2.2.27.21.4. Código de patrimônio se estiver cadastrado na BIOS;

2.2.27.21.5. Fabricante, versão e data da BIOS e informações da SMBIOS;

2.2.27.21.6. *Slots* de memória disponíveis;

2.2.27.21.7. Sistema operacional, pasta de instalação, *service pack*, versão, idioma, fuso horário;

2.2.27.21.8. *Patches* e *hotfixes* do sistema operacional e *softwares*;

2.2.27.21.9. Dispositivos configurados e respectivas configurações;

2.2.27.21.10. Drivers;

2.2.27.21.11. Endereço Mac;

2.2.27.21.12. Configurações TCP/IP de todas as placas de rede incluindo virtuais;

2.2.27.21.13. Indicação de endereço IP: fixo ou dinâmico;

2.2.27.21.14. Discos e pastas da rede mapeados;

2.2.27.21.15. Impressoras instaladas, compartilhadas e mapeadas pela rede;

2.2.27.21.16. Discos físicos e lógicos incluindo letras atribuídas, tamanho e propriedades;

2.2.27.21.17. Tamanho total em disco, total livre, na lixeira, em pastas temporárias e cache;

2.2.27.21.18. Particionamento dos discos e formato FAT ou NTFS;

2.2.27.21.19. Discos e pastas compartilhadas e respectivo acessos;

2.2.27.21.20. Status de compartilhamento administrativo;

2.2.27.21.21. Membros do grupo administração local;

2.2.27.21.22. Perfis de usuários existentes no computador;

2.2.27.21.23. Verificar grupos locais no computador;

2.2.27.21.24. Tarefas agendadas no sistema operacional;

2.2.27.21.25. Histórico de conexões à porta USB a qualquer horário;

2.2.27.21.26. *Softwares* registrados no Painel de Controle, incluindo ocultos;

2.2.27.21.27. *Softwares* residentes no computador independente de estarem instalados ou presentes no Painel de Controle;

2.2.27.21.28. Conexões ODBC de sistema;

2.2.27.22. Inventário de pelo menos os seguintes tipos de informação de computadores Mac:

2.2.27.22.1. Processador, quantidade, velocidade e tipo/marca;

2.2.27.22.2. Fabricante do *hardware*, modelo, número de série;

2.2.27.22.3. Código de patrimônio se estiver cadastrado no equivalente à BIOS;

2.2.27.22.4. Impressoras instaladas, compartilhadas e mapeadas pela rede;

2.2.27.22.5. Discos físicos e lógicos, tamanho e propriedades;

2.2.27.22.6. Tamanho total em disco, total livre, na lixeira, em pastas temporárias e cache;

2.2.27.22.7. Discos e pastas compartilhadas e respectivo acessos;

2.2.27.22.8. Status de compartilhamento administrativo;

2.2.27.22.9. Membros do grupo administração local;

2.2.27.22.10. Perfis de usuários existentes no computador;

2.2.27.22.11. Verificar grupos locais no computador;

2.2.27.22.12. Tarefas agendadas no sistema operacional;

2.2.27.22.13. Histórico de conexões à porta USB a qualquer horário;

2.2.27.22.14. *Softwares* instalados no computador, incluindo ocultos;

2.2.27.22.15. *Softwares* residentes no computador;

2.2.27.23. Inventário de pelo menos os seguintes tipos de informação de dispositivos com iOS e Android:

2.2.27.23.1. Processador, velocidade e tipo/marca;

2.2.27.23.2. Quantidade de memória disponível;

2.2.27.23.3. Sistema operacional, versão, idioma, fuso horário;

2.2.27.23.4. *Patches* e *hotfixes* do sistema operacional e *softwares*;

2.2.27.23.5. Endereço Mac;

2.2.27.23.6. Configurações TCP/IP;

2.2.27.23.7. *Softwares* instalados no dispositivo;

2.2.27.24. Fornecer informações sobre as mudanças que ocorrem em todas as estações de trabalho e servidores;

2.2.27.25. Manter histórico sobre quaisquer instalações e desinstalações de *software*, bem como sobre adições e remoções de *hardware* que ocorreram nas estações de trabalho e servidores;

2.2.27.26. Agrupamentos pré-definidos de *softwares* em suítes e grupos (ex: Microsoft Office, *browsers* e antivírus) com possibilidade de inclusões, alterações e exclusões pelo administrador inclusive para sistemas desenvolvidos internamente;

2.2.27.27. Funcionalidade de catálogo de *software* descrita na metodologia ITIL, possibilitando o cadastro de:

2.2.27.27.1. Pacotes de *software* instalados;

2.2.27.27.2. Pacotes passíveis de distribuição pela ferramenta;

2.2.27.27.3. Dependência e substituição de pacotes;

2.2.27.27.4. Mecanismo de detecção da instalação do *software*;

2.2.27.27.5. Tarefas de instalação e remoção;

2.2.28. Gerenciamento de Contratos e Uso de Softwares

2.2.28.1. Atribuição dos contratos aos respectivos computadores gerenciados;

2.2.28.2. Identificação de computadores sem contratos;

2.2.28.3. Identificação de *softwares* instalados versus usados versus licenciados;

2.2.28.4. Gestão de licenças de *software*;

2.2.28.5. Permitir cadastramento de ilimitados contratos e outros dados relacionados independente de licenças de usuário;

2.2.28.6. Medição e remoção de *software* não permitido;

2.2.28.7. Medição do uso de aplicações em computadores, sendo aplicativos compostos de vários arquivos ou executáveis simples;

2.2.28.8. Coleta e armazenamento de informações gerais sobre a utilização de aplicações: nome do arquivo, local, usuário, computador onde foi executado, data e hora;

2.2.28.9. Monitoramento de consumo de CPU e memória utilizado por aplicações definidas pelo administrador, permitindo visualizar média e pico de utilização destes recursos por aplicação ou computador;

2.2.28.10. Medição do tempo de uso de aplicações definidas pelo administrador, de forma que seja possível filtrar aplicações usadas somente em maior período do que o definido pelo administrador;

2.2.28.11. Políticas diferenciadas de medição do uso e remoção de *software* para grupos de computadores, permitindo que um mesmo *software* seja executado em um computador, mas não em outro;

2.2.28.12. Envio de eventos de monitoramento e remoção de *software* de forma on-line ou em frequências determinadas pelo administrador, válidas para determinadas políticas ou todas, criando a facilidade do administrador habilitar política de monitoramento de *software* crítico com notificação on-line e política com objetivo de notificar bloqueio de *software* com notificação diária ou semanal;

2.2.29. Empacotamento e Distribuição de Software

2.2.29.1. Distribuição e instalação de *softwares*, automatizar procedimentos de configuração ou manutenções rotineiras;

2.2.29.2. Captura de informação de um computador, solicitação de preenchimento de dados e, se necessário, realização de ações baseadas nas informações coletadas ou informadas pelo usuário em tempo real no momento da instalação;

2.2.29.3. Possuir um ponto central de instalação, atualização e desinstalação de software;

2.2.29.4. Acompanhamento em tempo real do status da distribuição;

2.2.29.5. Suporte a computadores Windows, MacOS e dispositivos móveis;

2.2.29.6. Instalar automaticamente as aplicações ou componentes requeridos de uma aplicação principal que for instalada pela solução;

2.2.29.7. de softwares de forma silenciosa, ou seja, sem interação com o usuário;

2.2.29.8. Controle centralizado do status de distribuição do pacote;

2.2.29.9. Controle centralizado do status da instalação ou desinstalação efetiva do pacote;

2.2.29.10. Possibilidade de criar políticas de distribuição de software com definição de data de início e término da validade da política;

2.2.29.11. Usar o horário do servidor de gerenciamento;

2.2.29.12. Notificação da disponibilidade da política para o usuário de forma opcional em cada política;

2.2.29.13. Notificação da entrega da política para o usuário de forma opcional em cada política;

2.2.29.14. Configuração de limite máximo de tempo para o usuário adiar a execução da política;

2.2.29.15. Flexibilidade no agendamento da política com possibilidade de combinação de qualquer uma das regras a seguir isoladas ou simultaneamente:

2.2.29.15.1. Assim que o computador se comunicar com servidor;

2.2.29.15.2. Somente em um determinado dia e horário;

2.2.29.15.3. Assim que possível após o horário agendado;

2.2.30. Gerenciamento de Patches

2.2.30.1. *Download* centralizado de *patches* da Internet;

2.2.30.2. Suporte a computadores Windows, MacOS e dispositivos móveis;

2.2.30.3. Automatização de *download* e instalação de patches Microsoft, Adobe, Google e de plug-ins de *browsers*;

2.2.30.4. Verificação remota de vulnerabilidades e necessidades de *updates*;

2.2.30.5. Relatórios gerenciais sobre vulnerabilidades e *status* dos *patches*;

2.2.30.6. Forçar a reinicialização do sistema operacional ao atualizar *patches* críticos para garantir que surtam efeito nos *endpoints*;

2.2.31. Medição e Bloqueio de Software

2.2.31.1. Medição do uso de aplicações em computadores Windows, sendo aplicativos compostos de vários arquivos ou executáveis simples;

2.2.31.2. Medição de *softwares* diversos, mesmo que não homologados;

2.2.31.3. Coleta e armazenamento em banco de dados de informações gerais sobre a utilização de aplicações: nome do arquivo, local, usuário, computador onde foi executado, data e hora;

2.2.31.4. Permitir medição e bloqueio do uso de aplicativos específicos para os usuários que estejam conectados à rede, desconectados móveis e remotos;

2.2.31.5. Enviar alertas ao administrador quando um aplicativo é bloqueado;

2.2.31.6. Identificação de softwares executados mesmo que não instalados;

2.2.31.7. Monitoramento de consumo de CPU e memória utilizado por aplicações definidas pelo administrador, permitindo visualizar média e pico de utilização destes recursos por aplicação ou computador;

2.2.31.8. Medição do tempo de uso de aplicações definidas pelo administrador, de forma que seja possível filtrar aplicações usadas somente em maior período do que X minutos, por exemplo;

2.2.31.9. Definição de lista de softwares não autorizados, baseada em nome de arquivo ou informações do cabeçalho do programa, permitindo que o bloqueio seja efetivo mesmo que o usuário modifique o nome do

arquivo;

2.2.31.10. Normalização e correção de nomes de softwares monitorados seguindo as mesmas regras de inventário, garantindo consistência em análises consolidadas de software instalado e software usado;

2.2.31.11. Bloqueio do uso de software de acordo com os seguintes critérios: Indefinidamente (sempre), Somente em determinados horários e Somente em determinados dias e horários;

2.2.31.12. Políticas de medição e bloqueio do uso de software diferenciadas para grupos de computadores, permitindo que um mesmo software seja executado em um computador mas não em outro;

2.2.31.13. Envio de eventos de monitoramento e bloqueio de forma on-line ou em frequências determinadas pelo administrador, válidas para determinadas políticas ou todas, criando a facilidade do administrador habilitar política de monitoramento de software crítico com notificação on-line e política com objetivo de notificar bloqueio de software com notificação diária ou semanal;

2.2.31.14. Log das alterações automáticas ou realizadas por usuários nos itens e atributos do CMDB que forem definidos pelo órgão para serem controlados, informando o dado anterior, o dado novo, o usuário e a data/hora da alteração;

2.2.32. Provisionamento de Imagens de Sistema Operacional

2.2.32.1. Capturar e distribuir imagens incluindo formato EXE universal para auto extração;

2.2.32.2. Permitir provisionar dinamicamente uma imagem, configurações e software para os computadores que se conectarem a rede usando regras por MAC Address, tipo de Hardware, Rede Local, e outros dados;

2.2.32.3. Com a capacidade de transmitir pacotes de multicast, o cliente deve receber a imagem e depois enviar via multicast para o resto dos clientes sem exigir configuração em roteadores para permitir a transmissão de pacotes de multicast ou um servidor na sub rede;

2.2.32.4. A solução deve permitir o encaminhamento de PXE, para que um cliente seja eleito para trafegar PXE sem ter de adicionar ou reconfigurar o hardware, sem requerem um servidor PXE separado em cada sub rede ou roteadores configurados para transmitir o tráfego PXE;

2.2.32.5. Gerenciar o computador remotamente mesmo que não tenha PXE e acesso físico através de partição de boot embutido.

2.2.33. Virtualização de Aplicativos

2.2.33.1. Suporte a computadores Windows;

2.2.33.2. Deve contemplar licenças de solução de virtualização de aplicativos para as estações, para um número ilimitado de aplicativos virtualizados;

2.2.33.3. Deve permitir que as camadas virtualizadas sejam automaticamente acessíveis para as demais aplicações instaladas fisicamente ou outras camadas virtualizadas;

2.2.33.4. Deve ser completamente integrado com o software de gerenciamento

instalado. Por completamente integrado entende-se que deve ser gerenciado pela mesma console, utilizando a mesma base de dados e fazer uso da estrutura de comunicação do cliente já instalado nas estações do MinC;

2.2.33.5. Deve se capaz de carregar e desabilitar aplicativos sem a necessidade de reinicialização do sistema operacional;

2.2.33.6. Deve ser capaz de editar o arquivo virtualizado, ou seja, alterar os arquivos e parâmetros nesse contido;

2.2.33.7. Deve ser capaz de exportar o aplicativo virtualizado em arquivo único;

2.2.33.8. A fim de inibir a cópia indevida dos aplicativos proprietários, o pacote virtualizado gerado não pode ser executado sem o agente da solução;

2.2.33.9. Deve ser capaz de customizar quais aplicativos virtualizados serão inicializados automaticamente com a máquina através da própria interface do cliente;

2.2.33.10. Deve ser capaz de capturar a instalação de um produto, independente dos demais processos em execução na máquina, ou seja, não utilizando tecnologia de snapshot do ambiente como um todo e utilizando MSI ou EXE sem necessidade de criar um novo pacote;

2.2.33.11. Deve ser capaz de gerar capturas globais, utilizando captura via snapshot do ambiente como um todo;

2.2.33.12. Permitir que as aplicações distribuídas, seja de forma física ou virtual, sejam passíveis de serem inventariadas pelo sistema de inventário – ou métodos tradicionais de inventário, sejam verificadas por software antivírus e ferramentas de auditoria de segurança;

2.2.33.13. Permitir modificações na aplicação virtual sem necessidade de reempacotar;

2.2.33.14. A aplicação virtual deve usar a conta system e manter elementos como registro, menus de atalho, registro em Painel de Controle, etc. normalmente como as aplicações físicas;

2.2.33.15. Suportar aplicações 64-bits;

2.2.33.16. Permitir classes de protocolo (para que links HTTP, por exemplo funcionem dentro das ferramentas de correio;

2.2.33.17. Suportar extensões shell;

2.2.34. Solução para Proteção Avançada de Servidores

2.2.34.1. Deve oferecer proteção proativa contra ataques tipo Dia-Zero diretamente no equipamento, para no mínimo:

2.2.34.1.1. Deve impedir a exploração maliciosa de sistemas e aplicações;

2.2.34.1.2. Deve prevenir a entrada e distribuição de códigos maliciosos;

2.2.34.2. Deve ter a capacidade de integração nativa com a tecnologia VMWare NSX, movendo de forma automática um determinado equipamento infectado para uma área de quarentena;

2.2.34.3. Deve ter a capacidade de liberar alguns serviços mesmo em área de quarentena, ao mover o equipamento identificado como infectado

dentro do VMWare NSX;

2.2.34.4. Deve manter em conformidade com as políticas de seguranças através de verificações continua em clientes e servidores;

2.2.34.5. Deve efetuar "hardening" de sistemas operacionais, aplicações e bancos de dados;

2.2.34.6. Deve conter políticas de segurança nativas para aplicativos Microsoft;

2.2.34.7. Deve conter políticas de "hardening" padrões e nativas, possibilitando o fechamento do hardware, protegendo aplicativos de alto risco e base de dados, contra arquivos executáveis não autorizados a "rodar";

2.2.34.8. Deve impedir a execução de aplicações não autorizadas;

2.2.34.9. Deve permitir ao Administrador bloquear trafego por porta, por protocolo, por IP ou por faixa de endereços IP;

2.2.34.10. Proteger arquivos e registros do sistema baseado em políticas;

2.2.34.11. Monitorar arquivos e registros do sistema baseado em políticas;

2.2.34.12. Deve possuir Sistema de Prevenção de Intrusos;

2.2.34.13. Deve possuir Sistema de Detecção de Intrusos;

2.2.34.14. Deve permitir ao administrador configurar filtros de eventos no agente, somente os eventos filtrados serão encaminhados para o servidor de gerenciamento;

2.2.34.15. Deve possuir sistema de atualização automática de políticas e pacotes de relatórios a partir do site do fabricante;

2.2.34.16. Deve ter a capacidade de importar e exportar políticas customizadas ou de terceiros;

2.2.34.17. Deve ter e capacidade de controlar o comportamento detectando e prevenindo ações especificas que uma aplicação ou usuários executem de forma a prejudicar o funcionamento do sistema ou aplicativo;

2.2.34.18. Deve possuir sistema de criação de usuários com perfis diferenciados de acesso aos recursos da console de gerenciamento;

2.2.34.19. Deve permitir o envio de alertas através de E-mail e SNMP baseados em filtros de eventos recebidos pela console de gerenciamento;

2.2.34.20. Deve possuir políticas predefinidas de monitoramento, de no mínimo os seguintes recursos:

2.2.34.20.1. Falha de acesso;

2.2.34.20.2. Logon com sucesso;

2.2.34.20.3. Detecção de logoff remoto;

2.2.34.20.4. Alteração de configuração pelo Usuário;

2.2.34.20.5. Alteração no grupo de gerenciamento;

2.2.34.21. Deve possuir agente remoto para monitorar arquivos e eventos em servidores sem o agente instalado;

2.2.34.22. Deve possuir recurso de prevenção contra acesso indevido de usuários e de aplicações a outros recursos do sistema, como arquivos, processos, bibliotecas e registros;

2.2.34.23. Deve ter a capacidade de através do recurso de controle de aplicação, monitorar com opção de bloqueio, as atividades da aplicação, assim

como o recurso de rede e de dispositivos, exemplo controle de uso do USB e recursos de rede;

2.2.34.24. Deve ter a capacidade de prevenção contra ataques de exploração, com regras pré-definidas baseadas no comportamento padrão das aplicações do servidor;

2.2.34.25. Deve ter a capacidade de prevenção de intrusão baseado no comportamento das aplicações;

2.2.34.26. Deve possuir recurso nativo de firewall, restringindo atividades de rede por IP e Porta nos sentidos de entrada e saída;

2.2.34.27. Deve ter a capacidade de prevenção contra alteração de privilégios do servidor;

2.2.34.28. Deve ter a capacidade de prevenir contra alterações em arquivos e registros do servidor;

2.2.34.29. Deve ter a capacidade de proteção contra execução de instalações e operações não autorizadas no servidor;

2.2.34.30. Deve ter a capacidade de controlar e monitorar mídias removíveis;

2.2.34.31. Deve ter a opção de monitoramento granular de arquivos e diretórios dos servidores e estações;

2.2.34.32. Deve ter a capacidade de prevenir a adição de códigos em processos em memória para servidores Windows (memory injection protection);

2.2.34.33. Deve ter a capacidade nativa para integrar com uma solução de SIEM de fabricação própria e de terceiros, possibilitando a coleta de logs de gerenciamento e correlação em "real-time";

2.2.34.34. Deve ter a capacidade de implementar "sandbox" para as aplicações conhecidos do administrador, independente se são aplicações de mercado e proprietárias;

2.2.34.35. A solução deve ter a capacidade de no mínimo:

2.2.34.35.1. Bloquear instalações de aplicações indevidas;

2.2.34.35.2. Proteger o "core" do sistema operacional;

2.2.34.35.3. Proteger as áreas "RAW" dos discos locais;

2.2.34.36. Deve ter a capacidade de implementar listas avançadas de aplicações autorizadas ("Advanced White List") a serem executadas, através da correlação das seguintes funcionalidades, sendo no mínimo os seguintes parâmetros:

2.2.34.36.1. Hash do arquivo executável para o processo específico (MD5 e SHA256);

2.2.34.36.2. Nome como é publicado, conforme é descrito no certificado emitido pelo fabricante da aplicação;

2.2.34.36.3. Assinatura digital das aplicações e aplicativos, incluindo componentes de sistema operacional, assinaturas Microsoft, assinaturas confiáveis, serviços e processos interativos;

2.2.34.36.4. Possibilidade de executar auditoria no AD, troca de usuário, reset de senha, permissão ou não, com relatórios sobre cada ajustes alterados na linha do tempo.

2.2.34.36.5. A solução deve ter a capacidade de implementar auditoria no Microsoft Active Directory, possibilitando elaborar relatórios com a periodicidade diária, semanal e mensal, para no mínimo:

- Reset de senha;
- Alteração de permissionamento;
- Troca de usuário;

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

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

2.2.34.38.1. Origem confiável;

2.2.34.38.2. Origem não confiável;

2.2.34.38.3. Tempo de existência do arquivo na internet;

2.2.34.38.4. Comportamento do arquivo;

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

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

2.2.34.40. Capacidade de identificar e proteger ataques direcionados, impossibilitando o início do ataque e não somente impedindo as ações após invasão do equipamento;

2.2.34.41. A solução deve ter a capacidade de implementar sem a necessidade de agente, em uma infraestrutura virtual serviço de antivírus, para no mínimo:

2.2.34.41.1. VMware ESXi 5.1 e superior;

2.2.34.41.2. VMware vCenter 5.5 e superior;

2.2.34.41.3. VMware NSX;

2.2.34.42. A solução deve ter a capacidade de implementar sem a necessidade de agente, em uma infraestrutura do VMware vSphere serviço de antivírus, funcionalidades de IDS e funcionalidades de IPS;

2.2.34.43. A solução deve ter a capacidade de implementar, em uma infraestrutura seja ela, física e virtual serviço de antivírus, funcionalidade de reputação de arquivos, funcionalidades de IDS, funcionalidades de IPS para no mínimo:

2.2.34.43.1. VMware ESXi 5.1 ou superior;

2.2.34.43.2. VMware vCenter 5.5 ou superior;

2.2.34.43.3. VMware NSX;

2.2.34.43.4. Windows 2000 Professional/Server/Advanced Server;

2.2.34.43.5. Windows XP Professional;

2.2.34.43.6. Windows Server 2003 Standard/ Enterprise 32-bit;

2.2.34.43.7. Windows Server 2003 Standard/ Enterprise 64-bit;

2.2.34.43.8. Windows NT Server 4 (6a);

2.2.34.43.9. SUN Solaris 9.0 /10.0 - 32-bit 64-bit;

2.2.34.43.10. Red Hat Enterprise Linux ES 4.0;

2.2.34.43.11. SUSE Enterprise Linux 9;

2.2.34.43.12. Hewlett-Packard HP-UX 11.23 (v2)/11.31 (v3) em Itanium 2® Processor;

2.2.34.44. A solução deve ter a capacidade de implementar sem a necessidade de agente, em uma infraestrutura do VMware vSphere, funcionalidade de no mínimo:

2.2.34.44.1. Bloqueio a acesso não autorizado a Chaves SSL;

2.2.34.44.2. Tamper Protection de Binários;

2.2.34.44.3. Bloqueio a acesso não autorizado a arquivos de configurações;

2.2.34.44.4. Bloqueio a acesso não autorizado a chaves de registro;

2.2.34.44.5. Bloqueio a acesso não autorizado a arquivos de Logs;

2.2.34.44.6. Controle sobre privilégios de usuários e processos;

2.2.34.44.7. Monitoração da Integridade dos arquivos de vCenter;

2.2.34.44.8. Monitoração da Integridade dos arquivos dos Servidores ESXi 5.1 e superiores;

2.2.34.44.9. Monitoração da Integridade dos arquivos de configurações das VM Guest;

2.2.34.44.10. Monitoração direta dos LOGs nos servidores ESX, ESXi e vCenter;

2.2.34.45. A solução deve ter a capacidade de implementar as funcionalidades de controle de dispositivos e aplicações;

2.2.34.46. A solução deve ter a capacidade de implementar a funcionalidade de "File and Configuration Lock Down";

2.2.34.47. A solução deve implementar em um único agente as funcionalidades de HIPS, HIDS, Host Firewall, Application e Device Control;

2.2.35. Compatibilidade

2.2.35.1. A solução deve suportar, no mínimo, os seguintes sistemas operacionais para a instalação dos binários da console de gerenciamento em ambientes físicos e virtuais:

2.2.35.1.1. Windows XP Professional;

2.2.35.1.2. Windows 7

2.2.35.1.3. Windows Server 2003 Standard/ Enterprise 32-bit;

2.2.35.1.4. Windows Server 2003 Standard/ Enterprise 64-bit;

2.2.35.1.5. Windows Server 2008 e 2008 R2;

2.2.35.1.6. Windows Server 2012;

2.2.35.2. A solução deve suportar, no mínimo, os seguintes sistemas operacionais

para a instalação dos binários do servidor de gerenciamento em ambientes físicos e virtuais:

2.2.35.2.1. Windows Server 2003 Standard/ Enterprise 32-bit;

2.2.35.2.2. Windows Server 2003 Standard/ Enterprise 64-bit;

2.2.35.2.3. Windows Server 2008 e 2008 R2;

2.2.35.2.4. Windows Server 2012;

2.2.35.3. A solução deve suportar, no mínimo, os seguintes sistemas operacionais para a instalação dos binários do agente:

2.2.35.3.1. Windows NT Server 4 (6a);

2.2.35.3.2. Windows 2000 Professional/Server/Advanced Server;

2.2.35.3.3. Windows XP Professional;

2.2.35.3.4. Windows Server 2003 Standard/ Enterprise 32-bit;

2.2.35.3.5. Windows Server 2003 Standard/ Enterprise 64-bit;

2.2.35.3.6. Windows 2008 e 2008 R2;

2.2.35.3.7. Windows 2012;

2.2.35.3.8. SUN Solaris 9.0, 10 e 11;

2.2.35.3.9. Red Hat Enterprise Linux ES 4.0 e 5.0;

2.2.35.3.10. SUSE Enterprise Linux 9, 10 e 11;

2.2.35.3.11. Hewlett-Packard HP-UX 11.23 (v2)/11.31 (v3) em Itanium 2® Processor;

2.2.35.3.12. AIX 6.1, 7.1 e superior;

2.2.35.3.13. CentOS 6 Kernel 2.6.32-71.*el6, 2.6.32.220.*el6, 2.6.32-279.*el6, 2.6.32-358.*el6;

2.2.35.3.14. Oracle LNX 5.8, 5.9, 6.3 e superior;

2.2.35.4. A solução deve ser suportada, no mínimo, nas seguintes versões de VMware:

2.2.35.4.1. VMware Workstation v5.0.0 e v5.5.4;

2.2.35.4.2. VMware ESX v3.0.1 e v3.0.2;

2.2.35.5. Os agentes devem ser suportados quando instalados nos seguintes sistemas operacionais tipo Guest em sistemas Virtualizados VMWare:

2.2.35.5.1. Windows NT Server 4 (6a);

2.2.35.5.2. Windows 2000 Professional/Server/Advanced Server;

2.2.35.5.3. Windows XP Professional;

2.2.35.5.4. Windows Server 2003 Standard/ Enterprise 32-bit;

2.2.35.5.5. Windows Server 2003 Standard/ Enterprise 64-bit;

2.2.35.5.6. Windows 2008 e 2008 R2;

2.2.35.5.7. Windows 2012;

2.2.35.5.8. SUN Solaris 9.0, 10 e 11;

2.2.35.5.9. Red Hat Enterprise Linux ES 4.0 e 5.0;

2.2.35.5.10. SUSE Enterprise Linux 9, 10 e 11;

2.2.35.5.11. Hewlett-Packard HP-UX 11.31 (v3) em Itanium 2® Processor;

2.2.35.5.12. AIX 6.1, 7.1 e superior;

2.2.35.5.13. CentOS 6 Kernel 2.6.32-71.*el6, 2.6.32.220.*el6, 2.6.32-279.*el6, 2.6.32-358.*el6;

2.2.35.6. O software deve suportar os componentes IDS e IPS, para no mínimo os seguintes sistemas operacionais:

2.2.35.6.1. Red Hat Enterprise Linux 4, 5 e 6;

2.2.35.6.2. CentOS 6;

2.2.35.6.3. Oracle Linux 5 e 6;

2.2.35.6.4. SuSE Linux Enterprise Server 10 e 11;

2.2.35.6.5. Solaris 10 e 11;

2.2.35.6.6. Hewlett-Packard HP-UX 11.31 (v3) em Itanium 2® Processor;

2.2.35.6.7. AIX 6.1, 7.1 e superior;

2.2.35.6.8. Windows NT4 SP6;

2.2.35.6.9. Windows 2000 SP4 Professional, Server e Advanced Server;

2.2.35.6.10. Windows XP Professional SP2, SP3;

2.2.35.6.11. Windows 2003 Standard e Enterprise (32 e 64 bit);

2.2.35.6.12. Windows 2008 Standard e Enterprise (32 e 64 bit);

2.2.35.7. **O software deve suportar o componente IDS, para no mínimo os seguintes sistemas operacionais:**

2.2.35.7.1. VMWare Server ESXi 5.5 Host;

2.2.35.7.2. VMWare Server ESXi 5.5 Host;

2.2.35.7.3. VMWare Server ESXi 5.0 Host;

2.2.35.7.4. VMWare Server ESXi 4.1 Host;

2.3. Segurança Proativa com Inteligência de Detecção

2.3.1. A Segurança Proativa deve ofereces informações sobre uma ampla gama de dados de ameaças e vulnerabilidades em tempo real, provendo ao órgão informações necessárias para proteger sua infraestrutura de forma proativa. Alertas personalizados garantindo que, a priorização das ações de mitigação, protejam as infraestruturas críticas contra ameaças emergentes e vulnerabilidades exploráveis.

2.3.1.1. A solução deve ter capacidade de integrar-se comprovadamente com no mínimo as seguintes soluções de segurança:

2.3.1.1.1. Snort;

2.3.1.1.2. Splunk;

2.3.1.1.3. HP ArcSight;

2.3.1.1.4. BMC Remedy;

2.3.1.1.5. Bind9;

2.3.1.1.6. Cisco Sourcefire;

2.3.1.1.7. Microsoft DNS Services;

2.3.1.1.8. Altiris Symantec Management Platform;

2.3.1.1.9. Symantec Endpoint Protecion;

2.3.1.1.10. Symantec Control Compliance Suite;

2.3.1.1.11. Symantec Data Loss Prevention;

2.3.1.1.12. Symantec™ Protection Center;

2.3.1.1.13. Symantec™ Validation and ID Protection Service;

2.3.1.1.14. Ferramenta de Workflow;

2.3.1.2. Deve ter a capacidade de municiar com informações de segurança, vulnerabilidades e reputação as ferramentas de GRC, analisadores de vulnerabilidades e correlacionadores de eventos de forma holística, sem a necessidade de serem do mesmo fabricante da solução, para no mínimo:

2.3.1.2.1. Snort;

2.3.1.2.2. Splunk;

2.3.1.2.3. ArcSight;

2.3.1.2.4. Bay Dynamics;

2.3.1.2.5. Bind;

2.3.1.2.6. Archer;

2.3.1.2.7. Microsoft DNS;

2.3.1.3. A solução deve ser um serviço de distribuição de conteúdo customizado para o ambiente computacional do órgão, referente as ameaças mundiais mais recentes, as quais possam ser exploradas em caso de não remediação;

2.3.1.4. A solução deve entregar dados referente a segurança da informação possibilitando integração com as ferramentas já existentes hoje em produção, assim como, com os produtos objetos deste certame, de forma customizada atendendo exatamente ao ambiente do órgão, enfatizando as ameaças relevantes ao ambiente existente, vulnerabilidades e reputação, permitindo ao órgão que ajuste sua postura de segurança, conforme necessário, com base em ameaças emergentes que podem afetar seus sistemas críticos;

2.3.1.5. A solução deve ter a capacidade de ampliar a visibilidade das ameaça e vulnerabilidades globais ajuda identificando e bloqueando ameaças antes que afetem sistemas críticos;

2.3.1.6. A solução deve ter a capacidade de ajustar as respostas do órgão com base no perfil de risco, através da combinação de ameaças, vulnerabilidades e informações de reputação permite ao órgão, definindo alertas com base em suas políticas individuais de infraestrutura de TI e de segurança, permitindo o ajuste da postura da área de segurança, conforme necessário;

2.3.1.7. Melhora a produtividade da equipe de segurança. Ter uma fonte de dados único que está focado apenas em ameaças e questões relevantes permite que a equipe de responder de forma eficaz, enquanto liberando

tempo para outras tarefas.

2.3.1.8. A solução deve ser baseada em uma coleta de dados referente as mais recentes ameaças, a qual deve ser realizada através da rede de Inteligência de Segurança do fabricante da solução com visibilidade global para o cenário de ameaças, com no mínimo:

2.3.1.8.1. Mais de 60 milhões de sensores de monitorarão de ataques distribuídos geograficamente;

2.3.1.8.2. Mais de 43 mil vulnerabilidades, cobrindo mais de 14.000 fornecedores;

2.3.1.8.3. Visibilidade em todas as portas e/ou protocolos para análise de ameaças;

2.3.1.8.4. Mais de 7 milhões de e-mails por dia analisados;

2.3.1.8.5. Mais de 1,2 bilhões de sites analisados por dia;

2.3.1.9. A solução de ter a capacidade de entregar informações referente as ameaças mundiais, possibilitando proteger a rede do órgão contra ameaças eminentes, sendo capaz de reconhecer "o que" e "quem" é susceptível a atacar, identificando se as vulnerabilidades identificadas podem ser explorados para atacar a rede corporativa do órgão;

2.3.1.10. A solução deve prover maior visibilidade no cenário mundial de Segurança da Informação, tornando a política de segurança proativa, identificando as possíveis ameaças antes de sua exploração, agregando dados das ameaças de várias fontes, tornando a identificação de ameaças relevantes e acarretando na priorização de ações para mitigar potenciais vulnerabilidades em tempo real;

2.3.1.11. A solução deve implementar uma análise minucioso sobre as ameaças, considerando-se no mínimo:

2.3.1.11.1. Análise de ameaças emergentes;

2.3.1.11.2. Vulnerabilidades;

2.3.1.11.3. Códigos Maliciosos;

2.3.1.11.4. Estratégias de mitigação;

2.3.1.11.5. Medidas de correção permitindo remediarão rápida de momentos de epidemia e surtos de ameaças;

2.3.1.12. A solução deve prover relatórios customizados conforme as necessidades do órgão, tomando por base um determinado parâmetro a ser definido, de acordo com a ameaça a ser identificada, verificando-se no mínimo:

2.3.1.12.1. Tipo do Evento;

2.3.1.12.2. Malcode (virus, worms, trojan horses, ...)

2.3.1.12.3. Origem e Destino das ameaças;

2.3.1.12.4. Características do equipamento atacado;

2.3.1.12.5. Portas utilizadas;

2.3.1.13. A solução deve prover metodologia nativa que possibilite customizar alertas de vulnerabilidade conforme a necessidade do ambiente do órgão, com no mínimo as seguintes variáveis:

2.3.1.13.1. Nome do filtro;

2.3.1.13.2. Atualização das informações na ocorrência do filtro configurado;

2.3.1.13.3. Alerta se as vulnerabilidades são possíveis de exploradas;

2.3.1.13.4. Implementar níveis de criticidade possibilitando priorizar as tarefas de mitigação da vulnerabilidade;

2.3.1.13.5. Implementar níveis de credibilidade, quanto a informação recebida, seja pela confirmação ou não quanto a vulnerabilidade por parte do fabricante da solução afetada, seja por informações não consistentes;

2.3.1.13.6. Deve informar informações básicas referente a tecnologia alvo da vulnerabilidade, tal como fabricante, produto e versão;

2.3.1.13.7. Deve ter a capacidade de informar qual o meio utilizado para receber alertas (E-mail, RSS, SMS, XML);

2.3.1.13.8. Deve ter a capacidade de definir em o formato de recebimento do alerta, seja PDF e TXT;

2.3.1.13.9. Implementar níveis de detalhamento da informação recebida, desde informações básicas até um detalhamento completo;

2.3.1.14. A solução deve implementar minimamente os seguintes níveis de detalhamento nos alertas enviados:

2.3.1.14.1. Informação - Incluindo o ID da vulnerabilidade, nível de urgência ou severidade, pequena discrição;

2.3.1.14.2. Detalhamento WEB - Indicar um endereço WEB do fabricante com o detalhamento completo da vulnerabilidade;

2.3.1.14.3. Sumário Operacional – Incluindo como assunto, vulnerabilidades locais ou remotas, últimos versionamentos, sistemas vulneráveis e não vulneráveis, impacto, estratégia de remediação sumário da vulnerabilidade;

2.3.1.14.4. Sumário Executivo – Resumo executivo da saúde dos sistemas, e quanto as novas ameaças;

2.3.1.14.5. Detalhado – Prover informações detalhadas ao máximo, contendo todas as informações existentes na base de conhecimento referente a ameaça;

2.3.1.15. A solução deve ter a capacidade de explorar eventos coletados no passado, através da determinação de uma faixa de tempo;

2.3.1.16. A solução deve ter a capacidade de implementar e configurar, de forma customizada às necessidades do órgão monitores do ambiente corporativo, para no mínimo:

2.3.1.16.1. Monitores de Vulnerabilidades – Monitora Vulnerabilidades inerentes ao ambiente do órgão;

2.3.1.16.2. Monitores de Códigos Maliciosos – Monitora ameaças as tecnologias utilizadas no órgão;

2.3.1.16.3. Monitores de Eventos – Monitora a atividade de eventos de forma proativa que possam ser exploradas;

2.3.1.16.4. Monitores de Portas – Monitora a atividade de ataques de forma proativa que possam ser explorados, sob as portas utilizadas em sues sistemas;

2.3.1.16.5. Monitores de Seguimento – Monitora a ocorrência de eventos suspeitos de forma proativa, em um segmento de negócio determinado, delimitado pela quantidade de eventos em uma determinada faixa de tempo;

2.3.1.16.6. Monitores de Tecnologia – Monitora a ocorrência de ataques de forma proativa, em determinadas tecnologias colocadas como alvo e utilizadas pelo órgão;

2.3.1.16.7. Monitores de Ameaças – Monitora de forma proativa novas ameaças e ameaças ligadas as tecnologias utilizadas pelo órgão;

2.3.1.17. A solução deve ter a capacidade a partir do nível de urgência, grau de severidade e impacto dos alertas de ameaças ao ambiente do órgão, determinar o nível de risco considerado como aceitável ou não;

2.3.1.18. A solução deve prover uma ferramenta precisa para submissão de ameaças, utilizando-se de métodos de comparação de hash para validar a identificação da ameaça;

2.3.1.19. A solução deve a partir da confirmação do hash, apresentar na própria console da solução uma descrição detalhada da ameaça, com sua nomenclatura e as últimas atualizações dos descritivos técnicos;

2.3.1.20. A solução deve prover uma metodologia para analisar ferramentas de terceiros e ferramentas de código aberto, validando a segurança da utilização interno ao ambiente do órgão, provendo em caso da detecção de uma eminente ameaça(s), no mínimo as seguintes informações:

2.3.1.20.1. Todas as ameaças constantes na ferramenta;

2.3.1.20.2. Todas as vulnerabilidades;

2.3.1.20.3. Alertas gerados onde a causa é a ferramenta;

2.3.1.20.4. Alertas associados a ferramenta;

2.3.1.20.5. CVE ID (se existirem);

2.3.1.20.6. Severidade;

2.3.1.20.7. Impacto;

2.3.1.20.8. Relatório detalhado da ameaça que a ferramenta causa;

2.3.2. DataFeeds

2.3.2.1. A solução deve prover métodos de integrar e alimentar as soluções de segurança de terceiros existentes, com a base de conhecimento através do consumo de um arquivo XML, que poderá ser aplicado em soluções como SIEM, gateways da Internet, ou outras soluções de segurança de rede;

2.3.2.2. A solução através da integração com as ferramentas de terceiros deve permitir de forma dinâmica, o refinamento das política de segurança, sem sobrecarga da área de TI para proteger por exemplo, o órgão contra

a comunicação com uma fonte externa mal-intencionado;

2.3.2.3. A solução deve fornecer em tempo real informações quanto as vulnerabilidades existentes, contando na base de dados do fabricante com, informações de no mínimo;

2.3.2.3.1. 100.000 (cem mil) tecnologias;

2.3.2.3.2. 14.000 (quatorze mil) fornecedores;

2.3.2.4. A solução deve correlacionar dados de urgência e impacto, juntamente com as informações em tempo real das vulnerabilidades, minimizando riscos e otimizando a utilização de recursos;

2.3.2.5. A solução deve prover análise de reputação para IPs, Domínios e URLs, correlacionando-se no mínimo informações referente a:

2.3.2.5.1. Participação em Ataques;

2.3.2.5.2. Originador de Malware;

2.3.2.5.3. Originador de Phishing;

2.3.2.5.4. Distribuição de Spam;

2.3.2.5.5. Infecções Bots;

2.3.3. Solução para Prevenção de Ataques Direcionados

2.3.3.1. A solução deverá prover as funcionalidades de gerenciamento centralizado para as soluções de analise de web e rede.

2.3.3.2. A solução deverá ser executada em Hardware e Software específicos (appliance) com sistema operacional especializado ou em Software Appliance. Todas as funcionalidades deverão ser executadas no mesmo equipamento. Toda a solução de hardware e software deverá ser fornecida pelo mesmo fabricante;

2.3.3.3. Hardware:

2.3.3.3.1. Possuir no máximo 2U padrão 19" Rack;

2.3.3.3.2. Possuir no mínimo 02 (dois) processadores Octa Core (8 cores);

2.3.3.3.3. Possuir no mínimo 64 GB de memória RAM;

2.3.3.3.4. Possuir no mínimo 02 (dois) discos rígidos 146GB;

2.3.3.3.5. Possuir configuração mínima de RAID entre os discos;

2.3.3.3.6. Possuir no mínimo 02 interfaces 10/100/1000BaseTX ou 10Gbps ;

2.3.3.3.7. Possuir fonte redundante e hot swappable;

2.3.3.3.8. Possuir interface de console do tipo RS-232, ou similar.

2.3.4. Características do Gerenciamento da Solução

2.3.4.1. Implementar gerenciamento centralizado com no mínimo as seguintes funções: criação de regras de tratamento de malware, administração de usuários, configurações de host e network;

2.3.4.2. Implementar a funcionalidade de event server, com mecanismo de rotação automático dos arquivos de evento;

2.3.4.3. Implementar mecanismo de triangulação e correlação dos vetores de ataque;

2.3.5. Características da Administração da Solução

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

2.3.5.2. Implementar interface CLI segura através do protocolo SSH ou interface serial RS-232 e similar;

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

2.3.5.4. Implementar sincronização de hora através de protocolo NTP;

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

2.3.5.6. 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;

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

2.3.5.8. Implementar através da interface gráfica mecanismo de dashboard onde seja possível a visualização de no mínimo as seguintes informações: Sumário de detecção e proteção, gráfico de top infecções, e gráfico da quantidade de e-mails monitorados;

2.3.5.9. Implementar através da interface de administração, configuração de mecanismo de alerta onde seja possível configurar o modo de operação;

2.3.5.10. Implementar a atualização (updates) dos appliances via mecanismo de push dos seguintes módulos: segurança de conteúdo e atualização de patch;

2.3.6. Requisitos da funcionalidade de Análise de Ataques Avançados REDE

2.3.6.1. A solução deverá prover as funcionalidades de inspeção inbound de Malware com filtro de ameaças avançadas e análise de execução em tempo real, inspeção outbound de call-backs;

2.3.6.2. A solução deverá suportar no mínimo 5.000 usuários simultâneos;

2.3.6.3. A solução deverá ser executada em Hardware e Software específicos (appliance) com sistema operacional especializado ou em Software Appliance. Todas as funcionalidades deverão ser executadas no mesmo equipamento, com exceção das funcionalidades de relatórios, as quais deverão ser executadas em appliance ou servidor dedicado para este fim. Toda a solução de hardware e software deverá ser fornecida pelo mesmo fabricante;

2.3.7. Hardware:

2.3.7.1. Possuir no máximo 2U padrão 19" Rack;

2.3.7.2. Possuir no mínimo 02 (dois) processadores Octa Core (8 cores);

2.3.7.3. Possuir no mínimo 32 GB de memória RAM;

2.3.7.4. Possuir no mínimo 02 (dois) discos de 146GB;

2.3.7.5. Possuir configuração mínima de RAID entre os discos;

2.3.7.6. Possuir no mínimo 06 interfaces 10/100/1000BaseTX ou 10Gbps;

2.3.7.7. Possuir fonte redundante e hot swappable;

2.3.7.8. Possuir interface de console do tipo RS-232, ou similar.

2.3.8. Características da Inspeção de Malware REDE

2.3.8.1. Suportar os protocolos HTTP (Inbound), e protocolos TCP e UDP sem exceções (outbound);

2.3.8.2. Implementar e identificar existência de Malware em comunicações de entrada e saída;

2.3.8.3. Implementar mecanismo de bloqueio de vazamento não intencional de dados oriundos de máquinas existentes no ambiente LAN;

2.3.8.4. Implementar detecção de Malwares que utilizem mecanismo de exploit em arquivos PDF;

2.3.8.5. Implementar detecção de Malwares que utilizem mecanismo do tipo zero-day ou semelhante nas seguintes aplicações: Microsoft Internet Explorer, Mozilla FireFox, Adobe Acrobat Reader, Adobe Acrobat, Microsoft Silverlight, SUN Java, RealPlayer, e Apple Quicktime, possibilitando integração com os módulos de Segurança de Endpoint (servidor e cliente), assim como, com o módulo de Segurança Avançada de Endpoint;

2.3.8.6. Implementar Rede de Inteligência proprietária do fabricantes existente em no mínimo 05 (cinco) localidades de forma a cobrir ataques originados de qualquer localidade global, com mecanismo opcional de retroalimentação de Malwares não identificados;

2.3.8.7. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;

2.3.8.8. Implementar no mínimo 02 modos de operação: in-line e out-of-band;

2.3.8.9. Implementar integração com ferramentas de SIEM;

2.3.8.10. Implementar mecanismo de integração com servidores Syslog;

2.3.9. Características da Analise de Malware REDE

2.3.9.1. Implementar atualização a base de dados da Rede de Inteligência de forma automático;

2.3.9.2. Toda análise deve ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador;

2.3.9.3. Todas as máquinas virtuais utilizadas na solução devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema;

2.3.9.4. Toda a verificação e análise de Malwares e/ou códigos maliciosos deve ocorrem em tempo real, não sendo aceitas verificações em cache engine ou batch mode;

2.3.10. Console de Gerenciamento

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

2.3.10.2. Implementar interface CLI segura através do protocolo SSH ou interface serial RS-232 e similar;

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

2.3.10.4. Implementar sincronização de hora através de protocolo NTP;

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

2.3.10.6. 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;

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

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

2.3.10.9. 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 troughput de tráfego monitorado;

2.3.11. Relatórios

2.3.11.1. A solução deve implementar geração de relatórios através da interface gráfica onde contenha no mínimo as seguintes informações: tipo de malware, id de evento, extensão do arquivo inspecionado, severidade da ameaça, horário do último evento, IP de origem, IP de destino;

2.3.11.2. A solução deve implementar mecanismo de pesquisa por diferentes intervalos de tempo;

2.3.11.3. A solução deve implementar através da interface gráfica, pesquisa aos eventos já reconhecidos;

2.3.11.4. A solução deve implementar através da interface gráfica mecanismo de busca dos eventos arquivados através de palavras-chave;.

2.3.11.5. A solução deve implementar através da interface gráfica os seguintes modelos de relatório: Sumário Executivo, Relatório de Hosts infectados, Atividade de Malware e detalhes dos alertas;

2.3.11.6. A solução deve implementar através da interface gráfica, a criação de filtros para apresentação dos alertas visualizados;

2.3.12. Solução para a Gestão e Análise de Ambiente Infraestrutura

2.3.12.1. A solução deve executar as seguintes funcionalidades complementares: gerar relatórios de conformidade do escopo de ativos monitorado, com as políticas, controles e normas internas e externas, a critério do Contratante, além de relatórios técnicos e gerenciais;

2.3.12.2. A solução deve garantir redundância e operar em alta disponibilidade, sem a necessidade de operar em cluster, provendo todos os

equipamentos e recursos necessários ao seu completo funcionamento, bem como se adaptar à configuração dos ativos e ao ambiente de rede do Contratante, e não deve exigir nenhuma modificação de arquitetura, permitindo coleta de informações com ou sem instalação de software em ativos do Contratante, exceto para os ativos que o Contratante julgar necessário possuir agentes para a coleta de eventos;

2.3.13. Console de Gerenciamento e Características Gerais

2.3.13.1. A solução deverá manter disponível de forma on-line todos os eventos capturados durante o período mínimo de 40 (quarenta dias), fornecendo, inclusive, a capacidade de armazenagem de dados suficiente para atender a este item;

2.3.13.2. A solução poderá ser constituída de hardware e software, appliance (hardware com software embarcado) ou virtual appliance;

2.3.13.3. No caso da solução ofertada ser composta de módulos, sua integração deverá ser nativa. Entende-se como integração nativa a comunicação entre os módulos sem a utilização de conectores externos, softwares de conexão de terceiros, exportação de dados ou quaisquer outros recursos de conectividade que necessitem de um sistema e/ou programa extra para essa comunicação;

2.3.13.4. Deve permitir gerenciar mais de um servidor de gateway a partir da mesma console;

2.3.13.5. Deve permitir definir políticas individuais por servidor de gateway e globais, a partir da mesma console;

2.3.13.6. Deve possuir capacidade de administrar de forma unificada, via interface Web (com criptografia), com diversos níveis de acesso (administração, relatórios, quarentena, apenas leitura);

2.3.13.7. Deve possuir possibilidade de acesso individual ao appliance via SSH, para execução de comandos via CLI (linha de comando);

2.3.14. Módulo de Gerência

2.3.14.1. Possuir integração com base de conhecimento sobre atividades anômalas na Internet (origens de ataques, protocolos, etc), obtida automaticamente do site do Fabricante, permitindo a correlação dinâmica dessas informações com os dados coletados na rede local, possibilitando ainda integração com o módulo de Serviço de Segurança Proativa com Inteligência de Detecção;

2.3.14.2. A atualização da base de conhecimento sobre atividades anômalas na Internet deverá possuir periodicidade mínima diária;

2.3.14.3. O processo de detecção de vulnerabilidade deve levar em consideração a normalização e base de conhecimento do fabricante, envolvendo efeitos, recursos e mecanismos utilizados;

2.3.14.4. Permitir a criação de tickets de resolução de incidentes. Possibilidade de incluir no Ticket os artigos da base de conhecimento relevantes ao incidente, e também permitir a inserção de tarefas adicionais manualmente;

2.3.14.5. Fabricante da solução deve possuir laboratórios de pesquisa próprios,

com visão global para detecção de novas ameaças e vulnerabilidades, para fornecer atualizações automáticas diárias para correlação dos eventos locais coletados;

2.3.14.6. Deve ter a capacidade de informar das vulnerabilidades e conformidades em ambiente Windows e Linux podendo executar a detecção de hotfixes, service packs, registros, peer to peer, Antivírus, juntamente com atualizações periódicas no mínimo diárias, recebidas quanto às vulnerabilidades mais recentes, IPs de BOT-NET, IPs maliciosos, Exploids, minimizando desta forma, os incidentes relacionados com os dados sensíveis, através da integração com o módulo de Serviço de Segurança Proativa com Inteligência de Detecção;

2.3.14.7. Deverá ter a capacidade de obter às informações de usabilidade de dados estruturados e não estruturados, indicando minimamente o proprietário do arquivo, o último usuário e o maior usuário deste dado;

2.3.14.8. Deverá ter a capacidade de obter quanto aos registros históricos e acessibilidade dos dados não estruturados, validando as atividades, monitorando arquivos e diretórios confidenciais, integrando a utilização dessas informações sensíveis sem autorização, alertando quanto a uma possível fuga de dado;

2.3.14.9. Deverá ter a capacidade de obter quanto aos dados não estruturados, seu uso suspeito, obtendo histórico de uso, bloqueando o uso caso necessário, prevenindo contra futuros furos de segurança;

2.3.14.10. Deve ter a capacidade de importar individualmente ativos para a verificação, possibilitando categorizar por qual tipo de ativo será importado;

2.3.14.11. Ter a capacidade de carregar a console de administração em um computador remoto;

2.3.15. Módulo Análise Estática

2.3.15.1. Deve oferecer um ambiente centralizado para a coleta e a gestão das evidências de concordâncias específicas para TI com Políticas, Frameworks e Normas;

2.3.15.2. Deve permitir o mapeamento de controles às políticas;

2.3.15.3. Deve permitir a criação de dashboards dinâmicos, acessíveis pela web, com suporte a "drill down" nas evidências;

2.3.15.4. Deve oferecer uma API via Web Services para permitir a integração com processos externos, workflow e ticketing;

2.3.15.5. Deve suportar de forma nativa os padrões da indústria, incluindo PCI, SOX, Cobit, ISO 27002, FISMA, HIPAA, GLBA, Basel II, CIS , NSA, dentre outros;

2.3.15.6. Deve permitir a criação de um novo padrão técnico através da cópia de um padrão técnico pré-definido, permitindo alteração das checagens pré-definidas;

2.3.15.7. Deve efetuar a desduplicação dos controles entre as várias políticas configuradas;

2.3.15.8. Deve ser capaz de realizar a verificação de concordância com

determinada política, framework e norma, cobrindo tanto os requisitos técnicos (configurações dos ativos), quanto procedurais (conscientização dos usuários), de forma automatizada;

2.3.15.9. Deve possuir console de administração de políticas integrado ao módulo de avaliação de controles técnicos, compartilhando a mesma infraestrutura de console, servidor e base de dados;

2.3.15.10. Deve possuir um repositório de políticas com workflow de edição, permitindo trabalhar a política através de fases com níveis de acesso diferenciado (ex: Rascunho, Em Revisão, Revisada, Aprovada, Publicada);

2.3.15.11. Deve permitir a coleta automatizada de evidências de controles técnicos e procedurais;

2.3.15.12. Possui módulo centralizador para a coleta e gestão das evidências de concordância com políticas, frameworks e normas;

2.3.15.13. Permite o controle de exceções às políticas, frameworks e normas, quando a aplicação da configuração recomendada gera impacto no ambiente, não podendo ser efetuada;

2.3.15.14. Permite a integração com sistemas de service desk, para o encaminhamento de tickets de serviço para a correção das não concordâncias;

2.3.15.15. Suporta os sistemas operacionais Windows, UNIX e VMWare, bem como os servidores de aplicação IIS e Apache, através de bases de conhecimento/melhores práticas publicadas pelo SANS, NIST e CIS;

2.3.15.16. Possui base de ativos, onde são armazenadas as informações pertinentes ao ativo, como:

2.3.15.16.1. Características básicas do ativo (sistema operacional, versão de service pack);

2.3.15.16.2. Dono do ativo;

2.3.15.16.3. Vulnerabilidades presentes no ativo;

2.3.15.16.4. Resultado de análise de concordância feitas sobre o ativo;

2.3.15.16.5. Indicadores de Confidencialidade, Integridade e Disponibilidade;

2.3.15.17. Rótulos para qualificar o ativo quanto à grupo, atividade, localidade, papel;

2.3.15.18. Exceções às políticas, frameworks e normas à que o ativo está sujeito.

2.3.16. Controles Técnicos:

2.3.16.1. Deve executar as auditorias do ambiente utilizando os dados coletados e registrados na base de dados;

2.3.16.2. Deve suportar a verificação de configurações e permissões nas plataformas Windows, Unix, Linux, Netware NDS, Oracle, SQL e Exchange;

2.3.16.3. Deve suportar as melhores práticas de configuração definidas pelo NIS, SANS e/ou CIS para as seguintes plataformas:

2.3.16.3.1. HP-UX;

2.3.16.3.2. Solaris;

2.3.16.3.3. VMWare ESX Server;

2.3.16.3.4. AIX;

2.3.16.3.5. Red Hat Enterprise Linux;

2.3.16.3.6. SuSE Enterprise Linux;

2.3.16.3.7. Windows XP;

2.3.16.3.8. Windows Vista;

2.3.16.3.9. Windows 7;

2.3.16.3.10. Windows Server 2000;

2.3.16.3.11. Windows Server 2003;

2.3.16.3.12. Windows Server 2008;

2.3.16.4. Deve ser possível classificar os ativos quanto à Confidencialidade, Integridade e Disponibilidade (CIA);

2.3.16.5. Deve utilizar as informações de CIA do ativo para pontuar o risco do ativo;

2.3.16.6. Deve permitir o gerenciamento de baselines de configuração dos ativos, que podem ser comparados com as novas avaliações para a determinação de desvios;

2.3.16.7. Deve permitir o gerenciamento de permissões em arquivos, através de workflow de coleta/revisão/aprovação;

2.3.16.8. Deve ter compatibilidade com o protocolo SCAP (Security Content Automation Protocol);

2.3.17. Relatórios Gerais

2.3.17.1. Deverá informar semanalmente quanto às informações de usabilidade de dados estruturados e não estruturados, indicando minimamente o proprietário do arquivo, o último usuário e o maior usuário deste arquivo;

2.3.17.2. Deverá informar semanalmente quanto aos registros históricos e acessibilidade dos arquivos não estruturados, validando as atividades, monitorando arquivos e diretórios confidenciais;

2.3.17.3. Deverá informar semanalmente quanto aos arquivos não estruturados quanto ao uso suspeito, obtendo seu histórico de uso, bloqueando seu uso caso necessário, prevenindo contra futuros furos de segurança;

2.3.17.4. Deve ter a capacidade de emitir relatórios conforme a norma PCI 3.0;

2.3.17.5. Permitir o agendamento de geração de relatórios periódicos e notificar/enviar automaticamente os relatórios gerados para os destinatários dos mesmos;

2.3.17.6. Possuir a capacidade de executar o gerenciamento, administração, configuração, customização de relatórios e subsistemas da solução, criação de regras de pré-processamento, visualização de eventos e acompanhamento da disponibilidade da solução.

2.3.18. Visualização e Relatórios

2.3.18.1. A visualização e relatórios são subsistemas para a visualização de

eventos de forma centralizada.

2.3.18.2. Possuir acesso seguro e criptografado de forma a garantir a autenticidade, confidencialidade e integridade dos dados.

2.3.18.3. Permitir a pesquisa nos eventos históricos, fornecendo capacidade de "drill-down", ou seja, visualizar os detalhes dos eventos, quando aplicável, para análise forense e investigação de incidentes;

2.3.19. Relatórios e Forense

2.3.19.1. Deverá ter capacidade de agendar relatórios de segurança em múltiplos perfis. Os relatórios deverão ser gerados automaticamente (agendados) com frequência e intervalo de tempo a serem definidos pelo órgão, conforme perfis dos elementos gerenciados.

2.3.19.2. Os relatórios deverão ser exportados no mínimo para os seguintes formatos: CVS, PDF, HTML/XML.

2.3.19.3. Deverá possuir modelos de relatório pré-definidos (operacionais e gerenciais).

2.3.19.4. Deverá suportar acesso ao módulo de relatórios através de cliente ou WEB, com suporte a autenticação e controle de acesso por usuário.

2.3.19.5. Deve prover relatórios do grau de conformidade com normas reguladoras de mercado.

2.3.19.6. Apresentar as análises de ameaças e relatórios de conformidade pré-definidas

2.3.20. Solução para a Gestão e Análise de Ambiente Usuários

2.3.20.1. A solução deve executar as seguintes funcionalidades complementares: gerar relatórios de conformidade do escopo de ativos monitorado, com as políticas, controles e normas internas e externas, a critério do Contratante, além de relatórios técnicos e gerenciais;

2.3.20.2. A solução deve garantir redundância e operar em alta disponibilidade, sem a necessidade de operar em cluster, provendo todos os equipamentos e recursos necessários ao seu completo funcionamento, bem como se adaptar à configuração dos ativos e ao ambiente de rede do Contratante, e não deve exigir nenhuma modificação de arquitetura, permitindo coleta de informações com ou sem instalação de software em ativos do Contratante, exceto para os ativos que o Contratante julgar necessário possuir agentes para a coleta de eventos;

2.3.21. Console de Gerenciamento e Características Gerais

2.3.21.1. A solução deverá manter disponível de forma on-line todos os eventos capturados durante o período mínimo de 40 (quarenta dias), fornecendo, inclusive, a capacidade de armazenagem de dados suficiente para atender a este item;

2.3.21.2. A solução poderá ser constituída de hardware e software, appliance (hardware com software embarcado) ou virtual appliance;

2.3.21.3. No caso da solução ofertada ser composta de módulos, sua integração deverá ser nativa. Entende-se como integração nativa a comunicação entre os módulos sem a utilização de conectores externos, softwares de conexão de terceiros, exportação de dados ou quaisquer outros recursos de conectividade que necessitem de um sistema e/ou programa extra

para essa comunicação;

2.3.21.4. Deve permitir gerenciar mais de um servidor de gateway a partir da mesma console;

2.3.21.5. Deve permitir definir políticas individuais por servidor de gateway e globais, a partir da mesma console;

2.3.21.6. Deve possuir capacidade de administrar de forma unificada, via interface Web (com criptografia), com diversos níveis de acesso (administração, relatórios, quarentena, apenas leitura);

2.3.21.7. Deve possuir possibilidade de acesso individual ao appliance via SSH, para execução de comandos via CLI (linha de comando);

2.3.22. Módulo de Gerência

2.3.22.1. Possuir integração com base de conhecimento sobre atividades anômalas na Internet (origens de ataques, protocolos, etc), obtida automaticamente do site do Fabricante, permitindo a correlação dinâmica dessas informações com os dados coletados na rede local, possibilitando ainda integração com o módulo de Serviço de Segurança Proativa com Inteligência de Detecção;

2.3.22.2. A atualização da base de conhecimento sobre atividades anômalas na Internet deverá possuir periodicidade mínima diária;

2.3.22.3. O processo de detecção de vulnerabilidade deve levar em consideração a normalização e base de conhecimento do fabricante, envolvendo efeitos, recursos e mecanismos utilizados;

2.3.22.4. Permitir a criação de tickets de resolução de incidentes. Possibilidade de incluir no Ticket os artigos da base de conhecimento relevantes ao incidente, e também permitir a inserção de tarefas adicionais manualmente;

2.3.22.5. Fabricante da solução deve possuir laboratórios de pesquisa próprios, com visão global para detecção de novas ameaças e vulnerabilidades, para fornecer atualizações automáticas diárias para correlação dos eventos locais coletados;

2.3.22.6. Deve ter a capacidade de informar das vulnerabilidades e conformidades em ambiente Windows e Linux podendo executar a detecção de hotfixes, service packs, registros, peer to peer, Antivírus, juntamente com atualizações periódicas no mínimo diárias, recebidas quanto às vulnerabilidades mais recentes, IPs de BOT-NET, IPs maliciosos, Exploids, minimizando desta forma, os incidentes relacionados com os dados sensíveis, através da integração com o módulo de Serviço de Segurança Proativa com Inteligência de Detecção;

2.3.22.7. Deverá ter a capacidade de obter às informações de usabilidade de dados estruturados e não estruturados, indicando minimamente o proprietário do arquivo, o último usuário e o maior usuário deste dado;

2.3.22.8. Deverá ter a capacidade de obter quanto aos registros históricos e acessibilidade dos dados não estruturados, validando as atividades, monitorando arquivos e diretórios confidenciais, integrando a utilização dessas informações sensíveis sem autorização, alertando quanto a uma possível fuga de dado;

2.3.22.9. Deverá ter a capacidade de obter quanto aos dados não estruturados, seu uso suspeito, obtendo histórico de uso, bloqueando o uso caso necessário, prevenindo contra futuros furos de segurança;

2.3.22.10. Deve ter a capacidade de importar individualmente ativos para a verificação, possibilitando categorizar por qual tipo de ativo será importado;

2.3.22.11. Ter a capacidade de carregar a console de administração em um computador remoto;

2.3.23. Controles Procedurais:

2.3.23.1. Deve possuir um módulo de criação e publicação de questionários para usuários e análise de resultados, via web;

2.3.23.2. Deve permitir determinar peso para cada pergunta e nível de risco para cada resposta;

2.3.23.3. Deve permitir cascateamento de perguntas, de acordo com a resposta escolhida (ex: se respondeu "A" pule para pergunta "X", se respondeu "B" pule para pergunta seguinte);

2.3.23.4. Deve possuir console de administração de políticas integrado ao módulo de avaliação de controles técnicos, compartilhando a mesma infraestrutura de console, servidor e base de dados;

2.3.24. Modulo de Análise do Negócio

2.3.24.1. Capacidade de monitorar a redução do risco de negócio ao longo do tempo;

2.3.24.2. Capacidade de definir limites de risco de negócio, alertas e notificações em dashboards para melhor controlar os níveis de risco de TI;

2.3.24.3. Capacidade de visualizar a exposição ao risco de negócio, analisar o histórico de tendências para ilustrar como o risco e o programa de conformidade esta reduzindo sistematicamente os riscos para o negócio ao longo do tempo;

2.3.24.4. Capacidade de priorizar os esforços de remediação com base no risco do negócio, em vez de severidade técnica;

2.3.24.5. Capacidade de transformar os riscos de TI em métricas do risco de negócios relevantes, podendo ser compartilhadas com as principais partes interessadas para conduzir a consciência, prestação de contas e ação sobre os mesmos;

2.3.24.6. Deve permitir a criação de um novo padrão procedural através da cópia de um padrão procedural pré-definido, permitindo alteração das perguntas e respostas pré-definidas;

2.3.24.7. Deve possuir um módulo de criação e publicação de questionários para usuários e análise de resultados, via web;

2.3.24.8. Deve permitir determinar peso para cada pergunta e nível de risco para cada resposta;

2.3.24.9. Deve permitir cascateamento de perguntas, de acordo com a resposta escolhida (ex: se respondeu "A" pule para pergunta "X", se respondeu "B" pule para pergunta seguinte);

2.3.24.10. Deve permitir publicar os questionários via web, enviando um e-mail de convite para os usuários alvo, acessando o questionário e

respondendo pelo seu navegador de internet;

2.3.24.11. Deve possuir visualização gráfica do resultado do questionário, indicando por código de cores qual o risco computado de cada seção e perguntas;

2.3.24.12. Deve possuir console de administração de políticas integrado ao módulo de avaliação de controles técnicos, compartilhando a mesma infra-estrutura de console, servidor e base de dados;

2.3.24.13. Deve possuir um workflow de gerenciamento de políticas escritas, desde a edição a publicação para usuários;

2.3.24.14. Deve possuir um repositório de políticas com workflow de edição, permitindo trabalhar a política através de fases com níveis de acesso diferenciado (ex: Rascunho, Em Revisão, Revisada, Aprovada, Publicada);

2.3.24.15. Deve permitir a definição dos objetivos de risco da organização, bem como a associação a eles dos ativos (de tecnologia e de negócio), e dos controles que serão implementados/monitorados para verificar o nível de risco da organização;

2.3.24.16. Os controles devem poder ser combinados através de pesos, para que seja possível mapear com precisão a sua relevância na gestão do objetivo de risco;

2.3.24.17. Deve permitir a definição de thresholds para acompanhar e monitorar a pontuação de risco;

2.3.24.18. Deve permitir a definição de planos de remediação/ação ou de exceção e associá-los aos objetivos de risco definidos;

2.3.24.19. Os planos de ação devem ser editáveis quando nos estágios Rascunho, Erro, Enviado, Em Progresso, Em Pausa ou Concluído. Devem ainda ter os estágios Fechado, Expirado e Rejeitado, nos quais a edição não é permitida;

2.3.24.20. Através dos planos de ação deve ser possível estimar o risco projetado após a sua implementação;

2.3.24.21. Deve oferecer dashboards dinâmicos, com capacidade de drill down, para a análise detalhada e gestão dos riscos.

2.3.24.22. Deve permitir ao usuário clicar numa opção que registre sua aceitação a política, rejeição, e também registrar dúvidas e solicitar exceção a política;

2.3.25. Relatórios Gerais

2.3.25.1. Deverá informar semanalmente quanto às informações de usabilidade de dados estruturados e não estruturados, indicando minimamente o proprietário do arquivo, o último usuário e o maior usuário deste arquivo;

2.3.25.2. Deverá informar semanalmente quanto aos registros históricos e acessibilidade dos arquivos não estruturados, validando as atividades, monitorando arquivos e diretórios confidenciais;

2.3.25.3. Deverá informar semanalmente quanto aos arquivos não estruturados quanto ao uso suspeito, obtendo seu histórico de uso, bloqueando seu

uso caso necessário, prevenindo contra futuros furos de segurança;

2.3.25.4. Deve ter a capacidade de emitir relatórios conforme a norma PCI 3.0;

2.3.25.5. Permitir o agendamento de geração de relatórios periódicos e notificar/enviar automaticamente os relatórios gerados para os destinatários dos mesmos;

2.3.25.6. Possuir a capacidade de executar o gerenciamento, administração, configuração, customização de relatórios e subsistemas da solução, criação de regras de pré-processamento, visualização de eventos e acompanhamento da disponibilidade da solução.

2.3.26. Visualização e Relatórios

2.3.26.1. A visualização e relatórios são subsistemas para a visualização de eventos de forma centralizada.

2.3.26.2. Possuir acesso seguro e criptografado de forma a garantir a autenticidade, confidencialidade e integridade dos dados.

2.3.26.3. Permitir a pesquisa nos eventos históricos, fornecendo capacidade de "drill-down", ou seja, visualizar os detalhes dos eventos, quando aplicável, para análise forense e investigação de incidentes;

2.3.27. Relatórios e Forense

2.3.27.1. Deverá ter capacidade de agendar relatórios de segurança em múltiplos perfis. Os relatórios deverão ser gerados automaticamente (agendados) com frequência e intervalo de tempo a serem definidos pelo órgão, conforme perfis dos elementos gerenciados.

2.3.27.2. Os relatórios deverão ser exportados no mínimo para os seguintes formatos: CVS, PDF, HTML/XML.

2.3.27.3. Deverá possuir modelos de relatório pré-definidos (operacionais e gerenciais).

2.3.27.4. Deverá suportar acesso ao módulo de relatórios através de cliente ou WEB, com suporte a autenticação e controle de acesso por usuário.

2.3.27.5. Deve prover relatórios do grau de conformidade com normas reguladoras de mercado.

2.3.27.6. Apresentar as análises de ameaças e relatórios de conformidade pré-definidas;

2.4. Implantação.

2.4.1. A implantação dessa solução se dará através de arquivo de licença e será realizada mediante a substituição das atuais licenças já adquiridas em 2009. O arquivo de licença deve disponibilizar acesso a servidor web contendo todos os softwares licenciados para instalação e upgrade das ferramentas fornecidas.

2.4.2. Em caso de novas soluções deve haver um acompanhamento técnico local por parte da Contratada visando a instalação e configuração inicial do Software e/ou equipamento.

2.5. Capacitação

2.5.1. A Contratada deverá repassar ao Contratante todas as informações solicitadas e

documentação exigida no Documento;

2.5.2. Deverá ser fornecido repasse de conhecimento customizado para o ambiente do Contratante da(s) solução(ões) adquirida(s);

2.5.3. O treinamento deverá ser ministrado por técnico certificado com certificações técnicas (não comerciais e/ou técnica-comercial) pelo fabricante nos componentes da solução ofertada;

2.5.4. O treinamento deverá capacitar as equipes locais e as do Contratante principal a operar, configurar, administrar e resolver problemas usuais na solução ofertada, englobando tanto os componentes de hardware quanto de software ofertados;

2.5.5. Deverá ser fornecido certificado de conclusão emitido pelo fabricante.

2.6. Segurança da informação

2.6.1. Atendimento à legislação, principalmente à Instrução Normativa GSI/PR nº 01, de 13.06.2008, do Gabinete de Segurança Institucional da Presidência da República, a qual disciplina a gestão de segurança da Informação e Comunicações na Administração Pública Federal, bem como ao Decreto nº 3505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

2.6.2. Atendimento à Política de Segurança da Informação e Comunicações do Contratante - Portaria MAPA nº 795, de 5 de setembro de 2012.

CLÁUSULA TERCEIRA - VIGÊNCIA

3.1 O Contrato terá vigência pelo período de: 09/**dezembro/2016 a** 09/**dezembro/2017**, não eximindo a Contratada de cumprir com o prazo da garantia de funcionamento, estabelecido no Termo de Referência - Anexo do **Pregão Eletrônico nº 21/2015-MAPA** e no **Termo de Referência** constante do **Processo Administrativo de Contratação n.º 48000.001679/2016-56-MME.**

CLÁUSULA QUARTA – PREÇO

4.1 O valor do presente Termo de Contrato é de **R$ 462.000,00** (quatrocentos e sessenta e dois mil reais).

Lote	Item	Descrição	Qtd	Valor Unitário	Valor Total
1	8	Aquisição de Solução para Prevenção de Ataques Direcionados, Symantec Advanced Threat Protection – Usuários	1200	R$ 385,00	R$ 462.000,00

4.1.1 No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução contratual, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação;

CLÁUSULA QUINTA – DOTAÇÃO ORÇAMENTÁRIA

5.1 As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria, prevista no orçamento da União, para o exercício de 2016, na classificação

abaixo:

Programa de Trabalho:	25.122.2119.2000.0001
PTRES:	091626
Natureza de Despesa:	44.90.39
UGR:	320016

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

CLÁUSULA SEXTA – PAGAMENTO

6.1 O pagamento será efetuado em até 30 (trinta) dias após recebimento definitivo e o ateste do objeto contratado pelo fiscal do Contrato, conforme disposto no Art. 73 da Lei nº 8.666/93, observado o disposto no Art. 36, § 3º da IN nº 02, de 30 de abril de 2008, mediante Ordem Bancária, por intermédio do Banco do Brasil - 001 Agência: 3413-4 e Conta Corrente nº 710710-2;

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

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

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

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

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

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

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

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

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

EM = I x N x VP, onde:
I = Índice de atualização financeira;

TX = Percentual da taxa de juros de mora anual;
M = Encargos moratórios;
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = Valor da parcela em atraso.

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

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

6.12 O Contratante não fará nenhum pagamento a Contratada antes de paga ou relevada a multa que porventura lhe tenha sido aplicada;

6.13 O Contratante rejeitará, todo ou em parte, qualquer material fornecido com imperfeições ou que contenha especificação dessemelhante ao objeto;

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

6.15 A Contratada regularmente inscrita no Simples Nacional, nos termos da LC nº 123 de 2006, não sofrerá a retenção tributária. No entanto, o pagamento ficará condicionado à apresentação de comprovação por meio de documento oficial de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar, a fim de evitar a retenção na fonte de tributos e contribuições, conforme legislação em vigor;

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

6.17 A quantia recebida indevidamente será descontada dos pagamentos devidos à Contratada, devendo o Contratante notificá-la do desconto e apresentar a correspondente memória de cálculo;

6.18 **PARÁGRAFO SEGUNDO** - Na hipótese de inexistirem pagamentos a serem efetuados, o Contratante deverá notificar a Contratada para que recolha, no prazo máximo de 05 (cinco) dias úteis da data do recebimento do comunicado, a quantia paga indevidamente, por meio da Guia de Recolhimento da União – GRU, a ser preenchida e impressa no sítio do Tesouro Nacional (www.tesouro.fazenda.gov.br) a com os seguintes campos:

Unidade Favorecida: Código 320004 - Gestão 00001
Recolhimento: Código
Contribuinte: CPF/CNPJ - Nome - Valor do Documento:

CLÁUSULA SÉTIMA – GARANTIA DOS BENS

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

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

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

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

7.5 As manutenções preventivas e corretivas serão de responsabilidade da Contratada, sem custos adicionais ao Contratante;

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

CLÁUSULA OITAVA - GARANTIA CONTRATUAL

8.1 A garantia contratual corresponderá a **5%** do valor contratado. Neste caso o Contratante exigirá da Contratada, no ato da assinatura do Contrato, a prestação de garantia contratual pela execução das obrigações assumidas, cabendo à Contratada optar por uma das modalidades previstas em Lei: caução em dinheiro ou título da dívida pública, fiança bancária e seguro-garantia.

8.1.1 A Contratada deverá apresentar **garantia correspondente a 5%** (cinco por cento) do valor global do Termo de Contrato, no prazo máximo de **10 (dez) dias úteis**, prorrogáveis por igual período, a critério do Contratante, contado da assinatura do Termo de Contrato em favor do Contratante, no valor **R$ 23.100,00 (vinte e três mil e cem reais)**.

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

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

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

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

8.3.3 Multas moratórias e punitivas aplicadas pela Administração à Contratada;

8.3.4 Obrigações trabalhistas, fiscais e previdenciárias de qualquer natureza, não adimplidas pela Contratada.

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

8.5 A garantia em dinheiro deverá ser efetuada na em conta específica com correção monetária, em favor do Contratante;

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

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

8.8 O garantidor não é parte interessada para figurar em processo administrativo instaurado pelo Contratante com o objetivo de apurar prejuízos e/ou aplicar sanções à Contratada;

8.9 A garantia será considerada extinta:

8.9.1 Com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da Administração, mediante termo circunstanciado, de que a Contratada cumpriu todas as cláusulas do Termo de Contrato;

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

8.11 Se a garantia for utilizada em pagamento de qualquer obrigação, a Contratada se obrigará a fazer a respectiva reposição, no prazo máximo de 48 horas (quarenta e oito) horas, a contar da data em que for notificada pelo Contratante;

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

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

8.14 A área responsável irá elaborar ofício autorizando a Contratada a retirar o valor, junto a instituição em que se encontra a garantia;

CLÁUSULA NONA - CONDIÇÕES DE ENTREGA E RECEBIMENTO

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

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

9.3 O prazo de entrega do objeto contratado é de 30 dias corridos, contados da assinatura do Contrato, em remessa única, no seguinte endereço: Esplanada dos Ministérios, Bloco U, Sede do Ministério de Minas e Energia, Térreo, na Coordenação Geral de Tecnologia da Informação – CGTI, Brasília, DF, CEP: 70065-900 - telefone (61) 2032-5646;

9.4 O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da Contratada pelos prejuízos resultantes da incorreta execução do Termo de Contrato, devendo obedecer às disposições contidas no **ITEM 16 – MODELO DE GESTÃO DE CONTRATO do Termo de Referência/MME** – Anexo deste Contrato.

CLÁUSULA DÉCIMA - FISCALIZAÇÃO

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

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

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

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

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

10.6 A fiscalização exercida pelo Contratante não excluirá ou reduzirá a responsabilidade da Contratada pela completa e perfeita execução dos serviços/fornecimento dos bens;

10.7 Os esclarecimentos solicitados pela fiscalização deverão ser prestados imediatamente;

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

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

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

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

CLÁUSULA DÉCIMA PRIMEIRA - OBRIGAÇÕES DO CONTRATANTE

11.1 O fornecimento do objeto, bem como as obrigações da Contratada, não reduz, diminui, exime ou exclui as obrigações do Contratante perante o fornecimento do objeto;

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

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

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

11.5 O Contratante se obriga a prestar todos os esclarecimentos necessários para a Contratada cumprir com as suas obrigações;

11.6 Comunicar oficialmente a Contratada quaisquer falhas verificadas no cumprimento do Termo de Contrato;

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

11.8 Consoante o artigo 45 da Lei nº 9.784, de 1999, a Administração Pública poderá, sem a

prévia manifestação do interessado, motivadamente, adotar providências acauteladoras;

11.9 Receber o objeto no prazo e condições estabelecidas neste Contrato;

11.10 Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes deste Contrato, para fins de aceitação e recebimento definitivo;

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

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

CLÁUSULA DÉCIMA SEGUNDA - OBRIGAÇÕES DA CONTRATADA

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

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

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

12.4 Não serão aceitos pela Administração quaisquer alegações por parte da Contratada quanto ao desconhecimento das condições descritas;

12.5 Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Edital e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: *marca, fabricante, modelo, procedência e prazo de garantia ou validade;*

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

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

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

12.9 Comunicar ao Contratante, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

12.10 Qualquer anormalidade no fornecimento será de responsabilidade única e exclusiva da Contratada;

12.11 No caso de pedido de suspensão do fornecimento solicitado exclusivamente pelo

Contratante, a Contratada deverá imediatamente suspendê-los até segunda ordem;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

12.26 Assumir inteira responsabilidade por quaisquer danos ou prejuízos causados por seus empregados ou por terceiros sob sua responsabilidade, por negligência, imprudência ou imperícia, não se excluindo ou reduzindo essa responsabilidade em razão da fiscalização ou do acompanhamento realizado pelo Contratante.

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

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

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

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

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

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

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

12.34 Providenciar a assinatura do Termo de Compromisso, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes no Contratante, pelo representante legal da CONTRATADA, conforme ANEXO I deste Contrato;

12.35 Providenciar a assinatura do Termo de Ciência da Declaração de Manutenção de Sigilo e das Normas de Segurança vigentes no Contratante, por todos os empregados da Contratada diretamente envolvidos na contratação, conforme modelo constate do Termo de Referência anexo deste Contrato.

12.36 Vedar a utilização, na execução dos serviços, de empregado que seja familiar de agente público ocupante de cargo em comissão ou função de confiança no órgão Contratante, nos termos do artigo 7° do Decreto n° 7.203, de 2010.

CLÁUSULA DÉCIMA TERCEIRA – ALTERAÇÃO SUBJETIVA

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

CLÁUSULA DÉCIMA QUARTA – SUBCONTRATAÇÃO

14.1 Não será admitida a subcontratação do objeto contratado.

CLÁUSULA DÉCIMA QUINTA - SANÇÕES ADMINISTRATIVAS

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

I – advertência;

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

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

IV – declaração de inidoneidade para licitar ou contratar com o Órgão Sancionador enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior;

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

VI - declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir o Contratante pelos prejuízos causados.

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

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

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

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

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

Grau	Correspondência
1	Advertência por ocorrência
2	0,1% do valor mensal do contrato, por ocorrência e até o 30º dia
3	0,2% do valor mensal do contrato, por ocorrência e até o 30º dia
4	0,1% do valor do contrato, até o 30º dia
5	0,2% do valor do contrato, após o 31º dia, licitado a 10% do valor total do contrato
6	5% do valor do contrato, por ocorrência, limitado a 10%
7	20% do valor do contrato, ensejando seu desfazimento

15.7 Abaixo consta a relação das inexecuções totais ou parciais:

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

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

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

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

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

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

15.13 A autoridade competente na aplicação das sanções levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade;

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

CLÁUSULA DÉCIMA SEXTA - RESCISÃO

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