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

CONTRATO Nº 34/2019

PROCESSO nº 08700.002988/2018-01

CONTRATO DE PRESTAÇÃO DE SERVIÇOS E FORNECIMENTO DE BENS QUE ENTRE SI CELEBRAM O CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA - CADE E A EMPRESA PISOTEC COMÉRCIO E SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO EIRELI PARA A CONTRATAÇÃO DE SOLUÇÃO DE SEGURANÇA E CONTROLE PATRIMONIAL.

CONTRATANTE:

CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA - Cade, AUTARQUIA FEDERAL, vinculada ao Ministério da Justiça, criada pela Lei nº 8.884, de 11 de junho de 1994, com sede no SEPN 515, Conjunto D, Lote 4, Ed. Carlos Taurisano, CEP 70.770-504, em Brasília–DF, inscrita no CNPJ/MF sob o nº 00.418.993/0001-16, doravante designado Contratante, neste ato representado por sua Ordenadora de Despesa pro Subdelegação, Sra. **LUANA NUNES SANTANA**, brasileira, portadora Carteira de Identidade n.º 28153792-6 – SSP/SP e do CPF n.º 221.509.228-94, no uso da atribuição que lhe confere o art. 1º, inciso II, alínea "b", da Portaria n.º 460, de 29 de setembro de 2012; e

CONTRATADA:

PISONTEC COMÉRCIO E SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO EIRELI, inscrita no CNPJ/MF sob nº 12.0007.998/0001-35, com sede no endereço Av. Presidente Gétulio Vargas, 1038 - Sala 03 CXPST 118, Bairro Novo - Olinda/PE, CEP: 53.030-010, fones: (81) 3257-5110 e (81) 98389-2210, e-mail gestao.licitacao@pisotec.com / licitacao@pisotec.com / qualidade@pisotec.com.br, doravante denominado(a) **CONTRATADA**, neste ato representado a por sua representante legal, **Sra. CARLA PATRICIA CARVALHO DA SILVA**, Identidade nº 369.5682 SDS/PE CPF nº 855.883.0004-59, devidamente qualificado, na forma da Lei nº 8.666, de 21 de junho de 1993, tendo em vista o que consta no Processo nº 08700.002988/2018-01, resolvem celebrar o presente **CONTRATO,** sujeitando-se as partes ao comando da Lei n. 10.520, de 17 de julho de 2002 e Lei 8.666, de 21 de junho de 1993 e alterações posteriores e demais normas pertinentes, observadas as cláusulas e condições seguintes:

DA FINALIDADE

O presente Contrato tem por finalidade formalizar e disciplinar o relacionamento contratual com vistas à execução dos trabalhos definidos e especificados na Cláusula Primeira – DO OBJETO, conforme Parecer Jurídico nº 126/2018, datado de 13/11/2018, da Procuradoria do Contratante exarada no Processo nº 08700.002988/2018-01.

DO FUNDAMENTO LEGAL

O presente Contrato decorre de adjudicação à Contratada do objeto do Pregão Eletrônico nº 12/2018, com base, integralmente, a Lei nº 10.520, de 19 de julho de 2002, publicada no D.O.U. de 22 de julho de 200; a Lei nº 8.078, de 11 de setembro de 1990, publicada no D.O.U de 12 de setembro de 1990; a Lei n° 12.529 de 30 de novembro de 2011, publicada no D.O.U. de 1° de novembro de 2011; o Decreto nº 3.555, de 08 de agosto de 2000, publicado no D.O.U. de 09 de agosto de 2000, o Decreto. nº 5.450, de 31 de maio de 2005, que regulamentam a modalidade de Pregão; a IN-SLTI/MP nº. 05/2017; Decreto nº 8.538/2015, que estabelece o tratamento diferenciado para as MEs e EPPs; a Instrução Normativa nº 1, de 19 de janeiro de 2010 a Instrução Normativa nº 02 da SLTI/MPOG, de 11 de outubro de 2010; a Instrução Normativa nº SLTI 04/2014 e, subsidiariamente, pela Lei nº 8.666/93 e alterações posteriores, conforme especificações constantes do Processo Administrativo nº 08700.002988/2018-01.

1. **CLÁUSULA PRIMEIRA - DO OBJETO**

1.1. Contratação de soluções de segurança para computadores, dispositivos móveis, servidores, caixas de email e proteção contra ataques persistentes avançados, provendo ao Conselho Administrativo de Defesa Econômica - Cade - capacidade de gerenciamento e proteção de ativos de tecnologia da informação na autarquia.

2. **CLÁUSULA SEGUNDA – DA VINCULAÇÃO**

2.1. O presente Contrato vincula-se, independentemente de transcrição, à proposta da Contratada, ao Edital do Pregão Eletrônico nº 12/2018, com seus Anexos e os demais elementos constantes do Processo nº 08700.002988/2018-01.

3. **CLÁUSULA TERCEIRA - DO LOCAL E DA FORMA DE PRESTAÇÃO DO SERVIÇO**

3.1. Os serviços serão prestados ao Conselho Administrativo de Defesa Econômica - Cade, em local a ser indicado conforme o caso, sempre dentro do Distrito Federal.

3.2. O local de execução dos serviços será no próprio espaço físico do Cade, localizado no SEPN, Quadra 515, conjunto D, Lote 04 – Asa Norte, Brasília/DF, nos termos do art. 9º da Portaria Cade nº 245/2018.

4. **CLÁUSULA QUARTA- DA DISCRIMINAÇÃO DOS SERVIÇOS**

Grupo	Item	Descrição	Unidade de medida	Órgão Gerenciador
1	1	Solução para segurança de computadores (500 entre desktops e laptops) e dispositivos móveis (200 entre tablets e smartphones Android e iOS) com ferramenta de gerência centralizada, instalação e suporte técnico, garantia e atualizações pelo período de 60 (sessenta) meses	Unidade	200
	2	Treinamento na solução de segurança de computadores e dispositivos móveis	Pessoa	2
	3	Solução para segurança de servidores (Linux e Windows) com ferramenta de gerência centralizada, instalação	Unidade	100

		e suporte técnico, garantia e atualizações pelo período de 60 (sessenta) meses		
	4	Treinamento na solução de segurança de servidores	Pessoa	2
	6	Treinamento na solução de proteção de caixas de e-mail e servidores Microsoft Exchange	Pessoa	2
	8	Treinamento na solução para proteção contra ameaças persistentes avançadas	Pessoa	2

4.1. **DOS REQUISITOS TECNOLÓGICOS**

CONSOLE ADMINISTRATIVA CENTRALIZADA

4.1.1. A console deve ser acessada via WEB (HTTPS) ou MMC

4.1.2. Console deve ser baseada no modelo cliente/servidor;

4.1.3. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;

4.1.4. Console deve ser totalmente integrada com as funcionalidades e módulos da Solução;

4.1.5. As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;

4.1.6. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;

4.1.7. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;

4.1.8. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;

4.1.9. A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças contratadas;

4.1.10. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;

4.1.11. Capacidade de instalar remotamente a solução de segurança em smartphones e tablets;

4.1.12. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;

4.1.13. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux) protegidos pela solução antivírus;

4.1.14. Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança;

4.1.15. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;

4.1.16. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;

4.1.17. A comunicação entre o cliente e o servidor de administração deve ser criptografada;

4.1.18. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

4.1.18.1. Nome do computador;

4.1.18.2. Nome do domínio;

4.1.18.3. Range de IP.

4.1.19. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;

4.1.20. Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional;

4.1.21. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;

4.1.22. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção;

4.1.23. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;

4.1.24. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;

4.1.25. Deve fornecer as seguintes informações dos computadores:

4.1.25.1. Se o antivírus está instalado;

4.1.25.2. Se o antivírus está iniciado;

4.1.25.3. Se o antivírus está atualizado;

4.1.25.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo;

4.1.25.5. Minutos/horas desde a última atualização de vacinas;

4.1.25.6. Data e horário da última verificação executada na máquina;

4.1.25.7. Versão do antivírus instalado na máquina;

4.1.25.8. Se é necessário reiniciar o computador para aplicar mudanças;

4.1.25.9. Data e horário de quando a máquina foi ligada;

4.1.25.10. Quantidade de vírus encontrados (contador) na máquina;

4.1.25.11. Nome do computador;

4.1.25.12. Domínio ou grupo de trabalho do computador;

4.1.25.13. Data e horário da última atualização de vacinas;

4.1.25.14. Sistema operacional com Service Pack;

4.1.25.15. Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);

4.1.25.16. Endereço IP;

4.1.25.17. Vulnerabilidades de aplicativos instalados na máquina.

4.1.26. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;

4.1.27. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão.

4.1.28. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;

4.1.29. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;

4.1.30. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;

4.1.31. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;

4.1.32. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;

4.1.33. Capacidade de gerar e exportar relatórios;

4.1.34. Capacidade de gerar traps SNMP para monitoramento de eventos;

4.1.35. Capacidade de enviar e-mails para contas específicas em caso de algum evento;

4.1.36. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);

4.1.37. Capacidade de realizar atualização incremental de vacinas nos computadores clientes.

4.1.38. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus; e

4.1.39. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores.

SOLUÇÃO DE SEGURANÇA PARA COMPUTADORES (ENDPOINTS)

Proteção antimalware

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

4.1.40.1. Windows 7 (x86/x64);

4.1.40.2. Windows 10 (x86/x64);

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

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

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

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

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

4.1.46. Deverá incluir regras específicas para detecção de ransomware;

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

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

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

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

4.1.48.3. Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip, exe, arj, mime/uu, Microsoft cab;

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

4.1.49. Deve possuir detecção heurística de vírus desconhecidos;

4.1.50. Deve permitir configuração de limitação ou disponibilização de recurso para a máquina caso esteja realizando uma varredura manual ou agendada;

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

4.1.51.1. Em tempo real de arquivos acessados pelo usuário;

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

4.1.51.3. Manual, imediato ou programável, com interface gráfica em janelas, personalizável, com opção de limpeza;

4.1.51.4. Por linha-de-comando, parametrizável, com opção de limpeza;

4.1.51.5. Automáticos do sistema com as seguintes opções:

- Escopo: todos os discos locais, discos específicos, pastas específicas ou arquivos específicos;
- Ação: somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena);
- Frequência: horária, diária, semanal e mensal;
- Exclusões: pastas ou arquivos (por nome e/ou extensão) que não devem ser rastreados;

4.1.52. Deve possuir mecanismo de cache de informações dos arquivos já escaneados;

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

4.1.54. Deve possuir ferramenta de alterações de parâmetros de comunicação entre o cliente antivírus e o servidor de gerenciamento da solução de antivírus;

4.1.55. Deve permitir a utilização de servidores locais ou em nuvem de reputação para análise de arquivos e URL's maliciosas, de modo a prover, rápida detecção de novas ameaças;

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

4.1.57. Deve ser capaz de detectar variantes de malwares que possam ser geradas em tempo real na memória da estação de trabalho ou notebook, permitindo que seja tomada ação de quarentenar a ameaça;

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

4.1.59. Deve permitir a restauração de maneira granular de arquivos quarentenados sob suspeita de representarem risco de segurança;

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

4.1.61. A solução de segurança para endpoints deverá integrar-se a tecnologias de análise de ameaças direcionadas/desconhecidas (grupo 1, item 7)**,** obedecendo as seguintes características:

4.1.61.1. A solução de segurança para endpoints deverá ser capaz de submeter automaticamente arquivos suspeitos a uma solução de análise de ameaças direcionadas/desconhecidas locais, não sendo realizada de maneira externa ao ambiente, apresentando como resultado da análise, no mínimo, as seguintes informações:

- Processos de AutoStart;
- Modificações de Arquivos de Sistema;
- Serviços criados e modificados;
- Atividade de Rede Suspeita;
- Modificações de Registros;

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

4.1.62.1. Microsoft Windows 7 em Português;

4.1.62.2. Windows XP em Português;

4.1.62.3. Microsoft Office: 2007, 2010 e 2013;

4.1.62.4. Adobe Reader: 9, X e XI;

4.1.62.5. Java;

4.1.62.6. Firefox;

4.1.62.7. Adobe Flash Player;

4.1.63. A solução de análise de ameaças direcionadas/desconhecidas deverá retroalimentar a solução de segurança de endpoints para que esse possa realizar automaticamente o bloqueio em ações suspeitas nos Desktops infectados com aquela ameaça analisada em sandbox;

Funcionalidade de Atualização

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

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

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

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

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

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

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

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

Funcionalidade de administração

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

4.1.73. Deve possibilitar instalação "silenciosa";

4.1.74. Deve permitir o bloqueio por nome de arquivo;

4.1.75. Deve permitir o rastreamento e bloqueio de infecções;

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

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

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

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

4.1.80. Deve ter a possibilidade de exportar/importar configurações da solução através da console de gerenciamento;

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

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

4.1.83. Deve permitir realização do backup da base de dados através de mapeamento de rede controlado por senha;

4.1.84. Deve permitir a deleção dos arquivos quarentenados;

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

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

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

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

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

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

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

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

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

4.1.94. Deve registrar no sistema de monitoração de eventos da console de antimalware informações relativas ao usuário logado no sistema operacional

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

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

4.1.97. Deve prover segurança através de comunicação criptografada entre o servidor e a console de gerenciamento web;

4.1.98. Deve prover segurança através de comunicação criptografada entre o servidor e os agentes de proteção;

4.1.99. Deve suportar múltiplas florestas e domínios confiáveis do Active Directory;

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

4.1.101. Deve permitir a criação de usuários locais de administração da console de antimalware;

4.1.102. Deve possuir a integração com o Active Directory para utilização de seus usuários para administração da console de antimalware;

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

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

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

4.1.106. Deve permitir a gerência de domínios através de usuários previamente definidos;

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

Funcionalidade de controle de dispositivos

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

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

4.1.110. Deve ser capaz de identificar smartphones e tablets como destinos de cópias de arquivos e tomar ações de controle da transmissão;

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

Funcionalidade de autoproteção

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

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

4.1.113.1. Autenticação de comandos IPC;

4.1.113.2. Proteção e verificação dos arquivos de assinatura;

4.1.113.3. Proteção dos processos do agente de segurança;

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

4.1.113.5. Proteção do diretório de instalação do agente de segurança;

Funcionalidade de HIPS – Host IPS e Host Firewall

4.1.114. Deve ser capaz de realizar a proteção nos seguintes sistemas operacionais:

4.1.114.1. Windows Server 2003, 2008, 2012 e superior (x86/x64);

4.1.114.2. Windows XP sp3 (x86/x64);

4.1.114.3. Windows 7 (x86/x64);

4.1.114.4. Windows 8 e 8.1 (x86/x64);

4.1.114.5. Windows 10 (x86/x64);

4.1.115. Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de HIPS e host firewall;

4.1.116. Todas as regras das funcionalidades de firewall devem permitir apenas detecção (log) ou prevenção (bloqueio);

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

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

4.1.119. Deve prover proteção contra as vulnerabilidades do sistema operacional Windows XP ou superior, por meio de regras de HIPS;

4.1.120. Deve efetuar varredura de segurança automática ou sob demanda que aponte vulnerabilidades de sistemas operacionais e aplicações e possibilite a aplicação de regras de host IPS para proteger a estação de trabalho ou notebook contra a possível exploração da vulnerabilidade;

4.1.121. Deve prover proteção contra as vulnerabilidades de aplicações terceiras, por meio de regras de host IPS, tais como oracle java, abobe pdf reader, adobe flash player, realnetworks real player, Microsoft office, apple itunes, apple quick time, apple safari, google chrome, mozilla firefox, opera browser, ms internet explorer, entre outras;

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

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

4.1.124. Deve permitir a emissão de alertas via smtp e snmp;

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

4.1.126. Deve permitir a criação de regras de firewall utilizando no mínimo os seguintes protocolos: ICMP, ICMPv6, IGMP, TCP, UDP.

4.1.127. Deve permitir a criação de regras de firewall por origem de IP ou MAC ou porta e destino de IP ou MAC ou porta;

4.1.128. Deve permitir a criação de regras de firewall por pelo menos um dos seguintes frame types: IP, IPv4, IPv6, ARP, REVARP.

4.1.129. Deve permitir a criação de grupos lógicos através de lista de IP, MAC ou portas;

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

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

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

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

Funcionalidade de controle de aplicações

4.1.134. Deve ser capaz de realizar o controle de nos seguintes sistemas operacionais:

4.1.134.1. Windows Server 2003, 2008, 2012 e superior (x86/x64);

4.1.134.2. Windows XP sp3 (x86/x64);

4.1.134.3. Windows 7 (x86/x64);

4.1.134.4. Windows 8 e 8.1 (x86/x64);

4.1.134.5. Windows 10 (x86/x64);

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

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

4.1.136.1. Range de endereços IPS;

4.1.136.2. Sistema operacional;

4.1.136.3. Grupos de máquinas espelhados do Active Directory;

4.1.136.4. Usuários ou grupos do Active Directory;

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

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

4.1.138.1. Nenhum;

4.1.138.2. Somente bloqueios;

4.1.138.3. Somente regras específicas;

4.1.138.4. Todas as aplicações executadas;

4.1.139. As políticas de segurança devem permitir o controle do intervalo de envio dos logs provenientes dos endpoints;

4.1.140. As políticas de segurança devem permitir o controle do intervalo para envio de atualização de cada política proveniente dos endpoints;

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

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

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

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

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

4.1.145.1. Permissão de execução;

4.1.145.2. Bloqueio de execução;

4.1.145.3. Bloqueio de novas instalações;

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

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

4.1.147.1. Assinatura SHA-1 do executável;

4.1.147.2. Atributos do certificado utilizado para assinatura digital do executável;

4.1.147.3. Caminho lógico do executável;

4.1.147.4. Base de assinaturas de certificados digitais válidos e seguros;

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

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

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

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

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

Funcionalidade de criptografia

4.1.153. Deve ser capaz de realizar a criptografia nos seguintes sistemas operacionais:

4.1.153.1. Windows 7 (x86/x64);

4.1.153.2. Windows 8 e 8.1 (x86/x64);

4.1.153.3. Windows 10 (x86 /x64);

4.1.154. Deve possuir módulo de criptografia para as estações de trabalho (desktops e notebooks), permitindo criptografia para: Disco completo (FDE – full disk encryption); Pastas e arquivos; Mídias removíveis; Anexos de e-mails ou Automática de disco;

4.1.155. Deve possuir autenticação durante a inicialização (boot) da estação de trabalho, antes do carregamento do sistema operacional, para a funcionalidade de criptografia do disco completo;

4.1.156. A autenticação durante a inicialização (boot) deve ser a partir das credenciais sincronizadas com o Active Directory;

4.1.157. Deve possuir suporte ao algoritmo de criptografia aes-256;

4.1.158. Deve possuir criptografia no canal de comunicação entre as estações de trabalho e o servidor de políticas;

4.1.159. Deve possuir certificação FIPS 140-2;

4.1.160. Deve possuir funcionalidade de criptografia por software ou hardware;

4.1.161. Deve possuir compatibilidade de autenticação por múltiplos fatores;

4.1.162. Deve permitir atualizações do sistema operacional mesmo quando o disco está criptografado;

4.1.163. Deve permitir que o administrador da solução forneça novas senhas ou usuários para o disco;

4.1.164. Deve possuir políticas por usuários, grupos e dispositivos;

4.1.165. Deve desbloquear um disco com no mínimo três dos seguintes métodos: Sequência de cores; Autenticação com AD; Single sign-on com AD; Senha pré-definida; Número PIN e Smartcard;

4.1.166. Deve possuir autoajuda para usuários que esquecerem a senha com a combinação de perguntas e respostas;

4.1.167. Deve possuir mecanismos de criptografia transparentes para o usuário;

4.1.168. Deve possuir mecanismo que permita desfazer a criptografia do disco no evento em que se torne corrompido, impedindo a inicialização da estação/notebook, ou seja, caso a máquina tenha sido reiniciada, assim retomando a tarefa quando houver o sistema operacional religado;

4.1.169. O acesso a este ambiente de execução de procedimentos de identificação de problema e realização de tarefas administrativos deve ser controlado através de política gerenciada remotamente pelo componente de gerenciamento da solução;

4.1.170. Deve prover ferramenta presente na estação de trabalho que possibilite migrá-la para um servidor de gerenciamento diferente;

4.1.171. Deve permitir a gerência das seguintes soluções terceiras de criptografia:

4.1.171.1. Microsoft bitlocker;

4.1.171.2. Apple filevault;

4.1.172. Deve permitir a visualização das estações de trabalho que tenham aplicação de política pendente a partir da console de administração centralizada;

4.1.173. Deve permitir a visualização do autor de determinada política a partir da console de administração centralizada;

4.1.174. Deve permitir a visualização de estações de trabalho que não possuam nenhuma política aplicada a partir da console de administração centralizada;

4.1.175. Deve permitir a adição de informações de contato a serem exibidas ao usuário final com texto customizável;

4.1.176. Deve permitir a exibição de aviso legal quando o agente de criptografia é instalado na estação de trabalho e quando a estação é inicializada;

4.1.177. Deve permitir, em nível de política, a indicação de pastas a serem criptografadas;

4.1.178. Deve possibilitar que cada política tenha uma chave de criptografia única;

4.1.179. Deve permitir, em nível de política, a escolha da chave de criptografia a ser utilizada, por exemplo:

4.1.179.1. Chave do usuário: somente o usuário tem acesso aos arquivos;

4.1.179.2. Chave da empresa: qualquer usuário da empresa tem acesso aos arquivos;

4.1.179.3. Chave da política: qualquer estação de trabalho que tenha aplicada a mesma política tem acesso aos arquivos;

4.1.180. Deve possibilitar a desativação de dispositivos de gravação de mídias óticas e de dispositivos de armazenamento USB;

4.1.181. Deve possibilitar o bloqueio da autenticação de usuários baseado no intervalo em que o dispositivo não tenha as políticas sincronizadas com o componente de administração centralizada;

4.1.182. Deve possibilitar a instauração de política de gerenciamento de complexidade e intervalo de troca de senha com os seguintes critérios:

4.1.183. Definição do intervalo de dias em que o usuário será forçado a mudar sua senha;

4.1.184. Possibilidade de definir senhas anteriores que não poderão ser reutilizadas como nova senha;

4.1.185. Definição do comprimento de caracteres mínimo a ser utilizado na nova senha;

4.1.186. Definição do número de caracteres especiais, caracteres numéricos, caracteres em caixa alta e caracteres em caixa baixa que deverão ser utilizados para a nova senha;

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

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

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

Solução para segurança de dispositivos móveis

4.1.190. O módulo de proteção de dispositivos móveis deve possuir agente para os seguintes sistemas operacionais:

4.1.191. Apple iOS 5.x, 7.x, 8.x ou superior;

4.1.192. Android OS 4.x, 5.x ou superior;

4.1.193. As funcionalidades estarão disponíveis de acordo com cada plataforma;

4.1.194. Deve possuir proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:

4.1.194.1. Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser;

4.1.194.2. Arquivos abertos no smartphone; e

4.1.194.3. Programas instalados usando a interface do smartphone.

4.1.195. Deve permitir o provisionamento de configurações de: Wi-fi, Exchange Activesync, vpn, proxy http global e certificados;

4.1.196. Deve possuir proteção de antimalware;

4.1.197. Deve ser capaz de realizar escaneamento de malwares em tempo real, do cartão sd e após atualização de vacinas;

4.1.198. Deve possuir capacidade de detecção de spam proveniente de SMS;

4.1.199. Deve permitir a proteção contra ameaças provenientes da web por meio de um sistema de reputação de segurança das URL's acessadas;

4.1.200. Deve permitir o controle de acesso a websites por meio de listas de bloqueio e aprovação;

4.1.201. Controle da política de segurança de senhas, com critérios mínimos de: Padrão de senha; Uso obrigatório de senha; Tamanho mínimo; Tempo de expiração; Bloqueio automático da tela; e Bloqueio por tentativas inválidas;

4.1.202. Controle de acesso às seguintes funções e status dos dispositivos móveis:

4.1.202.1. Bluetooth;

4.1.202.2. Câmera;

4.1.202.3. Wlan/wifi;

4.1.202.4. Instalação de aplicativos;

4.1.202.5. Sincronia automática enquanto em modo roaming;

4.1.202.6. Itunes, quando houver;

4.1.202.7. Imessage;

4.1.202.8. Browser / Navegadores internet incluindo Safari;

4.1.202.9. Captura de tela;

4.1.202.10. Youtube;

4.1.202.11. GPS;

4.1.202.12. Microsoft Activesync;

4.1.202.13. MMS/SMS;

4.1.202.14. Porta infravermelha; e

4.1.202.15. Armazenamento USB.

SOLUÇÃO DE SEGURANÇA PARA PROTEÇÃO DE SERVIDORES

4.1.203. Fornecer proteção para Servidores Físicos, Virtuais e em Nuvem;

4.1.204. A solução deverá permitir a implantação dos módulos de segurança, no mínimo para os seguintes sistemas operacionais:

4.1.204.1. Windows Server 2003, 2008, 2012 e versões superiores;

4.1.204.2. Sistemas Operacionais Linux, no mínimo para as distribuições: Red Hat, Suse, CentOs,Ubuntu e Debian;

4.1.205. Deve prover proteção de Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

4.1.206. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc);

4.1.207. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (*uninterruptible Power supply – UPS*);

4.1.208. Em caso de erros, deve ter capacidade de criar *logs* e *traces* automaticamente, sem necessidade de outros softwares;

4.1.209. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;

4.1.210. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;

4.1.211. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

4.1.212. Controle de vulnerabilidades do Windows e dos aplicativos instalados;

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

4.1.214. A solução deverá ser gerenciada por console de gerenciamento centralizado. Caso seja Web, suportando no mínimo os browsers Internet Explorer e Firefox.

4.1.215. A solução Deve suportar certificado digital para gerenciamento;

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

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

4.1.218. A solução deverá permitir que a distribuição de patterns e novos componentes possa ser efetuada por agentes de atualização espalhados pelo ambiente;

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

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

4.1.221. A solução deve permitir que relatórios no formato PDF, possam ser enviados para cada destinatário;

4.1.222. A console de gerenciamento deve armazenar políticas e logs em base de dados. A escolha da base de dados deve suportar no mínimo os bancos de dados Oracle e MS SQL;

4.1.223. A console deve se integrar com Microsoft Active Directory (AD) para que os usuários possam acessar a solução de acordo com as permissões que lhe forem atribuídas e para que possa ser efetuado o controle das máquinas no Active Directory;

4.1.224. A solução deverá suportar múltiplos níveis de permissões, podendo ainda customizá-las. Deverá incluir opções de permissionamento no mínimo para modos de visualização e edição de políticas;

4.1.225. Quando customizado o acesso, este deve permitir que um usuário tenha permissões de poder gerenciar a segurança de um único computador, podendo ainda definir em quais módulos de proteção será possível ou não editar ou criar novas politicas de segurança;

4.1.226. A solução deverá permitir a atribuição granular de permissões para servidores gerenciados podendo delimitar quais os servidores que podem ser visualizados e gerenciados para cada usuários ou grupo de usuários;

4.1.227. A comunicação entre a console de gerenciamento e os agentes deverá ser criptografada;

4.1.228. Cada agente deverá ter sua própria chave para criptografia de modo que a comunicação criptografada seja feita de forma diferente para cada agente;

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

4.1.230. Os agentes de atualização deverão buscar os updates das assinaturas e distribuí-las para os agentes. Quando ocorrer a atualização, esta deverá ocorrer de modo absolutamente seguro utilizando-se SSL com o servidor de onde ela buscará as informações;

4.1.231. Os agentes para plataforma Microsoft deverão ser instalados por pacote MSI e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente;

4.1.232. Os agentes para plataforma Linux deverão ser instalador por pacote RPM ou DEB e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente;

4.1.233. Para efeito de administração, deve ser possível replicar a estrutura do Active Directory na console de administração;

4.1.234. A solução deverá avisar quando um agente encontrar-se não conectado à sua console de gerenciamento;

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

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

4.1.237. A solução deverá vir com perfis default pré-definidos e aptos a funcionarem de acordo com sua denominação;

4.1.238. Deverá possuir uma hierarquia de prevalecimento de configurações, seguindo no mínimo a ordem: Global -> Perfis -> hosts;

4.1.239. Os agentes deverão ser capazes de executar rastreamento nas máquinas onde estão instalados e após isso deverão fornecer uma lista de todas as recomendações de segurança para os softwares que estejam instalados nas máquinas bem como do sistema operacional;

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

4.1.241. Brechas de segurança descobertas deverão ser protegidas de forma automática e transparente, interrompendo somente o tráfego de rede malicioso;

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

4.1.243. Deverá ser possível realizar o rastreamento por portas abertas, identificando possíveis serviços ativos;

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

4.1.245. A solução deverá ter a capacidade de se integrar com softwares SIEMs e SYSLOG Servers de modo a enviar os seus logs para essas soluções;

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

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

4.1.248. A solução deverão permitir que os relatórios sejam exportados para, no mínimo, os formatos PDF ou HTML;

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

4.1.250. As atualizações de assinaturas deverão ocorrer de forma agendada e automática possibilitando ser até mesmo de hora em hora;

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

4.1.252. Deve ser possível baixar as assinaturas na console de gerenciamento, mas não distribuí-las aos clientes;

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

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

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

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

4.1.257. Deverá possuir a capacidade de classificar eventos para que facilite a identificação e a visualização de eventos críticos em servidores críticos;

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

4.1.259. A solução deverá ser totalmente compatível e homologada para gerenciamento de máquinas virtuais nos ambientes HyperV e Vmware. Para cada plataforma de virtualização haverá uma forma diferente de integração, com ou sem agente, preservando no entanto a capacidade de implementação das funcionalidades (Antimalware, Firewall, IPS/IDS, Web Reputation, Monitoração de Integridade e Inspeção de Log’s);

4.1.260. Ter a capacidade de detectar e aplicar as regras necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs para cada servidor, de forma automática, ou pelo administrador;

4.1.261. A solução deverá incluir funcionalidades específicas de proteção contra Ransomware, incluindo reconhecimento de assinaturas e regras específicas de IDS/IPS para os servidores protegidos;

Funcionalidade de firewall

4.1.262. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

4.1.262.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

4.1.262.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados;

4.1.263. Operar como firewall de host stateful bidirecional monitorando as comunicações nos servidores protegidos;

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

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

4.1.266. A solução deverá ser capaz de reconhecer e possibilitar o bloqueio endereços IP que estejam realizando Network Scan, Port Scan, TCP Null Scan, TCP FYNSYN Scan, TCP Xmas Scan ou Computer OS Fingerprint por até 30 minutos.

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

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

4.1.269. Deverá permitir a criação e administração de regras de firewall, baseadas em objetos que podem ser lista de ips, lista de MACs, lista de portas;

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

4.1.271. O firewall deverá permitir liberar ou apenas logar eventos;

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

4.1.273. Deverá utilizar o conceito de regras implícitas para a regra ALLOW, negando o tráfego para todo o restante que não estiver liberado;

4.1.274. Deverá realizar pseudo stateful em tráfego UDP;

4.1.275. Deverá prevenir ack storm;

4.1.276. Deverão existir regras default que facilitem a criação e adição de novas regras;

Funcionalidade de inspeção de pacotes

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

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

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

4.1.280. Precisa conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem no mínimo os seguintes sistemas operacionais: Windows 2003, 2008 e 2012, além de aplicações padrão de mercado, tais como Microsoft IIS, SQL Server, Microsoft Exchange, Oracle Database, Adobe Acrobat, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome e Web Server Apache.

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

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

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

4.1.284. Deverá ser capaz de inspecionar tráfego incoming SSL;

4.1.285. As regras de blindagem contra vulnerabilidades deverão conter links com referências externas, isto quando aplicável, explicando a vulnerabilidade do fabricante ou CVE relacionado;

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

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

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

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

4.1.290. As regras de IPS de vulnerabilidade deverão apresentar severidade baseada para tratativa;

4.1.291. As regras de IPS poderão ter sua capacidade de LOG desabilitado;

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

4.1.293. As regras devem ser atualizadas pelo administrador da solução ou automaticamente pelo fabricante;

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

Funcionalidade de monitoramento de integridade

4.1.295. A solução deverá permitir a implantação da monitoração de integridade em uma das seguintes plataformas: Linux, Microsoft, Solaris, HP-UX e AIX, através ou não da instalação de agentes de acordo com a plataforma;

4.1.296. Em plataformas Microsoft, a solução deverá permitir o monitoramento de integridade de arquivos sem a necessidade de instalação de agentes adicionais do fabricante na máquina virtual a ser monitorada;

4.1.297. Precisa ter a capacidade de detectar mudanças de integridade em arquivos e diretórios do SO e aplicações terceiras;

4.1.298. Precisa ter a capacidade de detectar mudanças no estado de portas no em sistemas operacionais Linux;

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

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

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

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

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

4.1.304. Referente à integridade dos arquivos deverá rastrear por criação, última modificação, último acesso, permissões, owner, grupo, tamanho, SHA1, SHA256 e Flags;

4.1.305. Deverá alertar toda vez que uma modificação ocorrer em real time para ambiente Windows e pseudo real time para ambiente Linux, quando utilizamos agente;

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

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

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

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

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

Funcionalidade de inspeção de logs

4.1.311. A solução deverá permitir a implantação da inspeção de logs em ao menos na plataforma Microsoft, através ou não da instalação de agentes de acordo com a plataforma;

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

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

4.1.314. Precisa permitir a criação de regras de inspeção de logs adicionais para auditoria de logs de aplicações terceiras;

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

4.1.316. Deverá possibilitar a criação de regras de inspeção de logs para aplicações customizada;

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

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

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

4.1.320. Permitir modificação pelo administrador em regras para adequação ao ambiente.

Funcionalidade de reputação web

4.1.321. Deve permitir a proteção contra acesso a websites ou url consideradas maliciosas ou de baixa reputação;

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

4.1.323. A proteção deve possibilitar proteção através da instalação de agente de segurança do fabricante da solução de segurança.

Funcionalidade de antimalware

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

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

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

4.1.327. A solução deverá ter a capacidade de impedir a gravação de malwares realtime em ambientes virtuais, como hyper-v;

4.1.328. A solução deve permitir proteção de antimalware em ambientes Linux utilizando agentes;

4.1.329. A solução deverá permitir a proteção de antimalware em ambientes Windows com e sem agentes;

Funcionalidade de Controle de Aplicações

4.1.330. O controle de aplicações deverá ser realizado através de Hash, suportando no mínimo MD5, SHA1 e SHA256;

4.1.331. O agrupamento dos eventos deverá ser realizado pelo menos por Hash e por máquina;

4.1.332. A console deverá exibir eventos de no mínimo 30 dias;

4.1.333. A solução deverá possuir funcionalidades de bloquear o que não for permitido explicitamente e permitir o que não for bloqueado explicitamente;

4.1.334. A solução de segurança para servidores deverá integrar-se a tecnologias de análise de ameaças direcionadas/desconhecidas (grupo 1, item 7)**,** obedecendo as seguintes características:

4.1.334.1. A solução de segurança para servidores deverá ser capaz de submeter automaticamente arquivos suspeitos a uma solução de análise de ameaças direcionadas/desconhecidas locais, não sendo realizada de maneira externa ao ambiente, apresentando como resultado da análise, no mínimo, as seguintes informações:

- Processos de AutoStart;
- Modificações de Arquivos de Sistema;
- Serviços criados e modificados;
- Atividade de Rede Suspeita;
- Modificações de Registros;

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

4.1.335.1. Microsoft Windows 7 em Português;

4.1.335.2. Microsoft Windows 10 em Português;

4.1.335.3. Microsoft Office: 2007, 2010, 2013 e 2016;

4.1.335.4. Adobe Reader: 9, X e XI;

4.1.335.5. Java;

4.1.335.6. Firefox;

4.1.335.7. Adobe Flash Player;

4.1.336. A solução de análise de ameaças direcionadas/desconhecidas deverá retroalimentar a solução de segurança de servidores para que esse possa realizar automaticamente o bloqueio em ações suspeitas nos Servidores infectados com aquela ameaça analisada em sandbox;

SOLUÇÃO DE SEGURANÇA PARA PROTEÇÃO DE E-MAIL

Funcionalidades de proteção para Microsoft Exchange

4.1.337. Rastreamento em tempo real, para arquivos anexados as mensagens do Exchange, antes de entregar a mensagem na caixa postal do(s) destinatário(s), com as seguintes opções:

4.1.337.1. Limpar o arquivo infectado e entregá-lo limpo para o(s) destinatário(s);

4.1.337.2. Gravar o arquivo infectado na área de segurança (quarentena) e não entregá-lo para o(s) destinatário(s);

4.1.337.3. Gerar notificações e alertas e entregar o arquivo para o(s) destinatário(s);

4.1.338. Rastreamento manual às pastas do Exchange, com opção de limpeza;

4.1.339. Programação de rastreamentos automáticos do Exchange com as seguintes opções:

4.1.339.1. Escopo: Todas as pastas locais, ou pastas específicas;

4.1.339.2. Ação: Somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente ou mover automaticamente para área de segurança (quarentena);

4.1.339.3. Frequência: horária, diária, semanal, mensal;

4.1.340. Gerar registro (log) dos eventos de vírus em arquivo e local definido pelo Gestor da CONTRATANTE, com limite de tamanho opcional;

4.1.341. Gerar notificações de eventos de vírus por meio de mensagens do Exchange para quem enviou e quem recebeu a mensagem, e para um Gestor da CONTRATANTE;

4.1.342. Identificação de remetente e destinatário das mensagens.

4.1.343. Permitir bloqueios baseados nos seguintes critérios:

4.1.343.1. Tipo de arquivo;

4.1.343.2. Nome do arquivo;

4.1.343.3. Tamanho do arquivo;

4.1.344. Permitir a instalação em ambientes em Cluster Microsoft;

4.1.345. Capacidade de enviar notificações sobre vírus detectados para o administrador, para o recipiente e remetente da mensagem infectada;

4.1.346. Capacidade de gravar logs de atividade de vírus nos eventos do sistema e nos logs internos da aplicação;

4.1.347. Capacidade de detectar disseminação em massa de e-mails infectados, informando o administrador e registrando tais eventos nos logs do sistema e da aplicação;

4.1.348. Capacidade de verificar links inseridos em e-mails contra phishings;

Módulo de Gateway de e-mail

4.1.349. Permitir configurar filtro de vírus antes da chegada ao ambiente interno;

4.1.350. Permitir configurar filtro de SPAMs por reputação antes da chegada ao ambiente ;

4.1.351. Permitir configurar filtro de SPAMs por característica (heurística) antes da chegada ao ambiente;

4.1.352. Possui gerenciamento de configurações, local ou em nuvem, de forma integrada em uma única console de gerenciamento, interna e externa ao ambiente;

4.1.353. Permitir o Bloqueio de servidores spammers através da metodologia conhecida por Domain Keys Identified Mail (DKIM);

4.1.354. Deverá fazer listas de exceções para domínios utilizando-se de DKIM;

4.1.355. Possuir a detecção de SPAMs utilizando tecnologia heurística,

4.1.356. Possuir a mecanismo de checagem SPF;

4.1.357. Possuir configurações de sensibilidade na detecção de SPAMs, no mínimo em 3 níveis;

4.1.358. Permitir a criação de White e Black Lists para detecção de SPAMs;

4.1.359. Possuir proteção contra Phishings;

4.1.360. Deverá verificar o cabeçalho das mensagens em tempo real para proteção contra SPAMs;

4.1.361. Possuir inteligência contra ataques dos tipos, exploração de Códigos Avançados (Exploits) e Ataque de dia-zero (Zero-Day);

4.1.362. Possuir reputação de links que estejam dentro do corpo das mensagens;

4.1.363. Possuir níveis de sensibilidade derivados do Fabricante no bloqueio de mensagens com links de má reputação;

4.1.364. Permitir a verificação heurística contra vírus recém-lançados, mesmo sem uma vacina disponível;

4.1.365. Permitir a verificação do tipo real do arquivo, mesmo que o mesmo for renomeado;

4.1.366. Permitir que arquivos suspeitos sejam enviados automaticamente para análise em *sandbox*;

4.1.367. Permitir o escaneamento de arquivos executáveis comprimidos em tempo real;

4.1.368. Proteção contra Spywares, Dialers, Adwares, e Ferramentas para descobrir senhas de aplicativos, sem a necessidade de um software ou agente adicional;

4.1.369. Bloqueio de malware empacotado (packed malware) de forma heurística;

4.1.370. Permitir bloquear anexos pela extensão, pelo tipo real do arquivo, nome, tamanho, e número de anexos;

4.1.371. Permitir criar filtros definidos pelo tamanho de mensagem;

4.1.372. Possuir proteção contra Graymail;

4.1.373. Permitir criar exceções para os filtros, definidos por rotas, grupos de usuários ou usuários específicos;

4.1.374. Possuir recurso que retire anexos indesejados e entregue a mensagem original para o destinatário;

4.1.375. Possuir área de quarentena;

4.1.376. Permitir o bloqueio de arquivos anexos baseado em sua extensão, tamanho, tipo real do arquivo (independente da extensão) e dentro de arquivos compactados;

4.1.377. Permitir a verificação em arquivos compactados nos formatos mais utilizados em até 20 níveis de compactação;

4.1.378. Permitir criar regras distintas para mensagens que entram e saem do ambiente;

4.1.379. Possui regra específica para anexos protegidos por senha;

4.1.380. Permitir a checagem na rede Global (colaborativa) da reputação dos IPs que tentam se conectar ao ambiente para enviar mensagens;

4.1.381. Permitir a configuração individual de Reputação Global;

4.1.382. Permitir configurar o código de erro para mensagens rejeitadas;

4.1.383. Possuir configuração personalizada para cada tipo de ataque: SPAM, Vírus, Dicionário e Mensagens de Retorno (Bounced Mails);

4.1.384. Permitir personalizar os filtros baseado em: Tempo; Total de mensagens; Porcentagem de mensagens e Ação a ser tomada;

4.1.385. Prevenir contra ataques de SPAM e de Malwares;

4.1.386. Prevenir contra ataques DHA (Directory Harvest Attack);

4.1.387. Permitir verificar conexões suspeitas, apresentando o domínio responsável pela conexão, apresentado total de conexões e dessas, o percentual de conexões maliciosas;

4.1.388. Possuir recurso que permita adiar a entrega de determinadas mensagens para um horário específico;

4.1.389. Permitir enviar notificações de ocorrências customizadas ao administrador, remetente, destinatário;

4.1.390. Permitir customizar as ações que a ferramenta deve tomar de acordo com as necessidades do ambiente;

4.1.391. Permitir inserção de carimbo no assunto da mensagem;

4.1.392. Permitir a inserção de um header customizado (X-header);

4.1.393. Permitir apagar anexos indesejados, mas entregar a mensagem ao destinatário informando da ação;

4.1.394. Permitir a inserção de texto no corpo da mensagem;

4.1.395. Permitir customizar a mensagem que será inserida no corpo das mensagens;

4.1.396. Permitir a escolha do local onde se irá colocar a notificação customizada para o começo ou fim da mensagem original;

4.1.397. Permitir inserir variáveis nas notificações, onde informem no mínimo dois dos seguintes dados: Remetente; Destinatário; Assunto; Data; Nome do arquivo detectado; Nome do vírus detectado; Tamanho total da mensagem e seus anexos; Tamanho total do anexo; Número de anexos detectados pela regra; Ação tomada pela ferramenta e Nome da quarentena para onde a mensagem foi enviada;

4.1.398. Permitir configurar ações para mensagens fora do padrão (mensagens mal formadas);

4.1.399. Permitir quarentenar mensagens de SPAM;

4.1.400. Permitir arquivar as mensagens sem que o remetente ou destinatário saibam para fins de auditoria;

4.1.401. Permitir exclusão automática das mensagens em quarentena;

4.1.402. Permitir o gerenciamento via console web HTTPS suportando no mínimo os navegadores Internet Explorer e Firefox;

4.1.403. A solução deve possuir um modo de instalação passo a passo, na própria console de gerenciamento;

4.1.404. Gerenciamento das áreas de quarentena, com pesquisa, reprocessamento, entrega ou exclusão de mensagem;

4.1.405. Realizar atualização de vacinas de forma incremental

4.1.406. Realizar atualização da versão do software. A atualização deve permitir conexão através de serviço Proxy;

4.1.407. Possibilidade de configurar o “greeting” SMTP;

4.1.408. Permitir o controle de relay baseado no domínio e/ou endereço IP;

4.1.409. Possuir recurso que faça uma monitoração do sistema, alertando o administrador caso haja falta de espaço em disco, se o serviço estiver indisponível e se a fila de mensagens chegarem a um número estabelecido como máximo pelo administrador;

4.1.410. Capacidade de checagem por DNS reverso;

4.1.411. Permitir a definição de timeout de conexão SMTP

4.1.412. Capacidade de ter vários servidores de rastreamento de tráfego SMTP com possibilidade de integração com a console de gerenciamento;

4.1.413. Ter gerencia de área exclusiva para quarentena ou cópia de mensagens;

4.1.414. Possuir autenticação via TLS (Transport Layer Security);

4.1.415. A solução deve apresentar relatórios criados através de console web;

4.1.416. A solução deve disponibilizar relatórios gerenciais que podem ser "on demand" ou agendados;

4.1.417. A solução deve disponibilizar relatórios gerenciais de utilização de mensagens por destinatário, remetente, assunto;

4.1.418. A solução deve ter templates predefinidos para relatórios de forma a facilitar a geração de relatórios;

4.1.419. Possuir integração no mínimo com os seguintes serviços de diretório: LDAP (Microsoft Active Directory, OpenLDAP e Lotus Domino)

4.1.420. A solução deve ser capaz de receber trafego em TLS e realizar conexões em TLS para outros servidores;

4.1.421. A solução deve possibilitar trafego via Secure SMTP;

4.1.422. Permitir a importação e exportação de suas políticas através da console de gerenciamento;

4.1.423. A solução deve ser oferecida em formato de software appliance;

4.1.424. A solução deve ser gerenciada totalmente por sua console Web, além de possuir interface CLI intuitiva com gerenciamento dedica a solução;

4.1.425. A solução precisa ser compatível com as seguintes plataformas de virtualização;

4.1.426. VMware ESXi 5.0 ou superior; Microsoft Hyper-V Server 2008 R2 SP1 e superiores;

4.1.427. O modulo de gateway SMTP da solução de segurança para email deverá integrar-se a tecnologias de análise de ameaças direcionadas/desconhecidas (grupo 1, item 7)**,** obedecendo as seguintes características:

4.1.427.1. O modulo de gateway SMTP da solução de segurança para email deverá ser capaz de submeter automaticamente arquivos suspeitos a uma solução de análise de ameaças direcionadas/desconhecidas locais, não sendo realizada de maneira externa ao ambiente, apresentando como resultado da análise, no mínimo, as seguintes informações:

4.1.427.2. Processos de AutoStart;

4.1.427.3. Modificações de Arquivos de Sistema;

4.1.427.4. Serviços criados e modificados;

4.1.427.5. Atividade de Rede Suspeita;

4.1.427.6. Modificações de Registros;

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

4.1.427.8. Microsoft Windows 7 em Português;

4.1.427.9. Microsoft Windows 10 em Português;

4.1.427.10. Microsoft Office: 2007, 2010, 2013 e 2016;

4.1.427.11. Adobe Reader: 9, X e XI;

4.1.427.12. Java;

4.1.427.13. Firefox;

4.1.427.14. Adobe Flash Player;

4.1.428. A solução de análise de ameaças direcionadas/desconhecidas deverá retroalimentar o modulo de gateway SMTP da solução de segurança para e-mail para que esse possa realizar automaticamente o bloqueio de e-mails infectados com aquela ameaça analisada em sandbox;

FUNCIONALIDADE DE SEGURANÇA PARA AMEAÇAS AVANÇADAS (APTS) PARA ENDPOINTS

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

4.1.430. Deverá suportar IPV4 e IPV6;

4.1.431. Deverá proteger de forma integrada, no mínimo, os dispositivos licenciados nos itens que compõem a solução quantificada no item 2.3;

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

4.1.433. Deve permitir a criação de sandbox local utilizando, no mínimo, os seguintes sistemas operacionais: Windows XP 32-bits, Windows 7 64-bits e Windows 10;

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

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

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

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

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

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

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

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

4.1.442. Deverá identificar e executar arquivos de scripts no formato Visual Basic e Javascript inclusive quando estiverem ofuscada;

SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DOS PRODUTOS

4.1.443. A implantação dessa solução se dará através de arquivo de licença e será realizada mediante a substituição das ferramentas Symantec Endpoint Protection, Symantec Endpoint Protection Management e Symantec Mail Gateway, caso a solução adquirida seja composta de ferramentas diversas às atuais do Cade.

4.1.444. O arquivo de licença deve disponibilizar acesso a servidor web contendo todos os softwares licenciados para instalação e upgrade das ferramentas contratadas;

4.1.445. Em caso de novas soluções deve haver um acompanhamento técnico local por parte da contratada visando a REMOÇÃO DA SOLUÇÃO EXISTENTE e a instalação e configuração inicial do Software e/ou equipamento;

4.1.446. A instalação deverá acontecer de forma automatizada, mediante *scripts* de rede, preferencialmente por meio de política de grupos;

4.1.446.1. A contratada poderá instalar localmente, desde que mediante autorização do Cade ou em casos pontuais que a instalação automatizada não tenha sido efetiva;

TREINAMENTO OFICIAL NA SOLUÇÃO

4.1.447. A Contratada realizará treinamento oficial do fabricante ao corpo técnico do Cade, capacitando os servidores na solução e todas as funcionalidades contratadas;

4.1.448. O treinamento oficial do fabricante será de, no mínimo, 40 horas por instrutor certificado na ferramenta de cada item da solução;

4.1.449. O treinamento será realizado preferencialmente no modelo presencial, caso o instrutor tenha disponibilidade de presença física no Cade;

4.1.450. Caso haja inviabilidade de realização pelo modelo presencial, o treinamento será realizado no Cade com o modelo telepresencial (*online* por videoconferência), em português, utilizando ferramenta própria disponibilizada pela fabricante (ex.: Cisco Webex, Adobe Connect, etc.);

4.1.450.1. Caso não haja disponibilidade, a empresa custeará os gastos de passagens e estadia para o centro de treinamento mais próximo do endereço da contratante;

4.1.450.2. O Cade disponibilizará os computadores a serem utilizados pelos participantes do curso;

4.1.450.3. A empresa disponibilizará ambiente virtual para execução do treinamento;

4.1.450.4. A empresa disponibilizará material em formato digital (pdf) aos participantes e quaisquer conteúdos e ferramentas adicionais que venham a ser necessárias para o treinamento;

4.1.451. Elaborar manuais e procedimentos técnicos e operacionais da solução durante a implantação;

4.1.452. Enviar certificado aos participantes ao final do treinamento.

4.2. **Requisitos de manutenção, garantia e suporte técnico**

4.2.1. O prazo de garantia para suporte técnico é de 60 (sessenta) meses;

4.2.2. O prazo de garantia será contado a partir da emissão do Termo de Recebimento Definitivo da solução;

4.2.3. Em caso de mudança da sede deste Conselho para outro local no Distrito Federal, a execução de garantia deverá continuar sendo prestada, nas condições estabelecidas no Edital no endereço da nova sede;

4.2.4. O suporte técnico deve ser 24x7x365, ou seja, 24 (vinte e quatro) horas por dia em 7 (sete) dias da semana por 365 (trezentos e sessenta e cinco) dias por ano, em língua portuguesa;

4.2.5. Os serviços de suporte técnico têm por finalidade garantir a sustentação e a plena utilização da solução durante a vigência do contrato. Inclui o atendimento para sanar dúvidas relacionadas com instalação, configuração e uso do software e dos equipamentos ou para correção de problemas desses, em especial na configuração de parâmetros, falhas, erros, defeitos ou vícios identificados no funcionamento da solução. Deve contemplar, quando for o caso, atendimento a eventual problema de instalação ou configuração de softwares básicos e de infraestrutura de TI (sistemas operacionais, servidores de banco de dados, servidores de aplicação, etc.) necessários ao funcionamento da solução;

4.2.6. Deve contemplar a atualização de versões do software aplicativo, as quais incorporam correções de erros ou problemas registrados e melhorias implementadas pela fabricante, num empacotamento estável do sistema. O serviço de atualização de versão tem por finalidade assegurar a devida atualização da solução durante o período de vigência da garantia. Refere-se ao fornecimento de novas versões e releases da solução lançados no período. A cada nova liberação de versão e *release*, será disponibilizada em formato digital manuais e demais documentos técnicos, bem como nota informativa das funcionalidades implementadas. Em caso de lançamento de patch de correção, a contratada deverá comunicar o fato a contratante e indicar a forma de obtenção e os defeitos que serão corrigidos pelo patch. Em ambos os casos, a comunicação deve ser feita no prazo de até 30 (trinta) dias, a contar do lançamento de nova versão ou solução de correção;

4.2.7. A contratada será responsável pelos serviços de implantação das novas versões e *releases* dos produtos por ela fornecidos como partes do objeto, bem como pela aplicação dos *patches* de correção e pacotes de serviço (*service packs*) relativos a esses produtos. Para a implantação das novas versões/releases, bem como para a aplicação dos *patches*, deverá ser aberto chamado de suporte técnico com nível de severidade adequado e a prestação dos serviços deve ser agendada com os responsáveis pela solução na contratante;

4.2.8. Deverá ser prestado suporte técnico remoto com atendimento mediante registro de chamados em página de website, em sistema fornecido pela contratada e/ou pelo fabricante; e também através de contato telefônico. Esse serviço destina-se a esclarecimento de dúvidas e resolução de problemas relacionados à configuração e uso dos componentes da solução contratada;

4.2.9. As peças substitutas deverão apresentar padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento;

4.2.10. A contratada auxiliará o Cade na reinstalação das ferramentas, caso seja necessário, ao longo do tempo de garantia da ferramenta;

4.2.11. A contratada deverá auxiliar o Cade na comunicação junto ao fabricante;

4.2.12. A contratada deverá disponibilizar os seguintes canais de acesso ao suporte técnico: Portal Web, E-mail, Central 0800 e/ou telefone fixo.

4.3. **Requisitos da entrega**

4.3.1. A entrega dos equipamentos físicos da solução, caso existam, ocorrerá em Brasília, na Conselho Administrativo de Defesa Econômica, situado no SEPN 515, Conjunto D, Lote 04 - Edifício Carlos Taurisano, Asa Norte, em Brasília/DF;

4.3.2. O prazo da entrega, contado a partir da assinatura do contrato e/ou a entrega da Ordem de Serviço ou Fornecimento de Bens à Contratada, considerando o que acontecer primeiro, será de até 45 (quarenta e cinco) dias.

4.3.3. A entrega da solução dos equipamentos deverá ser agendada em data e hora a ser combinada previamente com a Coordenação-Geral de Tecnologia da Informação - CGTI, por meio do telefone (61) 3221-8552 e/ou e-mail cgti@cade.gov.br;

4.3.4. O transporte dos equipamentos até o Conselho Administrativo de Defesa Econômica deverá ser realizado pela Contratada, inclusive os procedimentos de seguro, embalagem e transporte até o espaço alocado pelo Cade para guarda;

4.3.5. Caberá ao Cade rejeitar no total ou em parte, os materiais entregues em desacordo com o objeto do Contrato.

4.3.6. O recebimento dos equipamentos será efetivado pela equipe designada pelo Cade, e dar-se-á da forma provisória e definitiva.

4.3.7. A instalação das ferramentas será realizadas em até 30 dias contados a partir da abertura da Ordem de Serviços;

4.3.8. A garantia do fabricante de 60 (sessenta) meses são contados a partir da data de assinatura do Termo de Recebimento Definitivo do serviço de instalação e configuração dos produtos;

4.3.9. O serviço de suporte técnico será válido mediante abertura de Ordem de Serviço, após a conclusão da instalação e configuração dos produtos;

4.3.10. A assistência técnica da garantia será realizada a pedido do Cade pela contratada ou suas autorizadas.

5. CLÁUSULA QUINTA - DAS OBRIGAÇÕES DA CONTRATADA

5.1. Realizar, em atenção à Resolução CADE nº 11/2014, cadastro como usuário externo no Sistema Eletrônico de Informações – SEI, cujo acesso encontra-se franqueado ao interessado por meio do seguinte endereço eletrônico: http://sei.cade.gov.br/sei/institucional/usuarioexterno/controlador_externo.php?acao=usuario_externo_logar&id_orgao_acesso_externo=0.

5.2. Comprometer-se, por si e por seus funcionários, a aceitar e aplicar rigorosamente todas as normas e procedimentos de segurança definidos na Política de Segurança da Informação e Comunicação – POSIC do CONTRATANTE. A POSIC está disponível no endereço eletrônico: http://www.cade.gov.br/acesso-a-informacao/publicacoes-institucionais/tecnologia-da-informacao/tecnologia_da_informacao.

5.3. Realizar a transição contratual com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações;

5.4. Realizar o objeto que lhe foi adjudicado, de acordo com a proposta apresentada e normas legais, ficando a seu cargo todas as despesas, diretas e indiretas, decorrentes do cumprimento das obrigações assumidas, sem qualquer ônus ao Cade, observando sempre os critérios deste Contrato para cumprimento de seu objeto;

5.5. Efetuar a entrega do objeto do presente processo, dentro dos parâmetros de qualidade e prazos estabelecidos, em observância às normas legais e regulamentares aplicáveis e, inclusive, às recomendações aceitas pela boa técnica;

5.6. Arcar com todas as despesas, diretas ou indiretas, decorrentes do cumprimento das obrigações assumidas, sem qualquer ônus ao Cade;

5.7. Reparar e responder pelos danos causados diretamente ao Cade ou a terceiros, por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da presente relação contratual, não excluindo ou reduzindo essa responsabilidade da fiscalização ou do acompanhamento da execução do objeto pela Administração do Cade;

5.8. Pagar ao Cade o valor correspondente, mediante ao pagamento da Guia de Recolhimento da União – GRU, a ser emitida pela Diretoria Administrativa e Planejamento no valor correspondente ao dano acrescido das demais penalidades, quando apurado o dano e caracterizada a sua autoria por qualquer empregado da Contratada;

5.9. Propiciar todos os meios e facilidades necessárias à fiscalização do cumprimento do objeto pelo Cade, cujo representante terá poderes para recusar o recebimento dos bens adquiridos, sustar o serviço, total ou parcialmente, em qualquer tempo, sempre que considerar a medida necessária, e/ou recusar os materiais e equipamentos empregados que julgar inadequado;

5.10. Comunicar à Coordenação-Geral de Tecnologia da Informação, no prazo máximo de 5 (cinco) dias que antecedam o prazo de vencimento da entrega, os motivos que impossibilitam o seu cumprimento, solicitando se possível, a prorrogação de prazos;

5.11. Manter durante a execução contratual, todas as condições de habilitação e qualificação exigidas na licitação;

5.12. Responder pelas despesas resultantes de quaisquer ações, demandas decorrentes de danos seja por culpa sua ou quaisquer de seus empregados e prepostos, obrigando-se, outrossim, por quaisquer responsabilidades decorrentes de ações judiciais de terceiros, que lhes venham a ser exigidas por força de Lei, ligadas ao cumprimento das obrigações contratuais;

5.13. Atender prontamente quaisquer orientações e exigências dos representantes do Cade inerente ao objeto deste Contrato;

5.14. Comunicar ao Cade, por escrito, qualquer anormalidade de caráter urgente e prestar os esclarecimentos julgados necessários, inclusive em relação ao fornecimento dos equipamentos objetos da contratação;

5.15. Não transferir a terceiros, por qualquer forma, nem subcontratar qualquer parte a que está obrigada, sem prévio consentimento, por escrito, do Cade;

5.16. Responsabilizar-se por todas as providências e obrigações estabelecidas na legislação específica de acidente do trabalho, quando, em ocorrência da espécie, forem vítimas seus empregados na execução do objeto, especialmente se acontecido nas dependências do Cade, ficando ainda, o Cade, isento de qualquer vínculo empregatício com os mesmos;

5.17. Responsabilizar-se por todos os encargos de possível demanda trabalhista, cível ou penal, relacionados com o objeto deste Contrato, originalmente ou vinculados por prevenção, conexão ou continência;

5.18. A inadimplência da Contratada, com referência aos encargos estabelecidos nos itens anteriores não transfere a responsabilidade por seu pagamento ao Cade, nem poderá onerar o objeto do presente certame, razão pela qual a Contratada renúncia, expressamente, a qualquer vínculo de solidariedade, ativa ou passiva, para com o Cade;

5.19. Atender prontamente quaisquer orientações e exigências dos representantes do Cade inerente ao objeto deste Contrato, bem como, acatar as orientações do Cade, sujeitando-se a mais ampla e irrestrita fiscalização, prestando os esclarecimentos solicitados e atendendo às reclamações formuladas;

5.20. Em nenhuma hipótese veicular publicidade ou qualquer outra informação acerca do objeto deste Contrato, sem prévia autorização do Cade;

5.21. Executar o objeto dentro dos parâmetros e rotinas estabelecidos pelo Cade no presente Contrato;

5.22. Indicar formalmente e manter, durante a execução contratual, um preposto aceito pelo Cade e apto a representar a Contratada sempre que se fizer necessário, que deverá responder pela fiel execução do obejto e apresentar solução rápida para eventuais dificuldades de operacionalização dos serviços contratados;

5.23. Responsabilizar-se pelos ônus resultantes de quaisquer ações, demandas, custos e despesas decorrentes de danos, ocorridos por culpa sua ou de qualquer de seus empregados e prepostos, obrigando-se, outrossim, por quaisquer responsabilidades decorrentes de ações judiciais movidas por terceiros que lhe venham a ser exigidas por força da Lei, ligadas ao cumprimento do Termo de Referência;

5.24. Responsabilizar-se por todas as despesas, diretas e indiretas, que decorrem da execução do objeto – tais como custos de entrega dos bens nos endereços solicitados pelo Cade; custos com alimentação, vestuário e transporte dos empregados; diárias, salários, benefícios, auxílios, indenizações civis e quaisquer outras verbas que forem devidas a seus empregados; tributos, contribuições previdenciárias e demais encargos fiscais, sociais e trabalhistas – e saldá-las na época própria, atentando para a inexistência de vínculo trabalhista entre o Cade e tais empregados;

5.25. Acatar as orientações do Cade, sujeitando-se a mais ampla e irrestrita fiscalização, prestando os esclarecimentos solicitados e atendendo às reclamações formuladas;

5.26. Manter, durante toda a execução do objeto, a capacidade de entrega para as demandas contratadas, bem como equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para a prestação dos serviços;

5.27. Substituir, às suas expensas, no total ou em parte, o objeto do presente Contrato em que se verificarem irregularidades no seu fornecimento;

5.28. Aceitar nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários de até 25% (vinte e cinco por cento) do valor inicial atualizado da ata de registro de preços a ser firmada;

5.29. Emitir fatura (nota fiscal) no valor pactuado e condições da contratação, apresentando-a ao Cade para ateste e pagamento;

5.30. Deverá constar na nota fiscal os itens de acordo com o descrito neste edital.

5.31. Entregar, nos locais determinados pelo contratante na Ordem de Serviço ou Fornecimento de Bens, o objeto da presente contratação, às suas expensas, dentro do prazo máximo de até trinta dias corridos.

5.32. Apresentar, quando da entrega dos equipamentos e materiais, o Termo de Suporte e Garantia informando as condições de prestação de serviços, os dados de acesso a Central de Suporte para efeitos da solicitação de serviços de garantia e suporte técnico.

5.33. Apresentar, quando da entrega dos equipamentos e materiais, documentação que comprove a origem dos bens, se importados, e da quitação dos tributos de importação a eles referentes, sob pena de rescisão contratual e/ou multa;

5.34. Corrigir todos os problemas técnicos decorrentes de erros identificados na execução da instalação e na configuração dos equipamentos, sejam operacionais ou por problemas de mau funcionamento, responsabilizando-se por todos os procedimentos e custos envolvidos para resolução, sob pena de incorrer nas sanções legais cabíveis, garantida a ampla defesa;

5.35. Transferir a tecnologia e o conhecimento acerca da configuração, do manuseio e das demais características técnicas inerentes e próprias de cada equipamento por modelo/tipo à equipe técnica do Cade;

5.36. Sanar as irregularidades identificadas na execução de qualquer uma das etapas, inclusive, substituir no prazo de 15 (quinze) dias da notificação, as suas expensas, todos os equipamentos fornecidos com problemas técnicos ou apresentados fora das especificações exigidas, sob pena de incorrer em sanções legais cabíveis, garantida a ampla defesa;

5.37. Substituir os equipamentos e materiais que apresentarem defeitos durante o período de garantia, sem ônus para o Cade, em conformidade aos níveis de serviços mínimos descritos no Termo de Referência;

5.38. Fornecer os equipamentos conforme especificações técnicas constantes do Termo de Referência e na proposta comercial, que não poderão ser inferiores às especificações contidas no Termo de Referência, e nos prazos constantes na Ordem de Serviço ou Fornecimento de Bens;

5.39. Fornecer, juntamente com os equipamentos, todos os produtos, bem como os catálogos, manuais, páginas impressas do sítio do fabricante na internet ou quaisquer outros documentos que comprovem o atendimento das especificações técnicas dos equipamentos fornecidos descritos no Termo de Referência, indicando onde encontrar suas características;

5.40. Fornecer equipamentos novos (sem uso, reforma ou recondicionamento) e que não estarão fora de linha de fabricação, pelo menos, nos próximos 90 (noventa) dias contados da nota de empenho, de maneira a não prejudicar a execução dos objetos a serem contratados;

5.41. É permitida a oferta de equipamentos comprovadamente superiores, pelo mesmo preço, no caso de indisponibilidade do originalmente proposto na Ata de Registro de Preços, devendo este também permanecer em linha de comercialização no tempo estabelecido.

5.42. Comunicar ao Cade sempre que houver descontinuidade ou alteração nos modelos propostos e suas modificações, mantendo o Cade atualizado;

5.43. Cumprir a garantia de funcionamento e prestar a assistência técnica dos equipamentos fornecidos, na forma e nos prazos estabelecidos;

5.44. Garantir a reposição de peças pelo período da garantia, caso haja *hardware* na solução, na forma estabelecida no Termo de Referência;

5.45. Fornecer, assim que finalizado o atendimento, cópia da respectiva Ordem de Serviço (chamado técnico), atestando a solução e os prazos praticados na Ordem de Serviço;

5.46. Arcar com eventuais prejuízos causados ao contratante ou a terceiros, decorrentes de erros na entrega ou provocados por ineficiência ou irregularidade cometida por seus empregados ou prepostos, na execução dos serviços;

5.47. Assumir inteira responsabilidade técnica e administrativa do objeto contratado, não podendo, sob qualquer hipótese, transferir a outras empresas a responsabilidade por problemas de funcionamento do serviço;

5.48. Zelar para que os dados, informações e quaisquer documentos elaborados com base nos serviços ora contratados tenham tratamento reservado, sendo vedada sua reprodução divulgação ou cessão a outrem, a qualquer título;

5.49. Responsabilizar-se pelo perfeito cumprimento das especificações contidas no termo de referência, cabendo-lhe, integralmente, o ônus decorrente destes, independentemente da fiscalização exercida pelo Cade;

5.50. Responsabilizar-se pela disciplina e o respeito hierárquico de seus empregados para com os empregados do Cade, objetivando sempre melhor qualidade no atendimento;

5.51. Cumprir e fazer cumprir por parte de seus prepostos ou empregados, as leis, regulamentos e posturas, bem como quaisquer determinações emanadas dos órgãos competentes, pertinentes à matéria do objeto especificado;

5.52. Responsabilizar-se pelas consequências decorrentes de qualquer transgressão cometida por seus prepostos ou empregados;

5.53. Responsabilizar-se pelo cumprimento, por parte de seus empregados, das normas disciplinares vigentes no Cade;

5.54. Reparar, corrigir ou substituir as suas expensas, no todo ou em parte, o objeto desta contratação, em que se verificarem vícios, defeitos ou incorreções resultantes da execução dos serviços, salvo quando o defeito for, comprovadamente, provocado por uso indevido por parte da contratante;

5.55. Submeter-se à Política de Segurança da Informação e Comunicações e demais normas de segurança vigentes na contratante e abster-se de veicular publicidade ou qualquer outra informação acerca das atividades desempenhadas, sem prévia autorização da contratante;

5.56. Providenciar a assinatura do Termo de Compromisso, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na contratante, pelo representante legal da Contratada.

5.57. Providenciar a assinatura do Termo de Ciência da Declaração de Manutenção de Sigilo e das Normas de Segurança vigentes na contratante, por todos os empregados da contratada diretamente envolvidos na contratação.

5.58. Comunicar imediatamente por escrito ao Cade qualquer anormalidade verificada, inclusive de ordem funcional, para que sejam adotadas as providências de regularização necessárias;

5.59. Para todos os serviços a serem prestados pela Contratada é imprescindível a economicidade e a qualidade, de acordo com os critérios estipulados;

5.60. Auxiliar o Cade na comunicação junto ao fabricante e na resolução de atendimentos, conforme o item 9.2.17;

5.61. Atender os prazos do item 9.2.10 para manter as funcionalidades contratadas;

5.62. Auxiliar o Cade na configuração, reinstalação e remediação de eventos que envolvam as ferramentas adquiridas.

6. CLÁUSULA SEXTA - DAS OBRIGAÇÕES DO CONTRATANTE

6.1. Proporcionar todas as facilidades e instruções necessárias para que a Contratada possa executar o objeto deste Contrato, inclusive prestando as informações e os esclarecimentos atinentes ao objeto do presente Edital que venham a ser solicitados pela Contratada.

6.2. Encaminhar formalmente a demanda por meio de Ordem de Serviço ou Fornecimento, de acordo com os critérios estabelecidos no Termo de Referência, observando-se o disposto no arts. 19 e 33 da IN 04/2014 SLTI/MP.

6.3. Disponibilizar as informações necessárias sobre o seu ambiente tecnológico para o fiel cumprimento do objeto, e, por meio de equipe técnica, assistir a Contratada nas etapas de execução, como forma de evitar a ocorrência de danos de qualquer natureza, inclusive a terceiros.

6.4. Acompanhar e fiscalizar todos os procedimentos de execução do objeto, referente à entrega dos equipamentos, se certificando do cumprimento das condições estabelecidas e tomando todas as medidas cabíveis para a plena execução contratual, por meio da Coordenação-Geral de Tecnologia da Informação, nos termos do art. 67 da Lei nº 8.666/93 e dos arts. 33 e 34 da Instrução Normativa SLTI/MPOG nº 04/2014, que anotará em registro próprio todas as ocorrências relacionadas com o mesmo.

6.5. Exercer a fiscalização e acompanhamento da execução do objeto, por meio da Coordenação-Geral de Tecnologia da Informação – CGTI, procedendo ao atesto das respectivas notas fiscais/faturas, com as ressalvas e/ou glosas que se fizerem necessárias.

6.6. Permitir ao pessoal técnico da Contratada, desde que identificado, livre acesso às instalações, onde se encontrarem os equipamentos, para execução do objeto, respeitadas todas as normas internas de segurança deste Conselho, inclusive àqueles referentes à identificação, trajes, trânsito e permanência em suas dependências.

6.7. Assegurar-se da boa execução do objeto, verificando sempre o seu bom desempenho.

6.8. Assegurar-se da efetiva entrega ou disponibilização do objeto da contratação, verificando sempre as especificações, características e quantidades cotadas.

6.9. Assegurar-se de que os preços contratados estão compatíveis com aqueles praticados no mercado, objeto a ser firmado entre as partes, de forma a garantir que continuem a ser os mais vantajosos para o Cade.

6.10. Fiscalizar o cumprimento das obrigações assumidas pela Contratada, inclusive quanto à continuidade da prestação dos serviços que, ressalvados os casos de força maior, justificados e aceitos pelo Cade, não deve ser interrompida.

6.11. Emitir, por intermédio da Coordenação-Geral de Tecnologia da Informação, pareceres sobre os atos relativos à execução contratual, em especial, quanto à entrega dos bens adquiridos e acompanhamento, fiscalização da prestação de serviços, aplicação de sanções, alterações e repactuações contratuais.

6.12. Comunicar à Contratada, por escrito, toda e qualquer ocorrência relacionada com o objeto deste Edital, inclusive sobre multas, penalidades e quaisquer outros débitos de sua responsabilidade, garantido o contraditório e a ampla defesa.

6.13. Acionar a Contratada em caso de necessidade de suporte técnico ou execução da garantia.

6.14. Efetuar os pagamentos devidos à Contratada nas condições e preços pactuados, nos prazos indicados neste Contrato, após a apresentação da nota fiscal ou fatura devidamente discriminada, desde que não exista fator impeditivo provocado pela Contratada.

6.15. Prestar as informações e os esclarecimentos atinentes ao objeto da presente contratação, que venham a ser solicitados pela(s) Contratada(s).

6.16. Comunicar a contratado toda e qualquer ocorrência relacionada à prestação de serviços.

6.17. Emitir para a Contratada em até 30 (trinta) dias úteis, contados a partir da entrega definitiva dos equipamentos, o Termo de Recebimento Definitivo que será condição para prosseguimento do processo de pagamento e constituindo a data de emissão do Termo de Recebimento Definitivo marco temporal para início da contagem do prazo de garantia.

7. CLÁUSULA SÉTIMA - DA FISCALIZAÇÃO E DO ACOMPANHAMENTO

7.1. As atividades de gestão e fiscalização da execução contratual são o conjunto de ações que tem por objetivo aferir o cumprimento dos resultados previstos pela Administração para o serviço contratado, verificar a regularidade das obrigações previdenciárias, fiscais e trabalhistas, bem como prestar apoio à instrução processual e o encaminhamento da documentação pertinente ao setor de contratos para a formalização dos procedimentos relativos a repactuação, alteração, reequilíbrio, prorrogação, pagamento, eventual aplicação de sanções, extinção do contrato, dentre outras, com vista a assegurar o cumprimento das cláusulas avençadas e a solução de problemas relativos ao objeto.

7.2. O conjunto de atividades de gestão e fiscalização compete ao gestor da execução do contrato, podendo ser auxiliado pela fiscalização técnica, administrativa, setorial e pelo público usuário. Conforme a Portaria nº 212/2017 do Cade, considera-se:

7.2.1. **Gestor de Execução do Contrato:** servidor com atribuições gerenciais, designado para coordenar as atividades de gestão de contratos, observadas as rotinas definidas no Guia de Fluxos de Gestão e Fiscalização de Contratos Administrativos do Cade, anexo desta Portaria;

7.2.2. **Fiscal Técnico:** servidor, preferencialmente representante da área demandante, com atribuições para subsidiar o Gestor de Execução do Contrato de informações sobre o cumprimento das condições contratuais, aferindo e declarando se a qualidade, quantidade, tempo e modo da prestação dos serviços ou fornecimento de bens estão compatíveis com os indicadores de níveis mínimos de desempenho estipulados no ato convocatório.; e

7.2.3. **Fiscal Administrativo:** servidor representante preferencialmente da UFA, com atribuições para subsidiar o Gestor de Execução do Contrato de informações de natureza administrativa, tais como: a vigência do contrato, o saldo disponível, o gerenciamento da conta vinculada, o cumprimento, pela empresa, das obrigações administrativas, inclusive trabalhistas, previdenciárias, sociais e comerciais aplicáveis à prestação dos serviços, atestando que a documentação administrativa está em conformidade O Fiscal Administrativo poderá ser dispensado nas hipóteses do art. 62 § 4º da Lei 8.666/1993.

7.3. As atividades de gestão e fiscalização da execução contratual devem ser realizadas de forma preventiva, rotineira e sistemática, podendo ser exercidas por servidores, equipe de fiscalização ou único servidor, desde que, no exercício dessas atribuições, fique assegurada a distinção dessas atividades e, em razão do volume de trabalho, não comprometa o desempenho de todas as ações relacionadas à Gestão do Contrato.

7.4. A fiscalização administrativa poderá ser efetivada com base em critérios estatísticos, levando-se em consideração falhas que impactem o contrato como um todo e não apenas erros e falhas eventuais no pagamento de alguma vantagem a um determinado empregado.

7.5. O descumprimento das obrigações trabalhistas ou a não manutenção das condições de habilitação pela CONTRATADA poderá dar ensejo à rescisão contratual, sem prejuízo das demais sanções.

7.6. A CONTRATANTE poderá conceder prazo para que a CONTRATADA regularize suas obrigações trabalhistas ou suas condições de habilitação, sob pena de rescisão contratual, quando não identificar má-fé ou a incapacidade de correção.

7.7. Durante a execução do objeto, o fiscal técnico deverá monitorar constantemente o nível de qualidade dos serviços para evitar a sua degeneração, devendo intervir para requerer à CONTRATADA a correção das faltas, falhas e irregularidades constatadas.

7.8. O fiscal técnico deverá apresentar ao preposto da CONTRATADA a avaliação da execução do objeto ou, se for o caso, a avaliação de desempenho e qualidade da prestação dos serviços realizada.

7.9. Em hipótese alguma, será admitido que a própria CONTRATADA materialize a avaliação de desempenho e qualidade da prestação dos serviços realizada.

7.10. A CONTRATADA poderá apresentar justificativa para a prestação do serviço com menor nível de conformidade, que poderá ser aceita pelo fiscal técnico, desde que comprovada a excepcionalidade da ocorrência, resultante exclusivamente de fatores imprevisíveis e alheios ao controle do prestador.

7.11. Na hipótese de comportamento contínuo de desconformidade da prestação do serviço em relação à qualidade exigida, bem como quando esta ultrapassar os níveis mínimos toleráveis previstos nos indicadores, além dos fatores redutores, devem ser aplicadas as sanções à CONTRATADA de acordo com as regras previstas no ato convocatório.

7.12. O fiscal técnico poderá realizar avaliação diária, semanal ou mensal, desde que o período escolhido seja suficiente para avaliar ou, se for o caso, aferir o desempenho e qualidade da prestação dos serviços.

7.13. O fiscal técnico, ao verificar que houve subdimensionamento da produtividade pactuada, sem perda da qualidade na execução do serviço, deverá comunicar à autoridade responsável para que esta promova a adequação contratual à produtividade efetivamente realizada, respeitando-se os limites de alteração dos valores contratuais previstos no § 1º do art. 65 da Lei nº 8.666, de 1993.

7.14. A conformidade do material a ser utilizado na execução dos serviços deverá ser verificada juntamente com o documento da CONTRATADA que contenha sua relação detalhada, de acordo com o estabelecido neste Contrato e na proposta, informando as respectivas quantidades e especificações técnicas, tais como: marca, qualidade e forma de uso.

7.15. O representante da CONTRATANTE deverá promover o registro das ocorrências verificadas, adotando as providências necessárias ao fiel cumprimento das cláusulas contratuais, conforme o disposto nos §§ 1º e 2º do art. 67 da Lei nº 8.666, de 1993.

7.16. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade da CONTRATANTE ou de seus agentes, gestores e fiscais, de conformidade com o art. 70 da Lei nº 8.666, de 1993.

7.17. A equipe de fiscalização que deverá:

7.17.1. Providenciar o atesto da nota fiscal verificando as informações do relatório de acompanhando do evento, que deverá estar adequada à cobrança;

7.17.2. Controlar o prazo de vigência do instrumento contratual;

7.17.3. Manter registro de ocorrências relacionadas com a execução do contrato, determinando todas as ações necessárias para a regularização das faltas ou defeitos;

7.17.4. Receber a Nota Fiscal ou Fatura, quando comprovada a execução contratual e a apresentação de toda a documentação exigida, deste Contrato;

7.17.5. Comunicar à CONTRATADA, formalmente, as irregularidades cometidas;

7.17.6. Encaminhar ao Gestor do Contrato eventuais pedidos de modificação contratual; e

7.17.7. Verificar e exigir que seja anexado à nota fiscal o relatório de acompanhamento do evento.

7.17.8. Verificar quantidade e valores cobrados pela contratada levando em consideração as quantidades estimadas, demandadas e efetivamente executadas.

7.17.9. A presença da fiscalização da CONTRATANTE não elide, nem diminui, a responsabilidade da CONTRATADA.

7.18. A fiscalização do contrato poderá agendar reuniões com as contratadas para fins de checagem da adequação e funcionamento pleno dos produtos e ajustes de detalhes específicos do fornecimento. A reunião deverá ser reduzida a termo em ata.

7.19. Caberá à Comissão de Fiscalização acompanhar a execução dos serviços, zelando pela racionalidade dos gastos públicos e pela excelência quanto ao conteúdo e qualidade técnica do evento, atestando a Nota Fiscal, bem como, elaborando o Relatório da Avaliação do Evento;

7.20. Caberá à equipe de fiscalização encaminhar ao Ordenador de Despesas, para fins de aprovação, Relatório de Avaliação do evento que, devidamente assinado e preenchido, encaminhará à Coordenação-Geral de Orçamento, Finanças e Logística-CGOFL, do CADE, com vistas ao pagamento da nota fiscal da prestação do serviço.

8. CLÁUSULA OITAVA- DAS SANÇÕES ADMINISTRATIVAS

8.1. Pela inexecução total ou parcial do objeto do contrato, o CONTRATANTE poderá, garantida a prévia defesa e o devido processo legal, aplicar as seguintes sanções:

I - Advertência, com base no art. 87, I, da Lei 8.666/93;

II - Multa de:

a) 0,1% (um décimo por cento) até 0,2% (dois décimos por cento) por dia sobre o valor adjudicado em caso de atraso na execução dos serviços, limitada a incidência a 15 (quinze) dias. Após o décimo quinto dia e a critério da Administração, no caso de execução com atraso, poderá ocorrer a não-aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença;

b) 0,1% (um décimo por cento) até 10% (dez por cento) sobre o valor adjudicado, em caso de atraso na execução do objeto, por período superior ao previsto no subitem acima ou de inexecução parcial da obrigação assumida;

c) 0,1% (um décimo por cento) até 15% (quinze por cento) sobre o valor adjudicado, em caso de inexecução total da obrigação assumida;

d) 0,2% a 3,2% por dia sobre o valor do contrato, conforme detalhamento constante das **tabelas 1 e 2** abaixo; e

e) 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso na apresentação da garantia (seja para reforço ou por ocasião de prorrogação), observado o máximo de 2% (dois por cento. O atraso superior a 25 (vinte e cinco) dias autorizará a Administração CONTRATANTE a promover a rescisão do contrato;

f) As penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si.

g) A aplicação das multas seguirá o detalhamento das tabelas a seguir

Tabela 1

GRAU	CORRESPONDÊNCIA
1	0,2% ao dia sobre o valor do contrato
2	0,4% ao dia sobre o valor do contrato
3	0,8% ao dia sobre o valor do contrato
4	1,6% ao dia sobre o valor do contrato
5	3,2% ao dia sobre o valor do contrato

Tabela 2

INFRAÇÃO		
ITEM	**DESCRIÇÃO**	**GRAU**
1	Permitir situação que crie a possibilidade de causar dano físico, lesão corporal ou conseqüências letais, por ocorrência;	05
2	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços contratuais por dia e por unidade de atendimento;	04
3	Servir-se de funcionário sem qualificação para executar os serviços	03

	contratados, por empregado e por dia;	
4	Recusar-se a executar serviço determinado pela fiscalização, por serviço e por dia;	02
Para os itens a seguir, deixar de:		
5	Cumprir determinação formal ou instrução complementar do órgão fiscalizador, por ocorrência;	02
6	Substituir empregado alocado que não atenda às necessidades do serviço, por funcionário e por dia;	01
7	Cumprir quaisquer dos itens do Edital e seus Anexos não previstos nesta tabela de multas, após reincidência formalmente notificada pelo órgão fiscalizador, por item e por ocorrência;	03
8	Indicar e manter durante a execução do contrato os prepostos previstos no edital/contrato;	01
9	Providenciar treinamento para seus funcionários conforme previsto na relação de obrigações da CONTRATADA	01

III - Suspensão temporária de participação em licitação e impedimento de contratar com a Administração, pelo prazo de até 2 (dois) anos, com base no art. 87, III, da Lei 8.666/93;

IV - Declaração de inidoneidade para licitar ou contratar com a Administração Pública, com base no art. 87, IV, da Lei 8.666/93;

V - Impedimento de licitar e de contratar com a União e descredenciamento no SICAF, pelo prazo de até 5 (cinco) anos, com base no art. 7º, da Lei 10.520/2002.

8.2. A multa moratória incidirá a partir do 2º (segundo) dia útil da inadimplência.

8.3. Se a multa for de valor superior ao valor da garantia prestada, além da perda desta, responderá a Contratada pela sua diferença, a qual será descontada dos pagamentos devidos pelo Contratante ou, quando for o caso, cobrada judicialmente.

8.4. As sanções previstas nos incisos I, III, IV e V do item 10.6.12 poderão ser aplicadas juntamente com as do inciso II, facultada a defesa prévia do interessado, no respectivo processo, no prazo de 5 (cinco) dias úteis, contados da notificação.

8.5. A contratada ficará sujeita, ainda, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

a) Falhar na execução do contrato: Pena - impedimento do direito de licitar e contratar com a União e descredenciamento do SICAF pelo período de 12 (doze) meses.

b) Fraudar na execução do contrato: Pena - impedimento do direito de licitar e contratar com a União e descredenciamento do SICAF pelo período de 30 (trinta) meses.

8.6. As penas previstas nas alíneas "a" a "b" serão agravadas em 50% (cinquenta por cento) de sua pena-base, para cada agravante, até o limite de 60 (sessenta) meses, quando restar comprovado que a contratada tenha sofrido registro de 3 (três) ou mais penalidades no Sistema de Cadastramento Unificado de Fornecedores – SICAF em decorrência da prática de qualquer das condutas tipificadas no presente termo nos 24 (vinte e quatro) meses que antecederam o fato em decorrência do qual será aplicada a penalidade

8.7. Em qualquer hipótese de aplicação de sanções, será assegurado à licitante vencedora e ao contratado o contraditório e a ampla defesa, conforme previsto nos §§ 2° e 3°, do art.86 da Lei n° 8.666/93.

8.8. Decorridos 30 (trinta) dias sem que a contratada tenha iniciado a prestação da obrigação assumida, estará caracterizada a inexecução contratual, ensejando a sua rescisão, conforme determina o art. 77, da Lei 8.666/93.

8.9. As penalidades serão obrigatoriamente registradas no SICAF.

9. **CLÁUSULA NONA- DA SUBCONTRATAÇÃO**

9.1. Não haverá subcontratação, salvo para eventual manutenção de *hardware* que venha a compor a solução, conforme item 3.14, e para o suporte junto ao fabricante contido deste Contrato.

10. **CLÁUSULA DEZ - DA VIGÊNCIA**

10.1. O prazo de vigência da contratação é de 12 (doze) meses contados de sua assinatura.

10.2. Previamente à contratação, a Administração realizará consulta “on line” ao SICAF, bem como ao Cadastro Informativo de Créditos não Quitados – CADIN, cujos resultados serão anexados aos autos do processo.

10.2.1. Na hipótese de irregularidade do registro no SICAF, o contratado deverá regularizar a sua situação perante o cadastro no prazo de até 05 (cinco) dias, sob pena de aplicação das penalidades previstas no edital e anexos.

10.3. O prazo previsto para assinatura ou aceite poderá ser prorrogado, por igual período, por solicitação justificada da empresa e aceita pela Administração.

11. **CLÁUSULA ONZE - DO REAJUSTE DO CONTRATO**

11.1. O preço consignado no contrato será corrigido anualmente, observado o interregno mínimo de um ano, contado a partir da data limite para a apresentação da proposta, pela variação do Índice de Custos da Tecnologia da Informação (ICTI), calculado e divulgado pelo Instituto de Pesquisa Econômica Aplicada (Ipea), com base na seguinte fórmula:

$$R = [(I - Io).P]/Io$$

Em que:

Para o primeiro reajuste:

R = reajuste procurado;

I = índice relativo ao mês do reajuste;

Io = índice relativo ao mês da data limite para apresentação da proposta;

P = preço atual dos serviços.

Para os reajustes subsequentes:

R = reajuste procurado;

I = índice relativo ao mês do novo reajuste;

Io = índice relativo ao mês do início dos efeitos financeiros do último reajuste efetuado;

P = preço do serviço atualizado até o último reajuste efetuado.

11.2. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

12. **CLÁUSULA DOZE - DOS ACRÉSCIMOS E SUPRESSÕES**

12.1. O futuro contratado fica obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até 25% (vinte e cinco por cento), calculados sobre o valor inicial atualizado do contrato.

12.2. Nenhum acréscimo ou supressão poderá exceder os limites estabelecidos no subitem anterior, salvo as supressões por acordo celebrado entre as partes

13. **CLÁUSULA TREZE- DO VALOR DO CONTRATO**

13.1. O valor total estimado do presente Contrato é de **R$183.796,00 (cento e oitenta e três mil setecentos e noventa e seis reais) ,** discriminado unitariamente na tabela abaixo, correndo a despesas a conta dos recursos consignados ao Contratante, no Orçamento Geral da União, sendo sua totalidade para o exercício de 2019, sob a seguinte classificação: Programa de Trabalho **149515**, Elemento de Despesa 4.4.9.0.40.05 e 3.3.9.0.40.20, devidamente empenhado, conforme Notas de Empenho nº 2019NE800412 e nº 2019NE800413, datas de 16/12/2019.

13.2. A despesa do exercício subsequente correrá à conta da Dotação Orçamentária consignada para essa atividade no respectivo exercício.

Grupo	Item	Descrição	Unidade de medida	Órgão Gerenciador	Custo Unitário	Valor Total
1	1	Solução para segurança de computadores (500 entre desktops e laptops) e dispositivos móveis (200 entre tablets e smartphones Android e iOS) com ferramenta de gerência centralizada, instalação e suporte técnico, garantia e atualizações pelo período de 60 (sessenta) meses	Unidade	200	R$489,90	R$97.980,00
	2	Treinamento na solução de segurança de computadores e dispositivos móveis	Pessoa	2	R$2.479,00	R$4.958,00
	3	Solução para segurança de servidores (Linux e Windows) com ferramenta de gerência centralizada, instalação e suporte técnico, garantia e atualizações pelo período de 60 (sessenta) meses	Unidade	100	R$649,00	R$64.900,00
	4	Treinamento na solução de segurança de servidores	Pessoa	2	R$2.479,00	R$4.958,00
	6	Treinamento na solução de proteção de caixas de e-mail e servidores Microsoft Exchange	Pessoa	2	R$2.500,00	R$5.000,00
	8	Treinamento na solução para proteção contra ameaças persistentes avançadas	Pessoa	2	R$3.000,00	R$6.000,00
VALOR TOTAL (R$)						**R$183.796,00**

14. **CLÁUSULA QUATORZE - DO PAGAMENTO**

14.1. O pagamento será efetuado pela Contratante no prazo de 30 (trinta) dias corridos, contados da apresentação da Nota Fiscal/Fatura, contendo o detalhamento dos serviços executados e os materiais empregados, através de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

14.2. Os pagamentos decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da Lei 8.666, de 1993, deverão ser efetuados no prazo de até 5 (cinco) dias úteis, contados da data da apresentação da Nota Fiscal/Fatura, nos termos do art. 5º, § 3º, da Lei nº 8.666, de 1993.

14.3. A apresentação da Nota Fiscal/Fatura deverá ocorrer no prazo de 10 (dez) dias, contado da data final do período de adimplemento da parcela da contratação a que aquela se referir.

14.4. A Nota Fiscal deverá ser digitalizada, em formato **PDF**, e encaminhada por endereço eletrônico a ser repassado pela contratante, para fins de comprovação, liquidação e pagamento.

14.5. O pagamento somente será autorizado depois de efetuado o "atesto" pelo servidor competente, condicionado este ato à verificação da conformidade da Nota Fiscal/Fatura apresentada em relação aos serviços efetivamente prestados, devidamente acompanhada das comprovações mencionadas no §1º do art. 36, da IN/SLTI nº 02, de 2008.

14.6. Havendo erro na apresentação da Nota Fiscal/Fatura ou dos documentos pertinentes à contratação, ou ainda, circunstância que impeça a liquidação da despesa, como por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante.

14.7. Será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:

I - não produziu os resultados acordados;

II - deixou de executar as atividades contratadas, ou não as executou com a qualidade mínima exigida;

III - deixou de utilizar os materiais e recursos humanos exigidos para a execução do serviço, ou utilizou-os com qualidade ou quantidade inferior à demandada,

14.8. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

14.9. Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

14.10. Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua advertência, por escrito, para que, no prazo de 5 (cinco) dias, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da contratante.

14.11. Não havendo regularização ou sendo a defesa considerada improcedente, a contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

14.12. Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.

14.13. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao SICAF.

14.14. Somente por motivo de economicidade, segurança nacional ou outro interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da contratante, não será rescindido o contrato em execução com a contratada inadimplente no SICAF.

14.15. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável, em especial a prevista no artigo 31 da Lei 8.212, de 1993.

14.16. A Contratada regularmente optante pelo Simples Nacional, exclusivamente para as atividades de prestação de serviços previstas no §5º-C, do artigo 18, da LC 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime, observando-se as exceções nele previstas. 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.

14.17. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP, sendo:

EM = Encargos moratórios;

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

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,00016438, assim apurado:

I = (TX)	I =	(6 / 100) / 365	I = 0,00016438 TX = Percentual da taxa anual = 6%

14.18. O Cade não estará sujeito à compensação financeira a que se refere o item anterior, se o atraso decorrer da prestação irregular dos serviços ou com ausência total ou parcial de documentação hábil, ou pendente de cumprimento pela CONTRATADA de quaisquer das cláusulas do contrato.

15. CLÁUSULA QUINZE - DO REGIME DE EXECUÇÃO E DAS ALTERAÇÕES

15.1. Eventuais alterações contratuais reger-se-ão pela disciplina do art. 65 da Lei nº 8.666, de 1993, bem como do Anexo X da Instrução Normativa SEGES/MP nº 05/2017.

15.2. A diferença percentual entre o valor global do contrato e o preço global de referência não poderá ser reduzida em favor do contratado em decorrência de aditamentos que modifiquem a planilha orçamentária.

15.3. Os serviços serão prestados mensalmente sob a forma de Execução Indireta no regime de Empreitada por preço global.

15.4. A diferença percentual entre o valor global do contrato e o preço global de referência poderá ser reduzida para a preservação do equilíbrio econômico-financeiro do contrato em casos excepcionais e justificados, desde que os custos unitários dos aditivos contratuais não excedam os custos unitários do sistema de referência utilizado na forma do Decreto n. 7.983/2013, assegurada a manutenção da vantagem da proposta vencedora ante a da segunda colocada na licitação.

15.5. O serviço adicionado ao contrato ou que sofra alteração em seu quantitativo ou preço deverá apresentar preço unitário inferior ao preço de referência da administração pública divulgado por ocasião da licitação, mantida a proporcionalidade entre o preço global contratado e o preço de referência, respeitados os limites do previstos no § 1º do art. 65 da Lei nº 8.666, de 1993.

15.6. Na hipótese de celebração de aditivos contratuais para a inclusão de novos serviços, o preço desses serviços será calculado considerando o custo de referência especificado no orçamento-base da licitação, subtraindo desse preço de referência a diferença percentual entre o valor do orçamento-base e o valor global do contrato obtido na licitação, com vistas a garantir o equilíbrio econômico-financeiro do contrato e a manutenção do percentual de desconto ofertado pelo contratado, em atendimento ao art. 37, inciso XXI, da Constituição Federal.

16. CLÁUSULA DEZESSEIS – DAS VEDAÇÕES

16.1. É vedado à CONTRATADA:

16.1.1. Caucionar ou utilizar este Termo de Contrato para qualquer operação financeira;

16.1.2. Interromper a execução dos serviços sob alegação de inadimplemento por parte da CONTRATANTE, salvo nos casos previstos em lei.

17. CLÁUSULA DEZESSETE – DA RESCISÃO

17.1. O presente Termo de Contrato poderá ser rescindido nas hipóteses previstas no art. 78 da Lei nº 8.666, de 1993, com as consequências indicadas no art. 80 da mesma Lei, sem prejuízo da aplicação das sanções previstas no Contrato, anexo do Edital.

17.2. Os casos de rescisão contratual serão formalmente motivados, assegurando-se à CONTRATADA o direito à prévia e ampla defesa.

17.3. A CONTRATADA reconhece os direitos da CONTRATANTE em caso de rescisão administrativa prevista no art. 77 da Lei nº 8.666, de 1993.

17.4. O termo de rescisão, sempre que possível, deverá indicar:

17.4.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos em relação ao cronograma físico-financeiro, atualizado;

17.4.2. Relação dos pagamentos já efetuados e ainda devidos;

17.4.3. Indenizações e multas.

18. CLÁUSULA DEZOITO - DOS CASOS OMISSOS

18.1. Os casos omissos ou situações não explicitadas nas cláusulas deste Contrato regular-se-ão pela Lei nº 8.666/1993 e pelos preceitos de direito público, aplicando-se-lhes, supletivamente, os princípios da teoria geral dos contratos e as disposições de direito privado, na forma dos arts. 54 e 55, inciso XII, da Lei n. 8.666, de 21 de junho de 1993 e alterações posteriores.

19. CLÁUSULA DEZENOVE - DA PUBLICAÇÃO

19.1. Caberá ao Contratante providenciar a publicação do presente Contrato, por extrato, no Diário Oficial da União, no prazo de 20 (vinte) dias a contar do quinto dia útil do mês seguinte à data da assinatura, com indicação da modalidade de licitação e de seu número de referência, conforme dispõe a legislação vigente, Lei nº 10.520, de 17 de julho de 2002 e Lei nº 8.666, de 17 de junho de 1993 e alterações posteriores.

20. CLÁUSULA VINTE - DO FORO

20.1. As partes elegem, de comum acordo, com renúncia a qualquer outro, por mais privilegiado que seja, o Foro da Justiça Federal da Seção Judiciária do Distrito Federal para dirimir as questões decorrentes do presente Contrato.

E, por assim estarem justas e acertadas, foi lavrado o presente **CONTRATO** e disponibilizado por meio eletrônico através do Sistema Eletrônico de Informações – SEI, conforme Resolução Cade n° 11, de 24 de novembro de 2014, publicada no D.O.U. Seção 1, no dia 02 de dezembro de 2014, o qual, depois de lido e achado conforme, vai assinado pelas partes, perante duas testemunhas a tudo presente.

Documento assinado eletronicamente por **CARLA PATRICIA CARVALHO DA SILVA**, **Usuário Externo**, em 17/12/2019, às 15:12, conforme horário oficial de Brasília e Resolução Cade nº 11, de 02 de dezembro de 2014.

Documento assinado eletronicamente por **Luana Nunes Santana**, **Coordenador-Geral e Ordenador de Despesas por Subdelegação**, em 17/12/2019, às 17:58, conforme horário oficial de Brasília e Resolução Cade nº 11, de 02 de dezembro de 2014.

Documento assinado eletronicamente por **Antônio Clóvis Melhor Galvão dos Santos**, **Testemunha**, em 17/12/2019, às 18:21, conforme horário oficial de Brasília e Resolução Cade nº 11, de 02 de dezembro de 2014.

Documento assinado eletronicamente por **Ana Carolina de Oliveira Passos**, **Testemunha**, em 17/12/2019, às 18:21, conforme horário oficial de Brasília e Resolução Cade nº 11, de 02 de dezembro de 2014.

A autenticidade deste documento pode ser conferida no site http://sei.cade.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0698498** e o código CRC **2118ED8A**.

Referência: Processo nº 08700.002988/2018-01 SEI nº 0698498