dos critérios para identificação do(s) alvo(s) de cada política;

3.1.9.5. As políticas de segurança devem permitir a definição dos logs que serão recebidos de acordo com os seguintes critérios:

a) Nenhum;
b) Somente bloqueios;
c) Somente regras específicas;
d) Todas as aplicações executadas;

3.1.9.6. As políticas de segurança devem permitir o controle do intervalo de envio dos logs;

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

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

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

3.1.9.10. As políticas de segurança devem permitir o controle do intervalo de quando os inventários de aplicações são executados;

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

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

a) Permissão de execução;
b) Bloqueio de execução;
c) Bloqueio de novas instalações;

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

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

a) Assinatura sha-1 do executável;
b) Atributos do certificado utilizado para assinatura digital do executável;
c) Caminho lógico do executável;
d) Base de assinaturas de certificados digitais válidos e seguros;

3.1.9.15. As regras de controle de aplicação devem possuir categorias de aplicações;

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

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

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

3.1.9.19. 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. Solução de Segurança para Proteção da camada de Servidores Virtuais e Físicos

4.1. A solução deverá ser licenciada para 350 (trezentos e cinquenta) ativos;

4.2. As licenças devem ser fornecidas com os módulos de Firewall, Inspeção de Pacotes, Controle de Acesso a Sites Maliciosos, Anti-malware, Monitoramento de Integridade e Controle de Aplicação, sem a necessidade de instalação de agente para ambiente VMWare v5.5 ou ambiente com NSX;

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

4.4. Características Gerais

4.4.1. 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;

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

4.4.3. A console de administração deverá permitir o envio de notificações via SMTP;

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

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

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

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

4.4.8. 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;

4.4.9. A solução precisa permitir que tarefas de criação de relatórios no formato PDF

4.4.10. A 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;

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

4.4.12. Quando operadas em modo alta disponibilidade, as consoles devem compartilhar a mesma database;

4.4.13. A 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;

4.4.14. 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";

4.4.15. 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;

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

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

4.4.18. Cada componente de proteção deverá ter sua própria chave para criptografia de modo que a comunicação seja criptografada de forma única;

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

4.4.20. Os componentes de atualização deverão buscar os updates das assinaturas e distribuí-las. Quando ocorrer a atualização, esta deverá ser feita de modo seguro, através de SSL com o servidor de atualização;

4.4.21. A console de gerenciamento deverá ser gerenciada por Internet Explorer, Chrome e Firefox;

4.4.22. Para efeito de administração, a solução deverá permitir a verificação do componente de proteção que não estiver conectado a sua console de gerenciamento;

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

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

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

4.4.26. Os componentes de proteção deverão ser capazes de executar rastreamento nas máquinas onde estão instalados e, após rastreamento, deverão fornecer uma lista de todas as recomendações de segurança para os softwares que estejam instalados nas máquinas bem como do sistema operacional, devendo permitir a implementação da proteção de forma automática e transparente, interrompendo somente o tráfego de rede malicioso;

4.4.27. Esses rastreamentos devem ocorrer de forma periódica a ser definida pelo administrador;

4.4.28. O administrador do sistema de segurança deverá ter a possibilidade de não aplicar automaticamente a proteção para as vulnerabilidades escolhendo o perfil ou o host;

4.4.29. Também deverá ser possível realizar o rastreamento por portas abertas, identificando possíveis serviços ativos e passivos;

4.4.30. 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;

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

4.4.32. 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;

4.4.33. 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;

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

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

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

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

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

4.4.39. A lista de contatos de recebimento de relatório poderá ser obtida através do Active Directory;

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

4.4.41. Após a atualização deve ser informado o que foi modificado ou adicionado;

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

4.4.43. A console de gerenciamento deve apresentar a capacidade de gerar roll back de suas atualizações de regras;

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

4.4.45. Deverá ter a capacidade de colocar etiquetas para a ocorrência de determinados eventos de modo a facilitar o gerenciamento, relatórios e visualização;

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

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

4.4.48. Possibilidade de customizar a escolha do serviço de Whois para a identificação dos IPs que estejam realizando ataques;

4.4.49. Deverá possibilitar o uso de etiquetas em eventos para visualização apenas dos eventos desejados;

4.4.50. Deverá medir o tempo de acesso a base de dados para efeitos de performance;

4.4.51. 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;

4.4.52. A 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 a console de gerenciamento da solução;

4.4.53. 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;

4.4.54. 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;

4.4.55. Este virtual appliance deverá integrar-se com as seguintes APIs VMware: VMSafe API e vShield Endpoint API, possibilitando que funcionalidades de Firewall, Proteção de Aplicações Web, Anti-malware, Controle de Acesso a Sites Maliciosos, Controle de Aplicações e IDS/IPS, possam ser efetuados diretamente via hypervisor e virtual appliance em conjunto, não necessitando a instalação de agentes adicionais de segurança do fabricante nos guests VMs protegidos;

4.4.56. Precisa ter a capacidade de detectar e aplicar as regras necessárias do módulo de IDS/IPS, para cada servidor, de forma automática e sem a intervenção do administrador;

4.4.57. Precisa ter a capacidade de desabilitar as regras não mais necessárias do módulo de IDS/IPS, na mesma tarefa de rastreamento que identifica as vulnerabilidades e recomendações de segurança para cada servidor, de forma automática e sem a intervenção do administrador;

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

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

4.4.60. 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, Web Reputation, Firewall, IDS/IPS, Monitoramento de Integridade, Log Inspection e Controle de Aplicações;

4.5. **Características para Firewall**

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

4.5.2. Precisa ter a capacidade de controlar o tráfego baseado no Endereço MAC, Frame types, Tipos de Protocolos, Endereços IP e intervalo de portas;

4.5.3. Precisa ter a capacidade de controlar conexões TCP baseado nas Flags TCP;

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

4.5.5. 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;

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

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

4.5.8. Precisa ter a capacidade de realização de varredura de portas nos servidores;

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

4.5.10. 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);

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

4.5.12. O firewall deverá ser stateful bidirecional;O firewall deverá permitir, liberar ou apenas logar eventos;

4.5.13. O firewall deverá permitir a criação de regras através do protocolo, origem do tráfego, frame type, tcp header flags, destino e direção;

4.5.14. As regras de Firewall deverão ter as seguintes ações, ou equivalentes: Allow, log only, bypass, force allow, deny;

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

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

4.5.17. Deverá realizar pseudo stateful em tráfego UDP;

4.5.18. Deverá logar a atividade stateful;

4.5.19. Deverá limitar o número de conexões entrantes de um determinado servidor;

4.5.20. Deverá limitar o número de conexões de saída para um determinado servidor;

4.5.21. Deverá limitar o número de meias conexões vindas de um servidor;

4.5.22. Deverá prevenir ack storm;

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

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

4.6. Características para Inspeção de Pacotes

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

4.6.2. 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;

4.6.3. 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;

4.6.4. Precisa conter 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.

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

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

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

4.6.8. 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;

4.6.9. Deverá permitir customização avançada e criação de novas regras de proteção de aplicações web, permitindo proteger contra vulnerabilidades específicas de sistemas web legados e/ou proprietários;

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

4.6.11. Regras de IDS/IPS poderão ser válidas de acordo com agendamento por horário ou dia da semana;

4.6.12. Deverá ser capaz de inspecionar tráfego incoming SSL;

4.6.13. Deverá inspecionar tráfego de aplicações Web em servidores buscando identificar: SQL Injection, Cross Site Scriptings, tamanho de URI fora de padrão, caracteres fora de padrão para requisição de URI, Double Decoding Exploit;

4.6.14. As regras de blindagem contra vulnerabilidades deverão conter links com referências externas, isto quando aplicável, explicando a vulnerabilidade do fabricante ou CVE relacionado, indicando quando aplicável o link para site onde está hospedado o patch de correção;

4.6.15. Deverá possibilitar a criação de regras manuais para o bloqueio de tráfego customizado. Como por exemplo bloquear acesso a um determinado website ou bloquear acesso de uma determinada aplicação;

4.6.16. Deverá possibilitar a criação de regras manuais baseadas em padrão XML, forma de assinatura ou padrões que possuam começo e fim coincidentes;

4.6.17. 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;

4.6.18. 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;

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

4.6.20. 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;

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

4.6.22. As regras de IPS poderão ter sua função de LOG desabilitada;

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

4.6.24. As regras devem ser atualizadas automaticamente pelo fabricante;

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

4.7. **Características para Controle de Acesso a Sites Maliciosos**

4.7.1. Deve permitir a proteção contra acesso a websites ou URLs consideradas maliciosas ou reputação ruim;

4.7.2. A lista de URLs deve ser fornecida e atualizada automaticamente pelo fabricante, permitindo a consulta em uma base local ou na nuvem da reputação das URLs acessadas;

4.7.3. Deve permitir a criação de listas de exclusão, permitindo que usuários acessem determinadas URLs especificadas pelo administrador do sistema;

4.7.4. A proteção deve suportar implementação sem a necessidade de instalação de agentes de segurança do fabricante da solução de segurança, através de integração com tecnologia VMware;

4.7.5. A solução de permitir o bloqueio de URLs com incidência de palavras chave definidas pelo administrador;

4.8. **Características para Anti-malware**

4.8.1. 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;

4.8.2. 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.;

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

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

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

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

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

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

4.8.9. A solução deve ter capacidade de monitorar documentos contra a criptografia não autorizada, a fim de detectar e bloquear Ransomware no ambiente;

4.8.10. Deve ser possível o envio automatizado de arquivos suspeitos para uma solução de sandbox;

4.8.11. Caso o arquivo suspeito seja detectado como potencialmente malicioso pela sandbox, a solução poder bloquear de forma automática a execução do mesmo em todo o ambiente de servidores protegidos;

4.8.12. Arquivos que sejam detectados como potencialmente maliciosos pela sandbox, mesmo que não enviados para análise pela solução, devem poder ser bloqueados de forma automática a sua execução em todo o ambiente de servidores protegidos;

4.8.13. A solução deve proteger Docker hosts;

4.8.14. Os hosts Docker devem ser gerenciados na mesma console, com um ícone diferenciado;

4.8.15. A solução deve proteger containers Docker com pelo menos Anti-malware e com módulo de IPS ;

4.9. **Características para Monitoramento de Integridade**

4.9.1. A solução deve permitir o monitoramento de integridade de arquivos sem a necessidade de instalação de agentes adicionais do fabricante na máquina virtual (VMWARE) a ser monitorada;

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

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

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

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

4.9.6. 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;

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

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

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

4.9.10. Deverá alertar toda vez que uma modificação ocorrer;

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

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

4.9.13. O monitoramento deverá ocorrer em real time ou sob demanda;

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

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

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

4.10. Características para Inspeção de Logs

4.10.1. A solução deve permitir a inspeção de logs do sistema com a necessidade de instalação de agentes adicionais do fabricante na máquina virtual (VMWARE) a ser monitorada;

4.10.2. Precisa ter a capacidade de monitorar e inspecionar arquivos de log do sistema operacional e demais aplicações, gravando uma cópia deste log em um banco de dados externo e notificando o administrador sobre eventos suspeitos;

4.10.3. Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de inspeção de logs de acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada;1Precisa permitir a criação de regras de inspeção de logs adicionais para auditoria de logs de aplicações terceiras;

4.10.4. Precisa permitir a customização de regras existentes, adicionando, removendo ou modificando regras de inspeção de logs;

4.10.5. Deverá rastrear e indicar/sugerir ao administrador do sistema quais softwares estão instalados e que possuem logs passíveis de inspeção;

4.10.6. Deverá possibilitar a criação de regras de inspeção de logs para aplicações customizadas;

4.10.7. Deverá ter inteligência para que a cada violação relevante no log inspecionado que possa comprometer a segurança do ambiente ou do servidor seja alertada;

4.10.8. Deverá ter inteligência para que a cada violação relevante no log inspecionado que seja suspeita no servidor seja alertada;

4.10.9. Deverá logar cada violação e colocar em relatório todas as violações relevantes que ocorram;

4.10.10. As regras poderão ser modificadas por severidade de ocorrência de eventos;

4.10.11. As regras devem se atualizar automaticamente pelo fabricante;

4.10.12. Permitir modificação pelo administrador em regras para adequação ao ambiente;

4.11. Características para Controle de Aplicação

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

4.11.2. Deve ter a capacidade de detectar, além de binários, arquivos Java, PHP, Python e shell scripts como aplicações;

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

4.12. Solução de inspeção avançada de tráfego

4.12.1. A solução deverá ser executada em Hardware e Software específicos (appliance ou solução de software + hardware homologado) contanto que o conjunto da solução seja suportado pela contratada. Todas as funcionalidades deverão ser executadas no mesmo equipamento;

4.12.2. Possuir no máximo 2U de altura e ser instalável em Rack padrão 19" e acompanhar ainda todos os trilhos necessários à sua instalação.

4.12.3. Possuir no mínimo 04 (quatro) discos rígidos de 1 TB (um Terabyte) cada;

4.12.4. Deverá suportar o funcionamento dos discos em padrão RAID 1+0;

4.12.5. Possuir no mínimo uma porta de gerenciamento padrão 10/100/1000 BASE-T RJ45.

4.12.6. Possuir no mínimo 4 portas de 1 Gbps padrão RJ45 ou SFP+ para conexão dos links de comunicação de dados a serem analisados, com respectivos transceivers.

4.12.7. A solução deverá suportar um throughput de análise de até 1000 Mbps;

4.12.8. Possuir fontes redundantes e hot swappable de no mínimo 750 watts, 50/60 HZ, 100 – 240VAC

4.12.9. A solução deverá ser gerenciada por console Web suportando no mínimo os browsers Internet Explorer e Firefox.

4.12.10. A solução deverá suportar a escalabilidade horizontal, permitindo que novas instâncias sejam habilitadas, aumentando sua capacidade de detecção e análise de tráfego;

4.12.11. A console de gerenciamento deverá ter dashboards para facilidade de monitoração. As janelas deverão ser customizadas pelo administrador em quantidade e período de monitoração;

4.12.12. Deverá permitir a customização das janelas de monitoramento no dashboard através de widgets, podendo o administrador livremente adicionar ou remover widgets de acordo com sua necessidade de visualização;

4.12.13. Deverá possuir mapa geográfico que permita a identificação visual sobre a origem de ameaças de modo a facilitar a visualização de eventos críticos para que ações imediatas sejam providenciadas;

4.12.14. Deverá possuir a capacidade de atualizar as vacinas, engines, assinaturas e recursos de inspeção de conteúdo de forma agendada e automática;

4.12.15. Deverá ser capaz de identificar ameaças evasivas em tempo real com o provimento de análise profunda e inteligência para identificar e prevenir ataques;

4.12.16. Deverá possuir capacidade de identificar a origem de ataques direcionados, incluindo a analise de artefatos por meio de analisador virtual com a capacidade de gerar internamente no mínimo 24 máquinas virtuais de análise;

4.12.17. Deverá ser capaz de correlacionar regras de detecção de conteúdo malicioso durante todas as fases de um ataque;

4.12.18. A solução deverá permitir a geração de logs e integração com SYSLOG Servers e deverá conter no mínimo:

a) Tipo de evento de detecções: Conteúdo malicioso, reputação de URL's, comportamentos maliciosos, comportamentos suspeitos, Exploits, correlações de eventos, Grayware;
b) Tipo de eventos de sistemas: Eventos de sistema e eventos de atualizações.

4.12.19. Deverá possuir capacidade de entregar relatório contendo informações da sequência de execução do artefato malicioso, assim como, detalhes de alterações locais da máquina, conexões externas e envio da informação para fora da rede corporativa;

4.12.20. A solução deve prover serviço de agregação e correlação de logs de eventos de segurança possibilitando coleta de fontes de monitoração para proporcionar informação e identificação de ameaças digitais conhecidas e desconhecidas em transito através de logs de sensor;

4.12.21. Solução deverá apresentar relatórios customizados de todas as suas funcionalidades e deverá conter no mínimo: Computadores infectados; Origem de infecções; Estatísticas de ameaças; Riscos potenciais de segurança; Risco de sistema comprometido; Risco de disseminação de ameaças; Eventos suspeitos; Infecções de malware.

4.12.22. A solução deverá apresentar função de pesquisa por logs contendo no mínimo:

a) Critérios de pesquisa por dia, mês e ano;
b) Possibilidade de pesquisa pelo nome do computador, domínio ou conta, endereço IP, endereço MAC e grupos;
c) Possibilidade de pesquisa por ameaças, URL's maliciosas, análises virtuais, correlação de incidentes, nome de malwares, protocolo e direção da detecção;

4.12.23. A solução deverá ser capaz de suportar a retenção de logs por no mínimo 120 dias;

4.12.24. A solução deverá permitir exportar Logs nos formatos PDF ou CSV;

4.12.25. A solução deverá suportar a geração de logs, no mínimo, nos padrões CEF Common Event Format (CEF) e LEEF Log Event Extended Format (LEEF);

4.12.26. Deverá permitir a monitoração de tráfego atuando na identificação de ameaças avançadas e permitindo a mitigação de riscos complementando a inspeção feita pelos mecanismos tradicionais de segurança (Firewall/IPS/IDS).

4.12.27. Deverá permitir a visibilidade de incidentes de segurança motivados por conexões da rede interna com sites maliciosos ou servidores de central de comando (C&C) externos além da detecção de malwares conhecidos e desconhecidos, Ransomware, Exploits, Botnets, Cross Site Script, SQL Injection, comunicações p2p, instant messengers; streaming, tentativas de scan de rede, tentativas de brute-force, situações de evasão e roubo de informação etc.;

4.12.28. Deverá permitir a criação de filtros para visualização de eventos específicos conforme contexto, localização e outras variáveis que permitam investigação profunda sobre causa raiz de incidentes de segurança;

4.12.29. Deverá permitir a customização de alertas em base ao tipo de incidente de segurança através da console de gerenciamento;

4.12.30. Deverá ter capacidade de verificar em tempo real a reputação de endereços web (URL's) e servidores de correio SMTP;

4.12.31. Capacidade de criar e salvar investigações customizadas dos incidentes de segurança;

4.12.32. Deverá permitir a integração nativa com firewalls de mercado: tais como Checkpoint para que através desta integração seja possível enviar ao equipamento de firewall requisições de ações dependendo do nível de criticidade do conteúdo malicioso detectado;

4.12.33. Deverá possuir a capacidade de detectar ameaças direcionadas, realizando inspeção de tráfego até a camada 7 de forma a prevenir ataques do dia zero e executar análise profunda de documentos que contenham conteúdo malicioso ou redirecionamentos para outras URL's maliciosas;

4.12.34. Deverá possuir a habilidade de detectar e analisar até 100 protocolos e aplicativos, entre eles: P2P, SMTP, POP3, IRC, DNS, HTTP, FTP, TFTP, SMB, MSN, AIM, YMSG, Yahoo Mail, Hotmail, RDP, DHCP, TELNET, File Transfer, VNC, Cisco-TELNET, Kerberos, DCE-RPC, SQL, HTTPS, SMB2, MMS, IMAP4, RTSP/RTP-UDP, RTSP/RTP-TCP, RTSP/RDT-UDP, RTSP/RDT-TCP, WMSP, RTMP, Bittorent, Kazaa, eDonkey_eMule, Gnutella/Limewire/Bearshare/Shareaza, Skype, Google Talk, eDonkey, AIM Express, eBuddy, ICQ2Go, ILoveIM Web Messenger, meebo, Yahoo Web Messenger, IP, ARP, TCP, UDP e IGMP, etc.

4.12.35. Deverá possuir capacidade de disponibilizar facilmente as amostras dos arquivos suspeitos detectados e do arquivo PCAP do contexto de captura;

4.12.36. Capacidade de identificar artefatos maliciosos direcionados para dispositivos moveis rodando o sistema operacional Android, tais como telefones inteligentes e tablets;

4.12.37. Deverá analisar em tempo real o comportamento através de simulação de execução de arquivos provenientes do tráfego de rede incluindo arquivos PDF´s, executáveis, PPT, DOC, XLS, ZIP e RAR;

4.12.38. Deverá possuir tecnologia de análise de arquivos binários através de simulação e avaliação de execução dos artefatos suspeitos para identificação de comportamento malicioso, com capacidade de operar vários ambientes simultâneos e integrados a solução para processamento de alto desempenho;

4.12.39. Deverá permitir o uso de base de conhecimento na Internet do próprio fabricante, com atualização automática de regras e assinaturas, para consultas automáticas em bases de reputação e correlacionamento de informações sobre ameaças conhecidas, identificando assim as respectivas recomendações de ações;

4.12.40. Deverá permitir o uso de portas espelhadas de switch (mirror port) para monitorar o tráfego e detectar potenciais riscos a Segurança;

4.12.41. Deverá possuir suporte para monitorar múltiplas interfaces de rede conectadas a diferentes VLANs ou Switches;

4.12.42. Deverá permitir o rastreio por malwares utilizando métodos de detecção baseados no tipo de arquivo (True File Type), múltiplas camadas de empacotamento (Multi-packed/Multi-layered files) e arquivos comprimidos(compactados);

4.12.43. Deverá analisar arquivos maliciosos na rede utilizando vacinas e técnicas de heurística.

4.12.44. Deverá possuir suporte para balanceamento de carga no sensor de inspeção de tráfego, possibilitando assim obter uma melhor performance;

4.12.45. Deverá ser capaz de identificar movimentos laterais em uma rede corporativa;

4.12.46. Deverá identificar por comportamento ameaças do tipo Ransomware

4.12.47. Deverá identificar e executar arquivos de scripts no formato Visual Basic e Javascript inclusive quando estiverem obfuscadas

4.12.48. Deverá atuar de forma passiva na captura de tráfego sem oferecer impacto no desempenho da rede;

4.12.49. Deverá possuir capacidade de envio de artefatos para o analisador virtual dedicado, que deverá suportar no mínimo os sistemas operacionais Windows 7, Windows 8 e Windows 10.

4.12.50. Deverá permitir a habilitação e desabilitação de regras de inspeção, individualmente, através de interface de gerenciamento web.

4.12.51. Deverá possuir regras que identifiquem comunicações de estações de trabalho e servidores com serviços não autorizados, tais como: consultas DNS em servidor não autorizado, utilização de SMTP server não autorizado, Proxy Server não autorizado;

4.12.52. Deverá possuir capacidade de geração de relatórios executivos e detalhados com no mínimo as seguintes informações:

a) Visão Geral dos Incidentes de Segurança;
b) Discriminação dos Tipos de Incidentes;
c) Top Ameaças Analisadas;
d) Top Hosts Infectados;
e) Recomendações de Segurança
f) Detalhamento técnico dos incidentes detectados
g) Estatística do tráfego analisado;
h) Indicadores de risco do ambiente;
i) Resultado das análises de sandbox.

4.12.53. Deve ser capaz de identificar, filtrar e exibir em interface gráfica, e dinamicamente atualizada, hosts com alto nível de risco, classificando os tipos de riscos/eventos detectados. A classificação de risco deve ser em no mínimo 10 níveis, porém agrupadas de acordo com a sua severidade.

4.12.54. Quando detectada uma ameaça, a solução deve prover informações sobre a ameaça, família da ameaça, estatísticas de segmentos de mercado afetados e recomendações de segurança para eliminar a ameaça, correlacionando estas informações com sites ou outros vetores por onde esta ameaça é disseminada;

4.12.55. Deverá possibilitar customização de Sandbox, permitindo ao cliente simular seu padrão de imagens e sistemas operacionais no módulo de análise virtual;

4.12.56. Deverá ser capaz de detectar tentativas de mascaramento ou evasão de detecção através do uso de portas comuns ou protocol tunneling;

4.12.57. Dever permitir busca por informações do destino e origem, incluindo estas: endereço IP, endereço MAC, porta e protocolo;

4.12.58. Capacidade de salvar uma investigação e de restaurá-la para dar continuidade ou consultá-la;

4.12.59. Deve sugerir consultas a bases de reputação e whois quando encontrados hosts e nomes de domínio;

4.12.60. Deve permitir investigação por tags (palavras-chave) pré-configuradas para facilitar a busca de eventos;

4.12.61. Deve permitir a configuração de alarmes personalizados, com base em investigações e ainda o envio de alertas via e-mail;

4.13. CARACTERÍSTICAS DO MÓDULO DE ANÁLISE VIRTUAL

4.13.1. A solução deverá ser executada em Hardware e Software específicos (appliance ou solução de software + hardware homologado) contanto que o conjunto da solução seja suportado pela contratada e que a análise em sandbox seja feita localmente (sem o envio de artefatos para nuvem do fabricante). Todas as funcionalidades deverão ser executadas no mesmo equipamento;

4.13.2. Possuir no máximo 2U de altura e ser instalável em Rack padrão 19" e acompanhar ainda todos os trilhos necessários à sua instalação;

4.13.3. A solução deverá suportar o uso de imagens virtuais para análise em sandbox de no mínimo 20 GB;

4.13.4. A solução deverá suportar até 3 imagens de sandbox diferentes com até 20 instâncias de cada, perfazendo um total de 60 instâncias;

4.13.5. Deverá suportar IPV4 e IPV6;

4.13.6. Devera suportar análise de, no mínimo, documentos do Microsoft Office 2013 (DOC, DOCX, XLS, XLSX, PPT, PPTX) e documentos PDF;

4.13.7. Deverá suportar múltiplos idiomas nas imagens de sistema operacional da sandbox sendo no mínimo, português (brasileiro) e inglês (americano) os idiomas suportados;

4.13.8. Deve permitir a criação de sandbox local utilizando, no mínimo, os seguintes sistemas operacionais: Windows XP 32-bits, Windows 7 32/64-bits, e Windows 8 32/64-bits, Windows Server 2003 e Windows Server 2008;

4.13.9. Deve submeter uma mesma amostra a sistemas operacionais diferentes, a fim de detectar ações específicas para cada sistema;

4.13.10. Deverá permitir a avaliação dos artefatos em sandbox com capacidade de execução simultânea em imagens de diferentes sistemas operacionais para processamento de alto desempenho;

4.13.11. Deverá possuir tecnologia de gerenciamento de máquinas virtuais proprietárias de execução local para verificação positiva de Malwares;

4.13.12. Deve permitir que seja customizada a versão do sistema operacional e dos softwares que fazem parte das imagens de sandbox que serão utilizadas para efetuar a detecção de APTs;

4.13.13. Deve permitir a utilização das matrizes de sistema operacional da contratante para detecção de APTs;

4.13.14. Deve analisar dinamicamente arquivos compactados (ZIP, BZIP2, RAR), binários PE de 32-bits e de 64-bits, bibliotecas dinâmicas (DLL), rootkits, arquivos do Adobe Flash (SWF) e Binários BHO;

4.13.15. Deverá permitir o isolamento total da rede de sandbox da rede de gerência;

4.13.16. Deverá realizar a análise localmente podendo ter consultas externas para reputação de IP e URL, mas sem envio da amostra;

4.13.17. Deverá ser capaz de gerar relatórios com eventos realizados pela amostra no sistema operacional testado, exibindo as funções com argumentos e retornos de execução;

4.13.18. Caso uma ameaça baixe outra enquanto na sandbox, essa também deverá ser analisada num evento correlacionado;

4.13.19. Deverá identificar e executar arquivos de scripts no formato Visual Basic e Javascript inclusive quando estiverem ofuscadas.

4.14. CONSOLE DE GERENCIAMENTO

4.14.1. A solução deverá ser fornecida em forma de licenças de software e suportar a instalação do servidor na plataforma Windows 2008 Server ou superior, seja o servidor físico ou virtual;

4.14.2. A solução deverá possuir console única capaz de consolidar informações coletadas dos módulos de Anti-malware, AntiSpam, filtro web, proteção de servidores e inspeção avançada de tráfego de forma centralizada;

4.14.3. A ferramenta de gerência deverá ser acessada por console Web suportando no mínimo os browsers Internet Explorer, Chrome e Firefox.

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

4.14.5. Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS:

4.14.6. Deve possuir integração com Microsoft Active Directory;

4.14.7. Implementar base de usuários local e consulta a base de usuários externa através do protocolo LDAP;

4.14.8. Deve gerenciar logs das atividades e eventos gerados pela solução;

4.14.9. Deve permitir a criação de políticas genéricas aplicáveis a grupos de máquinas, ou aplicáveis a grupos de usuários.

4.14.10. Implementar no mínimo 02 (dois) níveis de administração distintos (administrador e usuário);

4.14.11. Implementar através da interface gráfica, seleção dos níveis e módulos de geração de log, tais como: log de autenticação de usuário, log de uso da Interface Gráfica, log da atividade relacionada ao hardware, log do mecanismo de health-check e log da base de dados;

4.14.12. Implementar através da interface gráfica mecanismo para configuração de notificações dos alertas;

4.14.13. Implementar através da interface gráfica mecanismo de atualização da base de dados e de firmware da solução;

4.14.14. Implementar através da interface gráfica mecanismo de Dashboard onde seja possível a visualização das seguintes informações ou similares: Sumário de detecção e proteção, gráfico de top infecções, e gráfico do throughput de tráfego monitorado;

4.14.15. Deverá permitir a geração de relatórios e gráficos parametrizáveis nos formatos html, pdf, xml e csv;

4.14.16. Deve permitir criação de modelos de relatórios customizados;

4.14.17. Deve permitir pesquisas personalizadas para a consulta de eventos (logs) através de categorias;

4.14.18. Deve permitir logon via single sign-on com os demais produtos da solução;

4.14.19. Deve permitir diferentes níveis de administração, de maneira independente do login da rede;

4.14.20. Deve permitir pesquisas personalizadas para a consulta de eventos (logs), através de critérios lógicos, com base em todos os campos pertencentes aos eventos consultados;

4.14.21. Deve permitir a configuração da manutenção dos registros de eventos (logs), com base no intervalo de tempo que devem ser mantidos e no número máximo de registros, por tipo de evento;

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

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

a) Nome parcial ou completo das estações de trabalho, permitindo a utilização de caractere coringa para identificação do nome parcial da máquina;
b) Range de endereços IPS;
c) Sistema operacional;
d) Agrupamentos lógicos dos módulos;

4.14.24. As políticas de segurança devem permitir a combinação lógica dos critérios para identificação do(s) alvo(s) de cada política;

4.14.25. Deve permitir visualização de eventos de violação de segurança de todos os módulos gerenciados, agrupado por usuário numa linha de tempo configurável;

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

4.14.27. Deve possuir repositório central de identificadores de dados, que podem ser utilizados para a criação de políticas contra possíveis vazamentos de informações;

4.14.28. Deve permitir a investigação de incidentes de vazamento de informação através de um número identificador de incidentes;

4.15. **Funcionalidades do Anti-malware**

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

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

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

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

4.15.5. Deve possuir engine do antivírus comprovada por pelo menos 6 anos consecutivos de êxito nos testes realizados pelo instituto "Vírus Bulletin" (www.virusbtn.com) - VB100 Award;

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

5. OPERAÇÃO ASSISTIDA (45 dias)

5.1. A prestação do serviço de Operação Assistida compreende a organização, desenvolvimento, implantação, parametrização, migração, apoio ao gerenciamento, suporte técnico, execução, operação e monitoramento continuado do ambiente de Segurança dos Endpoints e dos Servidores;

5.2. A prestação do serviço de Operação Assistida será realizada de forma presencial nas instalações da Iplanrio, de segunda à sexta-feira, das 09:00 às 18:00h;

6. TREINAMENTO

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

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

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

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

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

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

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

6.7. 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 da Lei 8.666/93), poderá ser dispensada a assinatura do termo contratual, que será substituído pela Nota de empenho.

7. PRAZOS

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

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

7.3. O prazo de execução dos serviços de Operação Assistida será de 45 (quarenta e cinco) dias contados a partir da entrega/disponibilização das licenças de todas as licenças para a CONTRATANTE.

7.4. O prazo do Suporte Técnico descrito neste TR corresponderá ao prazo de vigência contratual, tendo início na entrega/disponibilização das licenças para a CONTRATANTE.

7.5. 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.

8. DA FISCALIZAÇÃO E DO ACEITE

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 (a) 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 (a) 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 (a) CONTRATANTE, ou perante terceiros, do mesmo modo que a ocorrência de eventuais irregularidades na execução dos serviços contratados não implicará corresponsabilidade do (a) CONTRATANTE ou de seus prepostos.

8.6. A aceitação do objeto deste contrato se dará mediante a avaliação da Comissão de Fiscalização prevista no subitem 8.2, que constatará se os serviços atendem a todas as especificações contidas no Edital e seus Anexos, e na Proposta que ensejou a presente contratação.

8.6.1. O Aceite Provisório ficará a cargo da Comissão de Aceitação que emitirá Termo de Aceitação Provisória em até 5 (cinco) dias após a entrega da solução instalada e configurada.

8.6.2. indicada nos subitens 8.2 e 8.6 somente emitirá o aceite do serviço de treinamento prestado após parecer favorável da Coordenadoria Técnica de Pessoas – CTP, que constatará se o serviço de treinamento atende a todas as especificações contidas neste Termo de Referência, emitido após atendida a condição prevista no item 8.6.1.

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

8.6.4. Na recusa de aceitação, por não atenderem às exigências da contratante, o fornecedor deverá reexecutar os serviços com outro instrutor de expertise técnica igual ou superior à exigida no TR, passando a contar os prazos para pagamento e demais compromissos a partir da data da efetiva aceitação.

8.7. Os serviços prestados em desacordo com a especificação do Edital e seus Anexos, 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.

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

9. QUALIFICAÇÃO TÉCNICA

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

9.2. 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.

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

9.4. Será admitida a soma dos atestados ou certidões apresentados pelas licitantes, desde que os mesmos sejam tecnicamente pertinentes e compatíveis em características, quantidades e prazos com o objeto da licitação.

10. OBRIGAÇÕES DA CONTRATADA

10.1. Deverá realizar os serviços de acordo com todas as exigências contidas no Termo de Referência.

10.2. Deverá tomar as medidas preventivas necessárias para evitar danos a terceiros, em consequência da execução dos serviços.

10.3. Deverá 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.

10.4. Deverá atender às determinações e exigências formuladas pela CONTRATANTE;

10.5. Deverá substituir, por sua conta e responsabilidade, os serviços recusados pela CONTRATANTE no prazo determinado pela Fiscalização;

10.6. 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.

10.7. Deverá manter as condições de habilitação e qualificação exigidas para a contratação durante todo prazo de execução contratual;

10.8. Deverá 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;

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

10.10. Deverá 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.

10.11. Deverá 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.

10.12. Deverá 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.

10.13. Deverá entregar as licenças oficiais dos produtos contratados, no prazo máximo de 15 (quinze) dias corridos, após a assinatura do contrato.

10.14. Deverá emitir um relatório oficial de consumo de licenças da contratante (Empresa Municipal de Informática S.A. – IPLANRIO), a cada 12 (doze) meses, que deverá ser enviado a Responsável Técnica até o dia 10 do mês seguinte ao final do trimestre.

10.15. Deverá comprovar que os profissionais alocados na prestação de serviços de instalação, configuração e Operação Assistida possuem certificação na solução ofertada.

10.16. comprovar que os instrutores possuem certificação na solução ofertada referente ao curso que forem ministrar.

10.17. Deverá ministrar o treinamento de acordo com as especificações contidas no item (item treinamento a ser incluso nos moldes utilizados pela Central de Gestão de Pessoas);

10.18. Deverá disponibilizar, no ato da contratação, instrutor(es), monitor(es) ou consultor(es) alocado(s) aos serviços de treinamento objeto deste Termo de Referencia.

10.19. Deverá disponibilizar local e infraestrutura de acordo com as especificações contidas no item (item treinamento a ser incluso nos moldes utilizados pela Central de Gestão de Pessoas) para a realização de treinamento;

10.20. Deverá 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.

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

10.22. Deverá emitir certificados de conclusão para cada servidor participante no final de cada curso;

10.23. Deverá designar um profissional que será responsável pela coordenação do serviço de treinamento;

10.24. Deverá 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;

10.25. 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.

10.26. A contratada deverá apresentar, no momento da assinatura do contrato, documento comprovando ser uma empresa credenciada junto fabricante da solução ofertada e que está autorizada a comercializar os produtos objeto desta contratação.

11. SUPORTE TÉCNICO

11.1. O suporte técnico relativo às subscrições adquiridas deverão contemplar a atualização de versão (upgrades) para novas versões ou patches e suporte técnico, publicadas durante o período de vigência do contrato, sem ônus para a CONTRATANTE.

11.2. Para as subscrições do objeto 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. O Suporte Técnico deverá ser prestado diretamente pelo fabricante da solução ofertada.

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

11.4. A CONTRATADA deverá disponibilizar e-mail e solução web para pesquisa em base de conhecimento de soluções de problemas e documentos técnicos da solução ofertada.

11.5. No caso das subscrições a CONTRATADA terá o prazo máximo de 01 (uma) hora, a partir da abertura do chamado técnico, para resposta a incidentes críticos e o prazo máximo de 04 (quatro) horas para resposta a incidentes normais.

11.6. Definem-se como incidentes críticos aqueles que tornam indisponível algum serviço daqueles homologados pelo fabricante da solução para a subscrição em uso pela CONTRATANTE.

11.7. Definem-se como incidentes normais aqueles que não são críticos.

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

12. SANÇÕES ADMINISTRATIVAS

12.1. Pelo descumprimento total ou parcial do Contrato, a CONTRATANTE poderá, sem prejuízo responsabilidade civil e criminal que couber, aplicar as seguintes sanções, previstas nos artigos 7º da Lei Federal 10.520/02 e 87 da Lei Federal n° 8.666/93 e art. 589 do RGCAF:

12.2. Pelo descumprimento total ou parcial da Ata de Registro de Preços ou do Contrato, o Órgão Gerenciador e os(as) CONTRATANTES, respectivamente, poderão, sem prejuízo responsabilidade civil e criminal que couber, aplicar as seguintes sanções, previstas nos artigos 7º da Lei Federal nº 10.520/02 e 87 da Lei Federal n° 8.666/93 e art. 589 do RGCAF:

(a) Advertência;

(b) Multa de mora de até 1% (um por cento) por dia útil sobre o valor do Contrato ou do saldo não atendido do Contrato;

(c) Multa de até 20% (vinte por cento) sobre o valor do Contrato ou do saldo não atendido do Contrato, conforme o caso, e, respectivamente, nas hipóteses de descumprimento total ou parcial da obrigação, inclusive nos casos de rescisão por culpa da CONTRATADA;

(d) Suspensão temporária de participação em licitação e impedimento de contratar com a Administração por prazo não superior a 02 (dois) anos;

(e) Declaração de inidoneidade para licitar ou contratar com a Administração Pública pelo prazo de até 5 (cinco) anos.

12.3. As sanções previstas nas alíneas “a”, “d” e “e” do item 12.2 poderão ser aplicadas juntamente com aquelas previstas nas alíneas “b” e “c” do item 10.6, e não excluem a possibilidade de rescisão unilateral do Contrato.

12.4. A sanção prevista na alínea “e” do item 12.2 poderá também ser aplicada às licitantes que, em outras licitações e/ou contratações com a Administração Pública Direta ou Indireta de qualquer nível federativo, tenham:

(a) Sofrido condenação definitiva por praticarem, por meios dolosos, fraudes fiscais no recolhimento de quaisquer tributos;

(b) Praticados atos ilícitos, visando a frustrar os objetivos da licitação

(c) Demonstrado não possuir idoneidade para contratar com a Administração Pública, em virtude de outros atos ilícitos praticados.

12.5. As multas previstas nas alíneas “b” e “c” do item 12.2 não possuem caráter compensatório, e, assim, o pagamento delas não eximirá a CONTRATADA de responsabilidade pelas perdas e danos decorrentes das infrações cometidas.

12.6. As multas aplicadas poderão ser compensadas com valores devidos à CONTRATADA mediante requerimento expresso nesse sentido.

12.7. Ressalvada a hipótese de existir requerimento de compensação devidamente formalizado, nenhum pagamento será efetuado à CONTRATADA antes da comprovação do recolhimento da multa ou da prova de sua relevação por ato da Administração, bem como antes da recomposição do valor original da garantia, que tenha sido descontado em virtude de multa imposta, salvo decisão fundamentada da autoridade competente que autorize o prosseguimento do processo de pagamento.

13. DA GARANTIA CONTRATUAL

13.1. A CONTRATADA prestará garantia de 2% (dois por cento) do valor total do Contrato, como determina o art. 457 do RGCAF, a ser prestada antes do ato de assinatura, em uma das modalidades previstas no art. 445 do RGCAF e no art. 56, § 1º, da Lei Federal nº 8.666/93. Seus reforços poderão ser igualmente prestados nas modalidades previstas no § 1º do art. 56 da Lei Federal nº 8.666/93.

13.2. 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.

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

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

13.5. A não observância do prazo estabelecido no subitem 11.1.3 caracteriza o descumprimento total da obrigação assumida, sujeitando a licitante vencedora às penalidades legalmente estabelecidas.

13.6. O (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.

13.7. 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.

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

13.9. 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 deste.

13.10. Caso o valor do Contrato seja alterado, de acordo com o art. 65 da Lei Federal nº 8.666/93, a CONTRATADA deverá complementar o valor da garantia para que seja mantido o percentual de 2% (dois por cento) do valor do Contrato.

13.11. 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.

13.12. Os reforços do valor da garantia poderão ser igualmente prestados em uma das modalidades previstas no art. 56, § 1º, da Lei Federal nº 8.666/93.

13.13. 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.

14. DA PROPOSTA DE PREÇOS

14.1. 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.

14.2. A proposta de preços deve ser apresentada nos moldes praticados pelo Município do Rio de Janeiro.

15. LOCAL DA ENTREGA E EXECUÇÃO DOS SEVIÇOS

15.1. 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.

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

a) Os serviços de instalação, configuração, suporte técnico 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 CONTRATADA com observância do item 6.

16. TIPO DE LICITAÇÃO

Menor preço global.

17. CONDIÇÕES DE PAGAMENTO

17.1. Os pagamentos serão efetuados à CONTRATADA, após a regular liquidação da despesa, nos termos do art. 63 da Lei Federal nº 4.320/64, observado o disposto no art. 73 da Lei Federal nº 8.666/93.

17.2. Os pagamentos serão realizados de forma mensal (forma de pagamento está sob revisão do setor técnico que estuda a hipótese de fracionar os aceites e as notas fiscais).

17.3. Os pagamentos serão efetuados à CONTRATADA, de acordo com os itens 12.2 e 12.3 deste TR, após a regular liquidação da despesa, nos termos do art. 63 da Lei Federal nº 4.320/64, observado o disposto no art. 73 da Lei Federal nº 8.666/93.

17.4. O documento de cobrança será apresentado à Fiscalização, para atestação, e, após, protocolado no setor pertinente da Empresa Municipal de Informática S/A – IPLANRIO.

17.5. O prazo para pagamento será de 30 (trinta) dias, contados da data do protocolo do documento de cobrança no setor pertinente da Empresa Municipal de Informática S/A - IPLANRIO e obedecido o disposto na legislação.

17.6. No caso de erro nos documentos de cobrança, estes serão devolvidos à CONTRATADA para retificação ou substituição, passando o prazo de pagamento a fluir, então, da reapresentação válida desses documentos.

17.7. 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.

17.8. O pagamento à CONTRATADA será realizado em razão dos serviços efetivamente prestados e aceitos no período-base mencionado no item anterior sem que a Empresa Municipal de Informática S/A – IPLANRIO esteja obrigada a pagar o valor total do Contrato.

17.9. 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, na forma do Anexo que integrará o Edital.

17.10. 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 Empresa Municipal de Informática S/A - IPLANRIO e a data do efetivo pagamento.

17.11. 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 Empresa Municipal de Informática S/A – IPLANRIO.

17.12. O pagamento será efetuado à CONTRATADA através de crédito em conta bancária do fornecedor cadastrado junto à Coordenação do Tesouro Municipal, conforme o disposto na Resolução SMF n.º 2.754, de 17.01.2013, efetuados em c/c aberta no Banco SANTANDER (Brasil) S.A, conforme Contrato n.º 103/2011, publicado no D.O Rio n.º 195, de 26/12/2011, decorrente da licitação CEL/SMF – PP 01/11, ou em outro Banco que venha a substituí-lo, nos conformes legais.

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. DA SUBCONTRATAÇÃO

19.1. Será admitida a subcontratação na parte dos serviços de Operação Assistida não podendo ultrapassar 30% do objeto global licitado.

Rio de Janeiro, 17 Outubro de 2017.

Mark David Nicodem
Técnico de Processamento de Dados
Gerência de Infraestrutura e Telecomunicações
Diretoria de Operações

Jorge Francisco Antunes
Gerência de Infraestrutura e Telecomunicações
Diretoria de Operações
IPLANRIO

Márcia Cristina de Castro Marques
Diretoria de Operações
IPLANRIO