CONTRATO [JUCEPA] Nº 23/2023

PAE nº 2023/750678

RESUMO

CONTRATANTE

JUNTA COMERCIAL DO ESTADO DO PARÁ | AUTARQUIA ESTADUAL
CNPJ nº 04.825.329/0001-42.

CONTRATADA

EMETH CONTABILIDADE E SERVIÇOS LTDA
CNPJ nº 30.759.519/0001-19

OBJETO

Contratação de solução de software antivírus corporativo, por subscrição (tempo determinado), para uso através de console de gerenciamento centralizado, incluindo os serviços de instalação, configuração, ativação, treinamento, suporte técnico, manutenção, assistência técnica e garantia de atualização da base de assinaturas e da versão da solução, visando a proteção dos computadores das estações de trabalho, notebooks e computador servidor, a fim de atender as necessidades do Prédio sede da JUCEPA. Esta contratação advém do PAE nº 2023/750678, o qual contém em seu seq 02, o TR que embasa a contratação que embasa a contratação, e no seq 09, a proposta comercial da empresa contratada.

LOCAL DA ENTREGA DOS BENS

Av. Gov Magalhães Barata, 1234 - São Brás, Belém - PA, 66060-281 (será prestado na Sede da JUCEPA)

VALOR TOTAL

A despesa total consiste no valor de R$ 49.000,00 (quarenta e nove mil reais)

REAJUSTE

Índice	Não aplicável
Período	Não haverá reajuste durante o período de 48 meses de vigência do contrato.

PAGAMENTO

Forma	Ordem bancária.
Prazo	**30 (trinta) dias corridos**, a contar do recebimento da nota fiscal ou fatura atestada pelo fiscal do contrato.

VIGÊNCIA

Prazo	**48 (quarenta e oito) meses**
Início	Data de assinatura
Fim	48 meses após a data de assinatura

CLÁUSULAS CONTRATUAIS

CLÁUSULA 1

Partes

Este contrato tem como PARTES:

CONTRATANTE	**JUNTA COMERCIAL DO ESTADO DO PARÁ**, autarquia estadual, CNPJ nº 04.825.329/0001-42, com sede na Av. Governador Magalhães Barata, nº 1234, CEP 66060-670, neste ato representado por sua presidente, **CILENE MOREIRA SABINO DE OLIVEIRA**.
CONTRATADA	**EMETH CONTABILIDADE E SERVIÇOS LTDA**, CNPJ nº 30.759.519/0001-19, com sede na Travessa Barão do Triunfo, nº 3540, Sala 1506, Cep. 66095-055, neste ato representado por [**TIAGO FARIAS DE BRITO**], CPF ***.976.822-**. Contatos: WhatsApp: (91) 3353-5968 ou (91) 98882-3833 / E-mail: contato@emethcontabilidade.com ou exatacontabilidadee@gmail.com

CLÁUSULA 2

Fundamento legal

O presente contrato é oriundo da **contratação direta por DISPENSA DE LICITAÇÃO nº 09/2023** constante no PAE nº 2023/750678 e é regido pela Lei Nacional nº 14.133/21, art. 75, II.

CLÁUSULA 3

Objeto

3.1 O objeto deste contrato consiste na contratação de solução de software antivírus corporativo, por subscrição (tempo determinado), para uso através de console de gerenciamento centralizado, incluindo os serviços de instalação, configuração, ativação, treinamento, suporte técnico, manutenção, assistência técnica e garantia de atualização da base de assinaturas e da versão da solução, visando a proteção dos computadores das estações de trabalho, notebooks e

computador servidor, a fim de atender as necessidades do Prédio sede da JUCEPA.

3.2 Este instrumento se vincula ao ato que tiver autorizado a contratação direta e à respectiva proposta citado na Cláusula 2, e aos anexos desses documentos.

3.3 Os serviços contratados são os seguintes itens descritos no termo de referência:

Item único	Descrição	Código SIMAS	Und.	Qtd.	Valor Unitário	Total
01 – Licenças por subscrição de uso de software antivírus corporativo	Contratação de solução de software antivírus corporativo, por subscrição (tempo determinado), para uso através de console de gerenciamento centralizado, incluindo os serviços de instalação, configuração, ativação, treinamento, suporte técnico, manutenção, assistência técnica e garantia de atualização da base de assinaturas e da versão da solução, visando a proteção dos computadores das estações de trabalho, notebooks e computador servidor, a fim de atender as necessidades do Prédio sede da JUCEPA.	23979-8	Unidade	200	R$ 245,00 (duzentos e quarenta e cinco reais)	R$ 49.000,00 (quarenta e nove mil reais)

Total	**R$ 49.000,00 (quarenta e nove mil reais)**

3.4. O serviço será prestado conforme emissão de ordem de serviço.

CLÁUSULA 4

Especificações técnicas do objeto

4.1.Solução de software antivírus corporativo

4.1.1 Deve possuir capacidade de instalação e pleno funcionamento dos módulos solicitados em estações de trabalho com no mínimo 3Gb de memória RAM.

4.1.2 Deve suportar as seguintes plataformas clientes: Windows 10; Windows 8.1; Windows 8; Mojave 10.14.x; High Sierra 10.13.x; Sierra 10.12.x; El Captain 10.11.x.

4.1.3 Deve suportar as seguintes plataformas servidores: Windows Server 2016;Windows Server 2012 R2; Windows Server 2012; Windows Storage Server 2012;

4.1.4 Deve inclusive suportar o modo Server Core.

4.1.5 Deve suportar, pelo menos as funções de antivírus e firewall de host, nas seguintes distribuições de Linux: Red Hat Enterprise 6.x, 7.x e 8.x, 64bits; SUSE Linux Enterprise Server 12.x e 15.x, 64bits; Ubuntu 16.04, 18.04, 19.10, 64bits; CentOS 6.x, 7.x e 8.x, 64bits; Oracle Linux 6, 7 e 8, 64bits; Amazon Linux 64bits.

4.1.6 Deve suportar a instalação de agente nos sistemas operacionais acima virtualizados nas seguintes plataformas: AWS; Azure; Citrix XenApp; Citrix XenDesktop; Citrix XenServer; Microsoft Hyper-V 2012 R2; Vmware ESXi; Vmware Player; Vmware vShpere; Vmware Workstation.

4.1.7 A solução deve compreender, no mínimo, as seguintes funcionalidades: Módulo antimalware; Módulo de firewall de host; Módulo de filtragem web; Módulo de proteção contra ameaças avançadas; Módulo para controle de dispositivos; Módulo para controle de aplicações;

4.1.8 Todas as funcionalidades deverão ser geridas por uma console única com as capacidades mínimas de: Relatórios; Dashboards; Políticas; Configuração; Instalação/Desinstalação;

4.1.9 O cliente deve ser capaz de operar em modo autônomo (self-managed) e permitir que as configurações sejam aplicadas diretamente no cliente.

4.1.10 O cliente deve ser capaz de atualizar as definições para detecção de ameaças, patches e hotfixes a partir de um servidor definido pelo administrador ou diretamente nos servidores do fabricante.

4.1.11 A solução de prevenção deve ser colaborativa, ou seja, os módulos exigidos devem ser capazes de trocarem informações para uma análise mais inteligente.

4.1.12 A solução deve possuir múltiplas camadas de proteção, não serão aceitas soluções baseadas apenas em assinaturas.

4.1.13 A solução deve conter módulo capaz de proteger contra botnets, negação de serviço, executáveis não confiáveis e conexões web maliciosas.

4.1.14 A solução deve conter módulo capaz de garantir uma navegação web segura, prevenindo contra sites maliciosos, downloads de ameaças e garantir a política de acesso (Permitir/Negar).

4.1.15 Possuir características de Módulo Antimalware (Clientes Windows).

4.1.16 Possuir características da prevenção contra exploração.

4.1.17 Deve possibilitar selecionar, no mínimo:

4.1.17.1 Dois modos de proteção (Padrão/Máximo);

4.1.17.2 Ativar/desativar a proteção contra escalonamento de privilégios genéricos;

4.1.17.3 Ativar/desativar a prevenção de execução de dados do Windows.

4.1.17.4 Selecionar dentre as ações de apenas bloquear ou apenas relatar ou bloquear e relatar;

4.1.17.5 Bloquear contra falsificação de IP (IP Spoofing).

4.1.17.6 Deve possibilitar incluir exclusões por: Processo; Nome; Caminho do Arquivo; Hash MD5; Módulo chamador; Nome; Caminho; Hash MD5; Signatário Digital.

4.2 Características da Proteção de acesso

4.2.1 Deve fornecer regras de proteção de maneira nativa, ou seja, pré-definidas pelo fabricante da solução, no mínimo, para: Acesso remoto a pastas locais; Alteração políticas de direitos dos usuários; Alterar os registros de extensão dos arquivos; Criação de novos arquivos na pasta Arquivo de Programas; Criação de novos executáveis na pasta Windows; Criar/Modificar remotamente arquivos Portable Executable, INI, PIF e as localizações do sistema; Criar ou Modificar remotamente arquivos ou pastas; Desativar o editor de registro e o gerenciador de tarefas; Executar arquivos das pastas do usuário; Execução de scripts pelo host de script do Windows; Instalar objetos de ajuda a navegação ou extensões de shell; Instalar novos CLSIDs, APPIDs e TYPELIBs; Modificar configurações de rede; Modificar configurações do Internet Explorer; Modificar processos principais do Windows; Navegadores iniciando programas da pasta de downloads; Registrar programas para execução automática. As regras especificadas devem permitir o: Bloqueio, ou evento de Informação, ou bloqueio e Evento de Informação.

4.2.2 Deve permitir ao administrador criar regras customizadas com no mínimo os seguintes parâmetros: Processos; Nome do processo; Hash MD5; Assinatura Digital; Usuário; Arquivos; Criação; Deletar; Executar; Alteração de permissão; Leitura; Renomear; Escrever; Chave de Registro; Escrever; Criar; Deletar; Ler; Enumerar; Carregar; Substituir; Restaurar; Alterar permissão; Valor de Registro; Ler; Criar; Deletar; Processo; Qualquer acesso; Criar thread; Modificar;Terminar; Executar.

4.2.3 Deve permitir a configuração de exclusões.

4.3. Características da varredura ao acessar

4.3.1 A Varredura deve ser passível de habilitação/desativação por opção do administrador.

4.3.2 Deve iniciar a proteção durante a inicialização do sistema operacional.

4.3.3 Deve ser capaz de realizar análise no setor de boot.

4.3.4 O administrador da solução deve especificar o tempo máximo de análise para um único arquivo.

4.3.5 Deve analisar dos processos durante inicialização do serviço e na atualização de conteúdo.

4.3.6 Deve possibilitar ao administrador a análise de instaladores confiáveis.

4.3.7 Deve realizar análise durante cópia entre pastas locais.

4.3.8 A solução deve possuir conexão com Centro de Inteligência do fabricante, passível de ativação ou desativação por parte do administrador.

4.3.9 Deve permitir a configuração do nível de agressividade da análise entre: Muito Baixo; Baixo; Médio; Alto; Muito Alto.

4.3.10 Deve possibilitar aplicar as configurações a todos os processos do sistema operacional ou a uma lista específica criada pelo administrador.

4.3.11 Deve realizar varredura quando o processo: Ler o disco; Gravar no disco; Deixar a solução decidir.

4.3.12 Deve possibilitar análise em: Unidades de Rede; Arquivos abertos para backup; Arquivos compactados, por exemplo.jar; Arquivos codificados (MIME).

4.3.13 Deve detectar programas indesejados, ameaças em programas desconhecidos e ameaças em macro desconhecidas.

4.3.14 Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar uma ameaça: Limpar o arquivo; Excluir o arquivo; Negar acesso ao arquivo.

4.3.15 Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar um programa indesejado: Limpar o arquivo; Excluir o arquivo; Permitir acesso ao arquivo; Negar acesso ao arquivo.

4.3.16 Deve possibilitar ao administrador a gestão de uma lista de exclusões.

4.3.17 Deve possuir módulo capaz de interceptar scripts (Javascript e VBScript) destinados ao Windows Host Scripting e analisá-lo para indicar se é malicioso ou não.

4.3.18 Deve permitir a criação de listas de exclusão de URLs que não sofrerão interceptação e análise de scripts.

4.3.19 Ao detectar uma ameaça o agente deverá emitir uma notificação ao usuário com uma mensagem a ser customizada pelo administrador da solução.

4.4 Características da Varredura sob demanda

4.4.1 Deve ser possível realizar varreduras agendadas com periodicidade diária ou semanal.

4.4.2 Deve permitir a criação de repetição da tarefa.

4.4.2.1 Deve permitir definir a hora da execução da tarefa de análise.

4.4.2.2 Deve permitir a criação da tarefa de varredura de maneira aleatória.

4.4.2.3 Deve permitir a realização de varreduras agendadas após logon do usuário ou durante inicialização do sistema operacional.

4.4.3 Deve permitir escolher (um ou mais) os alvos da varredura, dentre eles: Os locais da varredura; Memória para rootkits; Processos em execução; Arquivos registrados; Meu computador; Todas as unidades locais; Todas as unidades fixas; Todas as unidades removíveis; Todas as unidades mapeadas; Pasta inicial; Pasta de perfil do usuário; Pasta Windows; Pasta de arquivos de programas; Pasta temporária; Lixeira; Arquivo ou pasta especificada pelo administrador; Setor de inicialização (boot); Arquivos compactados; Arquivos MIME; Os tipos de arquivos que serão analisados; Opções adicionais, como por exemplo detecção de programas indesejados, ameaças em programas desconhecidos e ameaças em macro desconhecidas; e Áreas de exclusão que não deverão ser varridas,

4.4.4 Deve permitir a integração com o Centro de Inteligência do fabricante durante a varredura agendada.

4.4.5 Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar uma ameaça: Limpar o arquivo; Excluir o arquivo; e Negar acesso ao arquivo.

4.4.6 Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar um programa indesejado: Limpar o arquivo; Excluir o arquivo; Permitir acesso ao arquivo; e Negar acesso ao arquivo.

4.4.7 Para minimizar o impacto ao usuário, a solução deve permitir:

4.4.7.1 Utilização de cache, ou seja, arquivos que já foram analisados e não tiveram seu conteúdo alterado não serão novamente analisados;

4.4.7.2 Iniciar a varredura apenas quando o sistema estiver ocioso;

4.4.7.3 Permitir ao usuário retomar varreduras pausadas.

4.4.8 Deve permitir ao administrador inserir uma conta de domínio para realizar a análise de dispositivos de rede.

4.4.9 Possibilitar características de Módulo Antimalware (Clientes Linux).

4.4.10 Possibilitar características da prevenção de ameaças.

4.4.11 Deve permitir a atualização automática das vacinas de detecção.

4.4.12 Deve detectar ameaças usando métodos de acesso e de varredura sob demanda.

4.4.13 Deve permitir a execução de varreduras por meio da console centralizada por meio de tarefas.

4.4.14 Ao detectar uma ameaça, deverá responder com, no mínimo, as seguintes ações: Limpar o arquivo; Deletar o arquivo; Negar acesso ao arquivo.

4.4.15 Deve possibilitar ao administrador, criar exceções de análise, ou seja, não permitir que a ferramenta execute uma análise em determinadas pastas ou arquivos.

4.4.16 Deve permitir a opção de manter a configuração de exclusão realizada no

agente, não sendo sobrescrita pela política principal.

4.4.17 Deve permitir a gestão do agente local por meio de linha de comando.

4.4.18 Quando configurar a análise ao acessar, deve permitir: Quando analisar (exemplo: ao ler o arquivo); O que analisar (exemplo: todos os arquivos); Análise de arquivos compressos; Análise de volumes de rede; e Análise de programas não desejados.

4.4.19 Ao configurar a análise sob demanda, deve permitir: Análise de arquivos compressos; Análise de PUP; Análise de macros desconhecidos; Análise de programas desconhecidos; Caminhos da análise (path); Análise de pastas e subpastas; Análise de macros; Exclusão de paths, pastas e tipos de arquivos; Uso de cache; Ação Primária e Secundária.

4.4.20 Deve possuir quarentena local para armazenar ameaças desconhecidas.

4.4.21 Deve possuir ação para mover artefatos maliciosos para a área de quarentena.

4.4.22 Deve usar heurística para detectar arquivos potencialmente maliciosos.

4.4.23 Caso aconteça um timeout durante uma análise, deve permitir ao administrador a configuração de permitir ou negar o acesso ao arquivo.

4.5 Características do Módulo de Firewall de Host (Clientes Windows)

4.5.1 Deve permitir a ativação/desativação do módulo de Firewall através da console;

4.5.2 Deve ser capaz de prevenir intrusões e proteger os endpoints garantindo cobertura para ataques dia zero;

4.5.3 Deve possuir um firewall de estação stateful bloqueando tráfego de entrada e controlando o tráfego de saída; Deve possuir assinaturas de proteção para: Arquivos; Chave de Registro; Processos; Serviços.

4.5.4 Deve permitir o tráfego de saída somente após os serviços de Firewall estiverem iniciados.

4.5.5 Deve possibilitar bloquear tráfego bridge.

4.5.6 O módulo deve permitir a criação de regras de maneira adaptativa, ou seja, em uma estação modelo definida pelo administrador deve ser capaz de criar as regras de maneira automática.

4.5.7 Deve ser possível bloquear o tráfego de todos os processos identificados como não confiáveis.

4.5.8 Deve permitir a criação de uma lista de processos identificados como confiáveis por meio das seguintes informações: Nome; Nome do arquivo ou Caminho; Hash MD5; e Assinador Digital.

4.5.9 Deve permitir integração com o Centro de Inteligência do próprio fabricante para bloqueio de ameaças advindas por meio de conexões maliciosas.

4.5.10 As conexões identificadas pelo Centro de Inteligência devem poder ser configuradas por meio de reputação mínima a ser bloqueada, por exemplo Risco Alto ou Risco Médio.

4.5.11 Deve ser possível registrar os eventos de conexões bloqueadas e permitidas

pelo módulo.

4.5.12 Deve permitir inspeção do protocolo FTP.

4.5.13 Deve ser possível permitir tráfego de protocolos não suportados.

4.5.14 Deve vir módulo de Firewall com regras pré-indicadas pelo próprio fabricante.

4.5.15 No módulo de Firewall deve permitir a criação de regras customizadas, com no mínimo os seguintes parâmetros: Ação; Bloquear; Permitir; Direção; Ambas; Entrada; Saída; Protocolo; Qualquer protocolo; Protocolo IP; Ipv4; Ipv6; Protocolo Não-IP; Tipo de Conexão; Rede Sem Fio; Rede Cabeada; Rede Virtual; Especificação da Rede; Endereço IP; Subnet; Range; FQDN; Protocolo de Transporte; Todos; ICMP; ICMPv6; TCP; UDP; STP; GRE; IGMP; IPSEC AH; IPSEC ESP; Ipv6 in Ipv4; ISIS over Ipv4; L2TP; Agendamento; Dias da Semana; Hora Início; Hora Fim; Aplicações.

4.6 Características do Módulo de Firewall de Host (Clientes Linux)

4.6.1 Deve permitir a ativação/desativação do módulo de Firewall através da console.

4.6.2 Deve possuir um firewall de estação stateful bloqueando tráfego de entrada e controlando o tráfego de saída.

4.6.3 O módulo deve permitir a criação de regras de maneira adaptativa, ou seja, em uma estação modelo definida pelo administrador deve ser capaz de criar as regras de maneira automática.

4.6.4 Deve permitir inspeção do protocolo FTP.

4.6.5 Deve vir módulo Firewall com regras pré-indicadas pelo próprio fabricante.

4.6.6 No módulo de Firewall deve permitir a criação de regras customizadas, com no mínimo os seguintes parâmetros: Ação; Bloquear; Permitir; Direção; Ambas; Entrada; Saída; Protocolo; Qualquer protocolo; Protocolo IP; Ipv4; Tipo de Conexão; Rede Sem Fio; Rede Cabeada; Rede Virtual; Especificação da Rede; Endereço IP; Subnet; Range; FQDN; Protocolo de Transporte; Todos; ICMP; TCP; UDP; Agendamento; Dias da Semana; Hora Início; Hora Fim.

4.7 Características do Módulo de Filtragem Web

4.7.1 Deve permitir o bloqueio de browsers não suportados, dentre eles: Opera; Safari for Windows; Netscape; Maxthon; Flock; Avant Browser; Deepnet Explorer; PhaseOut;

4.7.2 Deve permitir o controle de browsers suportados, dentre eles: Chrome; Firefox; e Internet Explorer.

4.7.3 Deve ser capaz de utilizar lista de categorias para bloqueio de sites relacionados ao conteúdo não autorizado.

4.7.4 Deve possuir, no mínimo, as seguintes categorias: Browser Exploits; Download Maliciosos; Sites Maliciosos; Phishing; Pornografia; Hacking/Computer Crime; Spyware/Adware/Keyloggers; Anonymizer; Anonymizer Utilities; Alcohol; Blogs/Wiki; Business; Chat; Content Server; Dating; Dating/Social Networking; Digital Postcards; Discrimination; Drugs; Education; Entertainment; Extreme; Fashion; Finance; For Kids; Forum; Gambling; Game/Cartoon Violence; Games; General News; Government/Military; Gruesome Content; Health; Historical

Revisionism; History; Humor/Comics; Illegal UK; Incidental Nudity; Information Security; Instant Messaging; Interactive Web Applications; Internet Radio/TV; Internet Services; Job Search; Major Global Religions; Marketing/Merchandising; Media Downloads; Media Sharing; Messaging; Mobile Phone Moderated; Motor Vehicles; Non-Profit/Advocacy/NGO; Nudity; Online Shopping; P2P/File Sharing; Parked Domain; Personal Network Storage; Personal Pages; Pharmacy; Politics/Opinion; Portal Sites; Potential Criminal Activities; Potential Illegal Software; Potentially Unwanted Programs; Profanity; Professional Networking; Provocative Attire; Public Information; Real Estate; Recreation/Hobbies; Religion/Ideology; Remote Access; Residential IP Addresses; Resource Sharing; Restaurants; School Cheating Information; Search Engines; Sexual Materials; Shareware/Freeware; Social Networking; Software/Hardware; Spam URLs; Sports; Stock Trading; Streaming Media; Technical Information; Technical/Business Forums; Text Translators; Text/Spoken Only; Tobacco; Travel; Uncategorized; Usenet News; Violence; Visual Search Engine; Weapons; Web Ads; Web Mail; Web Meetings; Web Phone.

4.7.5 Deve ser possível bloquear um site conforme a sua classificação: Vermelho: Alto Risco; Amarelo: Médio Risco; e Cinza: Não categorizado.

4.7.6 Deve ser possível bloquear um site quando este nunca foi visto pelo Centro de Inteligência do Fabricante.

4.7.7 Deve ser possível bloquear páginas de phishing, mesmo que o conteúdo tenha acesso permitido.

4.7.8 Deve permitir a varredura de arquivos baixados da internet.

4.7.9 Deve ser possível excluir endereços IP da análise.

4.7.10 Deve permitir a busca segura para buscadores, dentre eles: Google; Yahoo; Bing; Ask.

4.7.11 Deve bloquear links que direcionem para sites com alto risco.

4.7.12 Deve permitir a customização das mensagens apresentadas para o usuário.

4.8 Características do Módulo de Ameaças Avançadas

4.8.1 A solução deve permitir o confinamento dinâmico de aplicativos e arquivos executáveis com indícios maliciosos (Ransomware).

4.8.2 A solução deve ser capaz de avaliar aplicações desconhecidas e potencialmente maliciosas executando-as em ambiente controlado.

4.8.3 Deve permitir a indicação de aplicações confiáveis para que não caiam no filtro de confinamento dinâmico.

4.8.4 Não deve requerer conexão com centro de inteligência do fabricante para que a proteção seja ativada ou executada.

4.8.5 Solução deve manter um cache de reputação local com informações de aplicações – conhecidas, desconhecidas e maliciosas.

4.8.6 Dentre os comportamentos maliciosos, deve ser capaz de:

4.8.6.1 Bloquear acesso local a partir de cookies;

4.8.6.2 Criação de arquivos a partir de arquivos com extensão .bat, .exe, html, hpg, bmp, job e .vbs;

4.8.6.3 Criação de arquivos em qualquer local de rede;

4.8.6.4 Criação de novos CLSIDs, APPIDs e TYPELIBs;

4.8.6.5 Criação de threads em outro processo;

4.8.6.6 Bloquear a desativação de executáveis críticos do sistema operacional;

4.8.6.7 Leitura/Exclusão/Gravação de arquivos visados por Ransomwares;

4.8.6.8 Gravação e Leitura na memória de outro processo;

4.8.6.9 Bloqueio de Modificação da política de firewall do Windows;

4.8.6.10 Bloqueio de Modificação da pasta de tarefas do Windows;

4.8.6.11 Bloqueio de Modificação de arquivos críticos do Windows e Locais do Registro;

4.8.6.12 Bloqueio de Modíficação de arquivos executáveis portáteis;

4.8.6.13 Bloqueio de Modificação de bit de atributo oculto;

4.8.6.14 Bloqueio de Modificação de bit de atributo somente leitura;

4.8.6.15 Bloqueio de Modificação de entradas de registro de DLL AppInit;

4.8.6.16 Bloqueio de Modificação de locais do registro de inicialização;

4.8.6.17 Bloqueio de Modificação de pastas de dados de usuários;

4.8.6.18 Bloqueio de Modificação do local do Registro de Serviços;

4.8.6.19 Bloqueio de Suspensão de um processo;

4.8.6.20 Bloqueio de Término de outro processo.

4.8.7 Dos comportamentos quando observados, deve ser possível bloquear ou apenas informar caso o mesmo ocorra.

4.8.8 Deve ser capaz de informar ao usuário as ameaças encontradas através de mensagem customizada.

4.8.9 Deve possuir modo de ativação de confinamento dinâmico para quaisquer arquivos desconhecidos acessados pelo sistema operacional e nunca antes visto pela solução.

4.8.10 Deve ser possível atribuir a regra conforme política equilibrada, visando maior segurança ou produtividade do usuário.

4.8.11 A proteção deve estar contida no mesmo agente de proteção, não requerendo outro software ou aplicação adicional na estação de trabalho para a execução e ativação da proteção.

4.8.12 Deve possuir capacidade de inspecionar arquivos suspeitos e detectar comportamentos maliciosos, utilizando técnicas de "machine-learning".

4.8.13 Características do módulo de reputação de arquivos e compartilhamento de informações de segurança:

4.8.13.1 Deve ser fornecida em formato de appliance virtual.

4.8.13.2 O appliance virtual deve ser compatível no mínimo com ambiente virtualizado VMWare ESX.

4.8.14 A solução deve possuir capacidade de criar uma reputação local ou utilizar uma já existente em nuvem através da catalogação de todos os executáveis

existentes no ambiente.

4.8.15 O servidor de orquestração deverá habilitar a troca de informação de ameaças entre os endpoints e servidores protegidos.

4.8.16 Este módulo deverá habilitar um protocolo de troca de informações de ameaças que permita o intercâmbio de informações entre soluções do mesmo fabricante e de fabricantes terceiros.

4.8.17 A troca de informação de ameaças deve se dar por meio de protocolo performático.

4.8.18 De forma a permitir menor impacto na rede, para tal método de consulta dos clientes a base de dados poderá ser síncrona ou assíncrona.

4.8.19 A solução deverá apresentar a reputação dos arquivos definida para cada um dos ativos conectados, dentre eles: reputação local e reputação do centro de inteligência.

4.8.20 Ao catalogar um arquivo, a solução deve apresentar, no mínimo as seguintes informações: Nome do arquivo; Caminho do arquivo; Hash sha-1; Hash 256; Primeira visualização do arquivo na rede; Última visualização do arquivo na rede; Tamanho do arquivo; Data de compilação; Se o mesmo consta no adicionar/remover programas; Se está registrado como serviço; Se está registrado para ser executado automaticamente; Tipo de compactador; Se é arquivo do sistema; Se foi executado a partir do cmd.exe; Se tem entrada no menu iniciar; Se foi executado a partir de uma mídia removível; e Se foi executado a partir da raiz da unidade do sistema.

4.8.21 Caso o arquivo tenha como origem a Internet, a solução deverá ser capaz de informar a partir de qual URL o arquivo foi obtido e a reputação desta última.

4.8.22 Deve ser possível realizar uma pesquisa do arquivo em base de conhecimento de terceiros (exemplo: Virus Total).

4.8.23 Após análise pela solução o administrador deve ter a possibilidade de:

4.8.23.1 Rastrear em quais estações o arquivo foi executado;

4.8.23.2 Identificar o arquivo como confiável;

4.8.23.3 Identificar o arquivo como desconhecido;

4.8.23.4 Identificar o arquivo como malicioso

4.8.23.5 Analisar o certificado associado ao arquivo;

4.8.23.6 Identificar o certificado associado como confiável ou malicioso.

4.8.24 Para minimizar o impacto a solução deve ter a capacidade de ser ativada no modo de observação nos endpoints e servidores protegidos.

4.8.25 Deve possibilitar bloquear a execução de arquivos nunca antes vistos ou suspeitos no ambiente e informar o usuário por meio de mensagem.

4.8.26 Deve ser capaz de identificar manualmente um arquivo como malicioso impedindo sua execução no ambiente.

4.8.27 Deve ser gerenciado pela mesma console de gerenciamento da solução de proteção de endpoints e servidores.

4.9 Características da solução de Detecção e Resposta a Incidentes

4.9.1 Capacidade de Detectar e Responder a incidentes relacionadas a ameaças avançadas, com capacidade avançada de investigação e que permita ao gestor da solução rápida resposta.

4.9.2 Deve permitir por meio de severidade dos alertas que o operador da solução facilmente entenda a ameaça e priorize o tratamento.

4.9.3 Deve facilitar a operação por meio de guias de investigação que automaticamente coleta, sumariza e visualmente evidencie, por meio de fontes diversas, a interação conforme a investigação avance.

4.9.4 A ferramenta deve possuir capacidade de monitoramento contínuo em tempo real.

4.9.5 Deve possuir base de dados analítica na nuvem, permitindo uma adoção mais rápida e otimizada das novas técnicas e motores analíticos para auxiliar na detecção de ameaça.

4.9.6 A ferramenta deve possuir mapeamento do framework do MITRE ATT&CK para determinar a fase de uma determinada ameaça, risco associado e que com base nestas informações auxilie na priorização de uma resposta.

4.9.7 Os guias de investigação devem utilizar inteligência artificial para auxiliar na identificação dos principais problemas detectados que identifiquem a causa raíz do ataque.

4.9.8 Deve permitir a integração com outras soluções e bases terceiras para coletar informações que agreguem mais contexto e relevância a investigação, como por exemplo: SIEM – Splunk Enterprise Security Manager; SIEM – Micros Focus ArcSight Enterprise Security Manager; SIEM – McAfee Enterprise Security Manager; Centro de Inteligência do próprio fabricante; e VirusTotal.

4.9.9 A solução deverá prover buscas diversas, abrangendo:

4.9.10 Busca histórica, permitindo a visibilidade, em detalhes, dos indicadores de comprometimento e indicadores de ataque. A informação deverá estar disponível mesmo que o dispositivo investigado esteja desligado.

4.9.11 Busca Tempo Real, permite o acesso em tempo real ao dispositivo investigado em busca de uma determinada informação.

- Busca Sob-Demanda, para suplementar uma investigação, deve permitir a captura de uma imagem (snapshot) do dispositivo investigado, permitindo que esta imagem seja capturada de máquinas gerenciadas e não gerenciadas.

4.9.12 A gestão dos dispositivos, pode ser feita por meio de console:

4.9.12.1 On-Premise: Toda camada de comunicação e gestão dos agentes é instalada no ambiente, entretanto a console de investigação está na nuvem do fabricante (SaaS).

4.9.12.2 SaaS: Toda camada de comunicação e gestão dos agentes é gestionada na nuvem do fabricante, em conjunto com a console de investigação.

4.9.13 Deve suportar sistemas operacionais nas arquiteturas 32-bits e 64-bits para os agentes, dentre os sistemas, deverão suportar, no mínimo: Windows; Windows 10 Enterprise; Windows 8.1 Enterprise; Windows 8; Windows Server 2016 (64-bits); Windows Server 2012 (64-bits); MacOS; Mojave 10.14; High Sierra 10.13; Linux;

CentOS (64-bits); Red Hat (64-bits); SUSE (64-bits).

4.9.14 A solução deve possuir capacidade investigativa, informando:

4.9.14.1 Total de investigações abertas;

4.9.14.2 Novas Investigações por dia;

4.9.14.3 Principais Detecções;

4.9.14.4 Tempo total gasto nas investigações;

4.9.14.5 Tempo total gasto nas investigações pelo usuário logado;

4.9.14.6 Quantidade de investigações com prioridade alta;

4.9.14.7 Quantidade de investigações fechadas;

4.9.14.8 Quantidade de investigações em aberto.

4.9.15 A solução deverá possuir um painel de alertas, contendo os principais "achados" (findings) detectados pela solução.

4.9.16 Deverá dividir os alertas por prioridade, entre: Alto,Médio e Baixo.

4.9.17 O painel de alerta, deverá possuir integração com o Framework do MITRE ATT&CK, apresentando: Data, hora e ano da ocorrência; Linha de comando envolvida; Tática; Técnica; Ativo envolvido; Nome do Processo e; Indicadores Suspeitos, com detalhes.

4.9.18 O Painel de Alertas deverá permitir ao analista, que este possa visualizar, em mais detalhes o alerta, apresentando:Versão do Sistema Operacional; Endereço IP; MAC Address; Última data de Boot; Tags e; Usuário Logado.

4.9.19 A solução deverá permitir buscas, nos dispositivos gerenciados, nos modos histórico e em temporeal.

4.9.20 No modo histórico, deverá apresentar as informações correlacionadas com o Framework do MITRE ATT&CK.

4.9.21 No modo histórico, ao selecionar um dos dispositivos gerenciados, deverá apresentar:

4.9.21.1 Detecções e Alertas, contendo: Data, hora e ano; ID do Processo envolvido; Nome do Processo; Linha de Comando; Usuário; Tática e; Técnicas.

4.9.21.2 Histórico de execução de Processos: Data, hora e ano; ID do processo; Usuário (Autor); Nome original do processo e; MD5/SHA-256.

4.9.21.3 Linha de Comando: Manipulação de arquivos; Data, hora e ano; Atividade (Deletado, Executado, Criado); MD5/SHA-256 do arquivo; Nome do arquivo; ID do Processo; Nome original do arquivo; Linha de comando de execução; Tamanho (bytes);

4.9.21.4 Criação de arquivos do tipo Archive: Data, hora e ano; Atividade; Nome do arquivo; Extensão (Exemplo: Bin, ZIP, dentre outros) e; Caminho.

4.9.21.5 Detecção de Scripts: Data, hora e ano; Atividade (Leitura, Criação, Movido, dentre outros); Nome do arquivo; Extensão (Exemplo: JS, Powershell);

4.9.21.6 Ferramentas Administrativas ou Hacking: Data, hora e ano; Usuário (Autor); Processo; ID do processo; MD5/SHA-256,

4.9.21.7 Linha de comando: Alteração dos Serviços do Sistema Operacional; Data,

hora e ano; Nome do Serviço; Ação (Exemplo: Adicionado, Modificado); Tipo.

4.9.21.8 Tipo de inicialização do processo: Conexão de Rede, Data, hora e ano; ID do Processo e;Tipo (Exemplo: Conexão aberta).

4.9.21.9 Direção do fluxo: Endereço IP de Origem; Porta de Origem; Endereço IP de Destino; Porta de Destino; Protocolo; Hostname.

4.9.21.10 Tarefas agendadas: Data, hora e ano; Usuário; Nome da tarefa; Comando da tarefa; Ação.

4.9.21.11 Requisições de DNS: Data, hora e ano; ID do processo; Domínio; Tipo;

4.9.21.12 Atividade de Logon: Data, hora e ano; Usuário; Tipo; Domínio; Tipo de Logon.

4.9.21.13 DLLs Carregadas: Data. Hora e ano.

4.9.21.14 Módulo: Caminho; Sha256 da DLL; Data, hora e ano que a dll foi carregada e; Id do processo.

4.9.22 Adicionalmente a busca histórica a ferramenta deve possuir capacidade de busca nos equipamentos gerenciados em tempo real.

4.9.23 Para a busca nos equipamentos gerenciados, a solução deve ser composta por coletores capazes de consolidar informações relacionadas a dados que devem ser monitorados e apresentados na console para investigação.

4.9.24 O fabricante deverá disponibilizar coletores para, no mínimo, a coleta das seguintes informações nos dispositivos gerenciados: Registro do Windows; Perfil dos Usuários; Dispositivos USB; Informação de inicialização do sistema operacional; Softwares instalados; Serviços do sistema operacional; Tarefas agendadas; Processos em execução; Drives de Rede; Sessão de Rede; Flows de Rede; Usuários Logados; Updates do Windows instalados.

4.9.25 Ferramenta deve permitir que coletores customizados sejam criados para as seguintes plataformas: Windows, Mac e Linux.

4.9.26 A criação de coletores customizados deve utilizar linguagem comum aos sistemas, como por exemplo: Powershell; Python; Visual Basic; Bash e; Comandos do sistema operacional.

4.9.27 A busca em tempo real, ao se obter o resultado desejado, deve permitir que se aplique reações, frente a busca realizada.

4.9.28 As reações devem conter: Isolamento de um Endpoint; Matar Processo; Remover um arquivo e; Logoff do usuário logado.

4.9.29 Deve permitir a criação de reações customizadas para atuar em conjunto com a busca realizada e seu respectivo resultado.

4.9.30 A busca em tempo real deve possuir capacidade de sugerir os parâmetros de busca para facilitar a obtenção do resultado desejado.

4.9.31 Caso a busca tenha um erro em sua sintaxe, a console deverá emitir um alerta de erro. Caso contrário, apresentar que a busca é válida.

4.9.32 Deve apresentar a quantidade de hosts que receberam o comando de busca em tempo real.

4.9.33 Deve prover registro do histórico de ações executados com as seguintes

informações em tela: Dispositivo; Ação; Sistema Operacional; Tag ePO; Endereço MAC e; Endereço IP.

4.9.34 Deve ser capaz de implementar visibilidade dos dados gerados pelo Endpoint, como por exemplo: Processos; Fluxos de comunicação de rede; Arquivos; Perfil de Usuários; Registro do Windows; Atualizações Instalados; Grupos Locais Informação do Host.

Deve ser capaz de apresentar, no mínimo, as seguintes informações após a busca: Endereço IP Local; Hash do processo em execução; ID do processo; Status da transação TCP; Número da porta que originou o pacote de rede; Nome do arquivo; Última data de gravação do arquivo; Data de Criação do arquivo; Data de deleção do arquivo; Versão do Sistema Operacional; Nome do Grupo de usuários; Se o grupo é local; SID do grupo; MAC de origem; MAC de destino; FLAGS TCP (ACK, SYN, RST e FIN); Número de transação TCP; Kernel Time; User Time; Comando que iniciou o processo; Quantidade de RAM utilizada pelo processo; Quantidade de Threads criadas pelo processo; MD5 do processo; SHA-1 do processo; Valor da chave de registro e; Caminho da chave de registro.

4.9.35 A resposta a uma determinada condição deverá ser executada como um serviço não interativo.

4.9.36 O Painel de investigação deve ser simples, intuitivo e capaz de informar, de maneira resumida, a postura corrente das investigações, em curso e fechadas.

4.9.37 Deve permitir a criação de até 10 investigações por hora.

4.9.38 Cada porção de dado coletado pela solução para apresentação no painel de investigação, deve ficar disponível por até 30 dias.

4.9.39 As investigações, podem ser classificadas por severidade (exemplo: Severidade Alta).

4.9.40 Ao acessar um caso de investigação, a solução deverá apresentar, de maneira sumarizada, a quantidade de artefatos descoberta, a quantidade de artefatos chave e a quantidade de pontos chave no qual o operador da solução deve focar.

4.9.41 Deve permitir adicionar integrações que suplementem a investigação de um determinado caso, a exemplo o envio de um phishing para análise pela solução e posterior adição a um caso de investigação.

4.9.42 Por meio de painéis interativos (widgets) a solução deve prover informações relacionadas a:

4.9.42.1 Sumário: informando a criação, dono da investigação e um campo para detalhamento da descrição

4.9.42.2 Notas: inserção de notas pertinentes a investigação em curso.

4.9.42.3 Itens Investigados: Sumário contendo a quantidade de dispositivos envolvidos, contas de usuário, endereços IP's, DNS, FQDN, processos, serviços, arquivos e conexões de rede.

4.10 Investigações Correlacionadas

4.10.1 Guias de Investigações: Os guias de investigação deverão ser baseados em:

4.10.1.1 Perguntas Respondidas: Contendo as principais perguntas que devem ser

respondidas pelos analistas, como por exemplo: Quais processos desconhecidos em execução foram encontrados?
Existe algum processo abrindo alguma comunicação de rede que não é comum? Existe processo em execução com nome randomizado? Existe alguma evidência de uso de ferramentas de hacking ou admin?

4.10.1.2 Questões Mitre: deve relacionar as principais respostas do MITRE framework relacionadas a evidências encontradas.

4.10.1.3 Hipótese: indicativo de comportamento anômalo baseado em hipótese com base em perguntas chave (Inteligência Artificial).

4.10.1.4 Visualização Geral da Investigação:

4.10.1.5 Sumarizada: Deve apresentar um sumário geral da situação, progresso, entidades envolvidas na investigação, investigações similares e os principais indicadores de comprometimento.

4.10.1.6 Gráfica: Apresentação em formato gráfico com os links de relacionamento entre todos os artefatos encontrados. A visualização gráfica deve se moldar, permitindo o drill-down desde o montante total de artefatos descobertos até os achados principais.

4.10.2 Deve ser possível identificar, por meio de cores distintas, os relacionamentos entre entidades externas e entidades internas.

4.10.3 Deve ser possível agrupar os artefatos descobertos e os principais indicios por grupo, para facilitar a visualização.

4.10.4 Deve ser possível filtrar o gráfico dentre as opções: Endereço IP; DNS Lookup; Dispositivo; FQDN; Arquivo; Conexão de Rede; Processo e; Serviço.

4.10.5 Ao interagir com algum dos indícios encontrados, a solução de investigação deverá apresentar um widget na qual deverá apresentar mais detalhes sobre os indicativos, inclusive permitindo a interação por meio de ações, como por exemplo:

4.10.5.1 Capturar uma imagem da máquina;

4.10.5.2 Isolar a máquina da rede e;

4.10.5.3 Buscar um processo executado em outras máquinas monitoradas;

4.10.6 O Widget deverá trazer informações capazes de suplementar a investigação, trazendo informações com mais detalhes.

4.10.7 Guias: deverá presentar um sumário do guia de investigação.

4.10.8 Tabulada: Visão geral sobre os artefatos identificados, com sumário e um detalhamento do mesmo.

4.10.9 Dispositivos: Dispositivos afetados, incluindo nome, versão do sistema operacional, identificador e o status.

4.10.10 Deverá possuir um painel de monitoramento onde a incidência de atividade maliciosa deve ser apresentada.

4.10.11 Para cada artefato malicioso monitorado, deve apresentar:

4.10.12 Painel de ação: Iniciar uma investigação e Excluir do monitoramento.

4.10.13 Painel com detalhes do processo: Modo de detecção; Primeira detecção; Última detecção; Dispositivos afetados; Tempo de vida no ambiente; MD5, SHA-1 e

SHA-256;

4.10.14 Painel de Ação – Dispositivos: Parar um processo; Parar e remover; Quarentenar a estação de trabalho; Painel de Comportamento; Apresentar as Técnicas observadas e compará-las a matriz do Mitre; Apresentar os indicadores suspeitos identificados; Atividade do Processo; Sumário e; Deve permitir comparar o observado com o guia SANS DFIR.

4.10.15 Deve apresentar a interação do processo por:

4.10.15.1 Modo sequencial: Sequência de interações do processo, até o ponto de identificação da atividade suspeita.

4.10.15.2 Modo Temporal: Linha de tempo, até o ponto de identificação da atividade suspeita;

4.10.15.3 Modo tabulado: Detalhamento dos eventos por linhas, até a identificação da atividade suspeita.

4.11 Solução de proteção para dispositivos móveis

4.11.1 A solução de "Proteção para dispositivos móveis", deve proteger a CONTRATANTE contra as ameaças em dispositivos móveis, Android e IOS, incluindo malwares, ameaças de rede, identificação de vulnerabilidades e defesa física dos dispositivos. O objetivo principal desta solução é proteger os usuários móveis, impedindo que ameaças nestes dispositivos possam impactar nos serviços e na rede da CONTRATANTE.

4.11.2 Características Gerais:

4.11.2.1 Deverá ser ofertado como um serviço on premises (local) ou em console baseada em nuvem de forma a garantir suas funcionalidades independente da rede que o dispositivo estiver conectado.

4.11.2.2 A solução deverá possuir console WEB para administração da solução.

4.11.2.3 Possuir dashboard com os principais indicadores da solução, como Distribuição de níveis de risco, dispositivos em não conformidade, total de dispositivos protegidos e incidentes recentes.

4.11.2.4 Apresentar, nos dashboards, uma visão geral dos riscos examinados nos dispositivos móveis, como ameaças de rede, vulnerabilidades e malwares encontrados.

4.11.2.5 Deverá possuir uma apresentação gráfica referente as informações dos dispositivos registrados na solução.

4.11.2.6 Associar o nome do usuário ao nome do dispositivo, o modelo e a versão do sistema operacional, em console gráfica.

4.11.2.7 A console deverá apresentar os principais incidentes gerados, contendo todos os detalhes sobre o mesmo e o dispositivo que gerou o incidente.

4.11.2.8 A solução deverá apresentar um relatório de ações recomendadas, para que com tais dados os administradores da solução possam criar ações para melhorar a segurança dos dispositivos móveis da empresa.

4.11.2.9 A solução deverá ser categorizada como uma solução de MTD (Mobile Threat Defense).

4.11.2.10 Deverá ser compatível com os sistemas operacionais IOS e Android.

4.11.2.11 Deverá integrar-se com as principais tecnologias de MDM ou EMM do mercado, no mínimo com MobileIron, Microsoft Intune e Airwatch.

4.11.2.12 O cliente da solução deverá estar disponível nas lojas oficiais dos fabricantes, sendo Apple Store para IOS e Google Play para Android.

4.11.2.13 Permitir configuração no cliente instalado nos dispositivos móveis para que nenhuma informação e alertas seja visível para o usuário final, através de modo não interativo.

4.11.2.14 Deverá possuir as seguintes características mínimas de proteção: Proteção contra Malwares: Proteção em tempo real contra malwares conhecidos e desconhecidos; Defesa física; Identificação de upgrades do sistema operacional; Identificação de dispositivo com root e; Identificação de configurações de segurança, como tela de bloqueio não habilitada.

4.11.2.15 Deverá ser possível instalar a solução através de integração com solução de MDM/EMM ou através da própria console, utilizando e-mail.

4.11.2.16 Poderá possuir lista branca (whitelist) de apps.

4.11.2.17 Deverá possuir integração com solução de SIEM de mercado.

4.11.2.18 A solução deve apresentar notificações de violações para o usuário final e para os administradores da solução, através de Email e Notificações Push.

4.12 Características do Módulo de Controle de Dispositivos

4.12.1 Deve controlar o uso de dispositivos por parte dos usuários, como por exemplo Mídias Removíveis, Unidades USB, Ipods, Dispositivos Bluetooth, DVDs, e CDS regraváveis;

4.12.2 Deve permitir a configuração dos dispositivos nos modos: Bloqueio ou Somente Leitura.

4.12.3 Deve classificar os dispositivos removíveis em 3 categorias: Gerenciado, Não Gerenciável (Exemplo: Bateria de Notebooks) e Não Gerenciado.

4.12.4 Deve ser capaz de identificar o dispositivo (plug and play) através das seguintes informações: Tipo de BUS; Classe do Dispositivo (Device Class); ID do fabricante (Vendor ID) e; ID do produto (Product ID).

4.12.5 Deve ser capaz de identificar Dispositivos Removíveis através das seguintes informações: Tipo de BUS; Se o sistema de arquivo é passível de escrita; Se o sistema de arquivo é somente leitura; Tipo de Sistema de Arquivo; Nome do Sistema de Arquivo e; Número de Série do Sistema de Arquivo.

4.12.6 Deve ser possível habilitar ou desabilitar uma determinada regra de proteção uma vez que esteja dentro da rede (Exemplo: Quando conectado à rede do órgão libera o uso de pen-drive).

4.13 Características do Módulo de Controle de Aplicações

4.13.1 O módulo de controle de aplicações deve prover a capacidade de visibilidade sobre as aplicações executadas e aplicar o controle de execução imposto pela política.

4.13.2 Deve ser capaz de realizar um inventário nas estações de trabalho protegidas informando todos os executáveis e arquivos de script presentes.

4.13.3 Como resultado do inventário, a solução deve armazenar o nome completo do arquivo, tamanho, checksum, tipo de arquivo, nome da aplicação e versão.

4.13.4 Ao detectar um executável, a solução deverá consultar a Solução de reputação de arquivos e compartilhamento de informações de segurança e esta deverá informar um nível de confidência (Bom, Mau ou Não Classificado).

4.13.5 Caso não seja possível efetuar comunicação com a Solução de reputação de arquivos e compartilhamento de informações de segurança o módulo deve realizar consulta de reputação para o Centro de Inteligência do fabricante.

4.13.6 Deve ser possível criar uma imagem base para a criação de uma política geral.

4.13.7 Capacidade de trabalhar no modo adaptativo, ou seja, adaptando-se à novas aplicações instaladas na máquina.

4.13.8 A solução deverá permitir a realização de varreduras por demandas em máquinas para executar a blindagem de aplicativos.

4.13.9 Para o controle de aplicativos, deve possuir, no mínimo, os seguintes modos de operação:

4.13.9.1 Desabilitado: proteção desativada;

4.13.9.2 Monitoramento: Monitora toda a atividade da Estação de Trabalho;

4.13.9.3 Atualização: a cada execução de aplicativo este é inserido em uma regra ou pacote de autorizações pré-estabelecido.

4.13.10 Deve identificar as aplicações de maneira única através do uso de hash (MD5 ou SHA- 1).

4.13.11 A solução deve suportar as seguintes modalidades de proteção:

4.13.11.1 Application Whitelisting: criação de uma lista de aplicações autorizadas que podem ser executadas no equipamento, onde todas as demais aplicações são impadidas de serem executadas.

4.13.11.2 Application Blocking / Blacklisting: criação de uma lista de aplicações não autorizadas que não podem ser executadas.

4.13.11.3 Memory Protection: monitoração e proteção de aplicativos e componentes críticos do sistema operacional de serem adulterados em tempo de execução, isto é, durante operação e execução em memória.

4.13.12 Solução suporta criação, configuração e manutenção de Whitelist dinamicamente através de definição de regras de confiança.

4.13.13 Em caso de um bloqueio indevido, o usuário poderá submeter o arquivo para revisão do administrador e solicitar a liberação do aplicativo ou arquivo.

4.13.14 Suporta os mecanismos:

4.13.14.1 Application Code Protection: permite que somente os programas em Whitelist (executáveis, binários, DLLs, Scripts, extensões customizadas, entre outros) possam ser executados.

4.13.14.2 Memory Protection: permite proteção para ataques e exploração de vulnerabilidades para os programas em Whitelist.

4.13.15 Suporta criação, configuração e manutenção de políticas, permitindo ou

bloqueando a adesão de Whitelist, através de:

4.13.15.1 Binário: binário específico identificado através de seu nome ou de algorítmo de verificação SHA-1.

4.13.15.2 Trusted Publisher: fornecedor específico, assinado digitalmente por um certificado de segurança.
emitido, para este fornecedor, por uma Autoridade Certificadora (CA - Certificate Authority).

4.13.15.3 Trusted Installer: software instalado por um programa instalador específico, identificações por seu algorítmo de verificação, independentemente de sua origem.

4.13.15.4 Trusted Directories: pasta compartilhada na rede, onde os programas instaladores para aplicações autorizadas e licenciadas são mantidos.

4.13.15.5 Trusted Program / Authorized Updater: programas identificados pelo nome, para adicionar e/ou atualizar aplicações.

4.13.15.6 Trusted Users / Authorized Users: somente usuários selecionados, substituindo a proteção de adulteração, para adicionar e/ou atualizar aplicações.

4.13.15.7 Trusted Time Window / Update Mode: janela de tempo para manutenção de aplicações.

4.13.16 Deve ser capaz de proteger em modo standalone - online ou offline.

4.13.17 Além de possuir um conjunto de regras, deve permitir por parte do administrador que este customize-as de forma a adaptar a necessidade da entidade.

4.13.18 Deve suportar o uso de variáveis de ambiente para a criação de regras e monitoramento (Exemplo: %HOMEPATH%, %HOMEDRIVE%, %USERPROFILE%, %APPDATA%).

4.13.19 Deve suportar variáveis de ambiente em sistemas 64-bits (Exemplo: %PROGRAMFILES (x86)%).

4.13.20 Deve prover, no mínimo, as seguintes técnicas para proteção de memória de forma a prevenir ataques dia zero:

4.13.20.1 Critical Address Space Protection;

4.13.20.2 NX - No eXecute (mp-nx);

4.13.20.3 Virtual Address Space Randomization;

4.13.20.4 Mp-vasr-randomization;

4.13.20.5 Mp-vasr-relocation;

4.13.20.6 Mp-vasr-reloc;

4.13.20.7 Forced DLL Relocation.

4.13.21 Deve possibilitar o controle e bloqueio da instalação de Active-X nas estações de trabalho.

4.13.22 Permitir o bloqueio de aplicações e os processos que a aplicação interage.

4.13.23 Permitir monitoração de aplicações onde se pode determinar quais processos poderão ser executados ou não.

4.13.24 Permitir monitoração de Hooking de aplicações onde se podem determinar quais processos pode ser executado ou não.

4.14 Características do Módulo de Gerenciamento

4.14.1 Deve ser disponibilizado em solução local (on-premise) ou em nuvem;

4.14.2 Solução de gerenciamento on-premise:

4.14.2.1 Deve suportar a instalação nos seguintes sistemas operacionais:Windows Server 2019; Windows Server 2016; Windows Server 2012 Release 2; Windows Server 2012;

4.14.2.2 A arquitetura dos Sistemas Operacionais deve ser 64-bits;

4.14.2.3 Deve suportar a instalação em Cluster Microsoft;

4.14.2.4 Deve suportar Ipv4 e Ipv6.

4.14.3 Deve suportar a virtualização do sistema operacional com base nos seguintes hypervisors:

4.14.3.1 Vmware ESX;

4.14.3.2 Citrix Xen Server;

4.14.3.3 Microsoft Hyper-V.

4.14.4 Deve possuir suporte a base de dados:

4.14.4.1 SQL Server 2012 ou superior;

4.14.4.2 Não serão aceitas soluções que usam SQL Express ou Base de dados embutidas;

4.14.5 Deve ser possível segregar a instalação da solução em:

4.14.5.1 Servidor Console Central;

4.14.5.2 Servidor Base de Dados;

4.14.5.3 Servidor de Interação com os Agentes;

4.14.5.4 Agentes Distribuidores de Vacina.

4.14.6 Deve suportar o uso do SQL Server em ambientes SAN.

4.14.7 Permitir a instalação dos Módulos da Solução a partir de um único servidor.

4.14.8 A console de gerência deve ser acessada via WEB.

4.14.9 Deve possuir compatibilidade com os seguintes browsers:

4.14.9.1 Google Chrome;

4.14.9.2 Firefox;

4.14.9.3 Internet Explorer 7 ou superior;

4.14.9.4 Safari 6.0 ou superior.

4.14.10 Permitir a alteração das configurações dos Módulos da Solução nos clientes de maneira remota.

4.14.11 Permitir a atualização incremental da lista de definições de vírus nos clientes, a partir de um único ponto da rede local.

4.14.12 Visualização das características básicas de hardware das máquinas.

4.14.13 Integração e Importação automática da estrutura de domínios do Active

Directory já existentes na rede local.

4.14.14 Permitir a criação de tarefas de atualização, verificação de vírus e upgrades em períodos de tempo pré-determinados, na inicialização do Sistema Operacional ou no Logon na rede.

4.14.15 Permitir o armazenamento das informações coletadas nos clientes em um banco de dados centralizado.

4.14.16 Permitir diferentes níveis de administração do servidor, de maneira independente do login da rede.

4.14.17 Suporte a múltiplos usuários, com diferentes níveis de acesso e permissões aos produtos gerenciados.

4.14.18 Criação de grupos de máquinas baseadas em regras definidas em função do número IP do cliente.

4.14.19 Permitir a criação de grupos virtuais através de marcadores.

4.14.20 Permitir aplicar as marcações nos sistemas por vários critérios incluindo: produtos instalados, versão de sistema operacional, quantidade de memória, dentre outros.

4.14.21 Forçar a configuração determinada no servidor para os clientes.

4.14.22 Caso o cliente altere a configuração, deverá ser possível retornar ao padrão estabelecido no servidor, quando for verificada pelo agente.

4.14.23 A comunicação entre as máquinas clientes e o servidor de gerenciamento deve ser segura usando protocolo de autenticação HTTPS.

4.14.24 Forçar a instalação dos Módulos da Solução nos clientes.

4.14.25 Caso o cliente desinstale os Módulos da Solução, os mesmos deverão ser reinstalados, quando o agente verificar o ocorrido.

4.14.26 Quanto ao módulo de gestão deverá ser realizada a gestão, no mínimo, a solução para proteção de estações de trabalho e servidores,

4.14.27 O módulo de gestão deverá apresentar relatórios e dashboards consolidados visando a solução para proteção de estações de trabalho e servidores.

4.14.28 Deve ser possível realizar a customização dos relatórios gráficos gerados;

4.14.29 Exportação dos relatórios para os seguintes formatos: HTML, CSV, PDF, XML.

4.14.30 Geração de relatórios que contenham as seguintes informações:

4.14.30.1 Máquinas com a lista de definições de vírus desatualizada;

4.14.30.2 Qual a versão do software (inclusive versão gerenciada pela nuvem) instalado em cada máquina;

4.14.30.3 Os vírus que mais foram detectados;

4.14.30.4 As máquinas que mais sofreram infecções em um determinado período;

4.14.30.5 Os usuários que mais sofreram infecções em um determinado período;

4.14.31 A solução de gestão deve possuir dashboards no gerenciamento da solução.

4.14.32 Estes dashboards devem conter no mínimo todos os seguintes relatórios de

fácil visualização:

4.14.32.1 Relatório dos últimos 30 dias da detecção de códigos maliciosos;

4.14.32.2 Top 10 Computadores com Infecções e;

4.14.32.3 Top 10 Computadores com Sites bloqueados pela política.

4.14.33 Gerenciar a atualização do antivírus em computadores portáteis (notebooks), automaticamente, mediante conexão em rede local ou remota (VPN).

4.14.34 Suportar o uso de múltiplos repositórios para atualização de produtos e arquivo de vacina com replicação seletiva.

4.14.35 Ter a capacidade de gerar registros/logs para auditoria.

4.14.36 A solução de gerenciamento deve ter a capacidade de atribuir etiquetas as máquinas, facilitando assim a distribuição automática dentro dos grupos hierárquicos na estrutura de gerenciamento.

4.14.37 A solução de gerenciamento deve permitir acesso a sua console via web.

4.15 Solução de proteção para ambientes virtualizados

Características Gerais

4.15.1 Deve ser uma solução específica e otimizada para funcionar e interoperar com ambiente virtual, sem a necessidade de instalação de módulo antivírus para cada servidor virtualizado.

4.15.2 Deve eliminar o uso de agentes para a tecnologia antivírus.

Deve suportar a infraestrutura de virtualização VMWare, conforme descrito abaixo:

4.15.2.1 VMware NSX Manager 6.3.3 ou superior;

4.15.2.2 VMware ESXi 6.0 U2 ou superior;

4.15.2.3 VMware vCenter 6.0 U2 ou superior.

4.15.3 A solução deverá ser capaz de ser implantada em ambientes VMWare mesmo sem a existência das APIs informadas no item anterior.

4.15.4 Para ambientes sem as APIs VMWare, o ambiente suportado deverá ser:

4.15.4.1 VMware ESXi 5.0 ou superiores;

4.15.4.2 Deve integrar a console de gerência proposta, através de conector nativo, com o VMWare vSphere.

4.15.5 A varredura de arquivos deverá ser realizada por um servidor virtual blindado e instalado de maneira centralizada.

4.15.6 A solução deverá possuir capacidade de proteger máquinas “guest” para ambientes não Vmware, incluindo:

4.15.6.1 Citrix Xen Server 6 ou superior;

4.15.6.2 Microsoft Windows Server 2012 Hyper-V;

4.15.6.3 Microsoft Windows Server 2012 R2 Hyper-V;

4.15.6.4 Microsoft Windows Server 2016 Hyper-V.

4.16 Características do Software

4.16.1 Toda a operação relacionada aos procedimentos de antivírus deverá ser realizada por um servidor virtual blindado e centralizado. Dentre as funcionalidades este servidor deverá:

4.16.1.1 Receber a configuração de proteção;

4.16.1.2 Atualizar assinaturas de proteção;

4.16.1.3 Efetuar operação de varredura (Scan).

4.16.2 Deve suportar análise no momento que um arquivo é acessado.

4.16.3 Deverá suportar análise de todos os arquivos em uma máquina virtual (scan sob demanda) permitindo agendar a frequência das verificações.

4.16.4 Deve possuir agendamento inteligente das varreduras (scan) de forma a não causar impacto no Hypervisor.

4.16.5 Deve suportar os seguintes sistemas em máquinas "Guest" de maneira Agentless: Red Hat Enterprise Linux 7 – 64 bits; Suse Linux Enterprise Server 12 – 64 bits; Ubuntu 14.04 LTS – 64 bits; Windows 2012; Windows 2012 R2; Windows 2016; Windows 8; Windows 8.1 e; Windows 10.

4.16.6 Através da integração com o VMWare vSphere deve ser possível descobrir e importar as instâncias de máquinas virtuais paradas ou em execução.

4.16.7 A solução deverá contar com um cache que permita otimizar os recursos evitando analisar arquivo que já tenham sido analisados anteriormente e não tenha sofrido alterações.

4.16.8 O cache deve ser tanto local (guest machine) quanto centralizado em cada analisador (scanner).

4.16.9 O tamanho do cache deve ser configurável.

4.16.10 Deve ser possível configurar a quantidade de análises simultâneas que devem ser executadas em cada analisador.

4.16.11 Deve ser possível configurar o tipo de arquivo a ser analisado.

4.16.12 Deve manter uma quarentena local em cada servidor ou em um compartilhamento remoto em casa de detecção de ameaça.

4.16.13 Como resultado da ação deve ser possível manter o arquivo ou eliminá-lo.

4.16.14 Deve ser capaz de analisar unidades de rede.

4.16.15 Deve suportar vMotion.

4.16.16 Deve ser possível criar análises específicas com base em: Grupos, Resource Pools e Máquinas Virtuais específicas.

4.16.17 Toda e qualquer ameaça encontrada deve ser informada na console de gestão centralizada.

4.17 Características de Arquitetura

4.17.1 A solução deve possuir gestão única por meio da mesma console da solução para proteção de estações de trabalho e servidores.

4.17.2 Deverá permitir a instalação e criação de analisadores em alta disponibilidade.

4.17.3 Deverá suportar analisadores em alta disponibilidade com possibilidade de instalá-lo fora do cluster existente.

4.17.4 Não deve requerer reinício do Hypervisor durante a instalação da solução.

4.17.5 O analisador deve possuir comunicação com o Centro de Inteligência do

fabricante para classificar arquivos suspeitos.

4.17.6 Deve permitir a adição/remoção de servidores centrais de análise de maneira automática.

4.17.7 Para o caso de instalação em múltiplos Hypervisors, o instalador deve prover um meio automatizado de execução.

4.18 Características de Gestão

4.18.1 A console de gestão deve permitir designar máquinas virtuais para cada analisador.

4.18.2 Deverá permitir a configuração centralizada das análises contra artefatos maliciosos.

4.18.3 Deve ser possível criar uma política por máquina virtual.

4.18.4 A solução deve permitir o download de atualizações de vacina e engines de maneira periódica e automática e aplicá-las aos componentes da solução.

4.18.5 Deve permitir configurar, de maneira centralizada, ações de resposta a uma ameaça existente no ambiente.

4.18.6 Deve possibilitar a criação de alertas para notificar a incidência de artefatos maliciosos nos servidores.

4.18.7 A gerência deve possuir dashboards específicos para a solução proposta de maneira nativa.

4.18.8 Deve possuir logs que indiquem o indicativo de atividade maliciosa no ambiente gerenciado.

4.18.9 Deve possuir relatórios nativos para a solução proposta, dentre eles:

4.18.9.1 Top 10 – Extensões de arquivos por servidor centralizado de análise;

4.18.9.2 Top 10 – Arquivos analisados por servidor centralizado de análise;

4.18.9.3 Top 10 – Ameaças detectadas;

4.18.9.4 Top 10 – Processos analisados;

4.18.9.5 Quantidade de clientes conectados em cada servidor centralizado de análise;

4.18.9.6 Servidor Centralizado de Análise com alto tempo de processamento – Últimos 7 dias.

4.18.10 Deve possibilitar monitorar a saúde dos servidores centralizados de análise pela console de gerência.

4.18.11 Deve possuir capacidade de customizar as buscas em banco de dados da própria solução para montar relatórios customizados, com no mínimo os seguintes relatórios prontos:

4.18.11.1 Versão de assinatura;

4.18.11.2 Nome de ameaças detectadas por semana;

4.18.11.3 Ameaças detectadas nas últimas 24 horas;

4.18.11.4 Contagem de ameaças por severidade;

4.18.11.5 Máquinas virtuais com Ameaças detectadas por semana;

4.18.11.6 Serviço de implantação e migração da solução para proteção de

endpoints e servidores.

CLÁUSULA 5

DO LOCAL, PRAZO DE ENTREGA E CONDIÇÕES DE RECEBIMENTO DO OBJETO

5.1 As licenças, através do fornecimento das respectivas mídias ópticas ou dos procedimentos para download no site do fabricante, deverão ser entregues e instaladas nos computadores do **Prédio-sede da Junta Comercial do Estado do Pará**, localizado no endereço: **Avenida Magalhães Barata, 1234 – São Brás – Belém-Pará, CEP: 66.060-281, Telefone: (091) 3217-5864, no horário de 08:00 às 13:00 horas**, em dias de expediente, de segunda a sexta-feira, mediante o acompanhamento e as orientações da equipe técnica da Coordenação do Núcleo de Recursos Tecnológicos (NRT).

5.2 O prazo para entrega das licenças será de até 15 (quinze) dias úteis, contados do recebimento da nota de empenho.

5.3 Dentro do prazo de entrega da solução, a contratada deverá prestar os serviços de instalação, configuração e ativação da console de gerenciamento e das licenças, no computador servidor, nos computadores das estações de trabalho e notebooks, devendo realizar o treinamento para utilização dos respectivos softwares.

5.4 As licenças, por subscrição, de uso do software antivírus corporativo deverão ser fornecidas em sua totalidade e de acordo com as especificações técnicas presentes neste instrumento, devendo estarem em nome da Junta Comercial do Estado do Pará, pelo **período de 48 (quarenta e oito)** meses, sendo admitidas somente licenças originais e legalizadas.

5.5 Todos os componentes que fazem parte da solução de segurança para os computadores deverão ser fornecidos pelo mesmo fabricante, não sendo aceitas composições de produtos de fabricantes diferentes.

5.6 No caso de fornecimento de mídias ópticas, as mesmas deverão ser novas e entregues acondicionadas, adequadamente, em embalagens lacradas, de forma a permitir a completa segurança durante o transporte.

5.7 Todos os códigos e as senhas de ativação e/ou acesso necessários para download e instalação das licenças deverão serão enviados para o Núcleo de Recursos Tecnológicos (NRT) da JUCEPA, por meio do e-mail nrt@jucepa.pa.gov.br.

5.8 A contratada deverá fornecer no ato da entrega a versão mais atual do software comercializada no mercado e em idioma português (Brasil), inclusive os seus manuais e documentação.

5.9 No ato da entrega, a contratada deverá apresentar documento que comprove o direito de uso das licenças por parte da JUCEPA, de acordo com as exigências

específicas do fabricante.

5.10 Para entrega e execução dos serviços de implementação das licenças deverá ser realizado prévio agendamento de data e horário junto à Coordenação do NRT desta JUCEPA.

5.11 O objeto deste contrato, será recebido:

5.11.1 Provisoriamente, mediante a emissão de Termo de Recebimento Provisório, no prazo de até 05 (cinco) dias úteis após a realização da instalação, configuração e ativação, representada pela conferência da quantidade das licenças aplicadas e a conformidade com as informações da proposta comercial, acompanhado da(s) assinatura(s) do(s) servidor(es) designado(s) para esse fim, em canhoto de fatura/nota fiscal.

5.11.1.1 Na hipótese de ser verificada impropriedade de alguma licença de software antívirus no ato da instalação, a mesma será rejeitada, no todo ou em parte, a critério da fiscalização responsável pelo seu recebimento, sendo a empresa contratada notificada a proceder à substituição no prazo máximo de 7 (sete) dias úteis após a verificação, a contar da notificação da JUCEPA, sem prejuízo da aplicação de penalidades.

5.11.1.2 No caso de correção dos serviços (instalação/configuração/ativação) e/ou substituição de software(s), será feita uma nova averiguação, considerando o prazo de 5 (cinco) dias úteis.

5.11.2 Definitivamente, mediante atesto na nota fiscal/fatura e emissão de Termo de Recebimento Definitivo correspondente, no prazo de até 5 (cinco) dias úteis, contados do recebimento do Termo de Recebimento Provisório emitido pela Junta Comercial do Estado do Pará.

5.11.3 O recebimento provisório ou definitivo das licenças e dos serviços para sua implementação não exclui a responsabilidade da empresa pelos prejuízos decorrentes da incorreta execução do contrato.

CLÁUSULA 6

DA VIGÊNCIA DAS LICENÇAS E DA GARANTIA DE ATUALIZAÇÃO DE VERSÃO

6.1 As licenças, por subscrição, de uso de software antivírus e garantia de atualização de versão deverão ter duração de 48 (quarenta e oito) meses a contar da ativação.

6.2 A Contratada deverá prover toda e qualquer atualização ao produto durante a vigência do contrato.

6.3 Durante o prazo de garantia de atualização de versão, fará parte o fornecimento de qualquer evolução do produto, incluindo patchs, bugfixes,

correções, updates, service packs e novas versões lançadas pelo fabricante, sem quaisquer ônus adicionais à JUCEPA durante a vigência do contrato.

6.4 Deverão ser enviadas à JUCEPA todas as atualizações de versão, tanto da base de dados do antivírus quanto dos softwares, devidamente acompanhadas das instruções para sua instalação, configuração e ativação.

6.5 As atualizações deverão ser disponibilizadas através do site do fabricante na Internet ou através do próprio software de gerenciamento da solução.

6.6 A contratada deverá fornecer no ato da entrega o certificado de registro do direito de uso e de atualização das licenças pelo período de 48 (quarenta e oito) meses, em nome da JUCEPA.

6.7 A aplicação das atualizações e qualquer outra intervenção no ambiente da solução deverão ser comunicadas e negociadas previamente, mediante acordo com a equipe técnica do NRT/JUCEPA, para que sejam definidas a data e o horário de sua realização.

CLÁUSULA 7

DO TREINAMENTO E SUPORTE TÉCNICO ESPECIALIZADO, INCLUINDO MANUTENÇÃO E ASSISTÊNCIA TÉCNICA

7.1 O treinamento deverá ser realizado pela empresa contratada, na modalidade presencial, no **prédio-sede da JUCEPA**, com carga horária suficiente para apresentar a utilização, configuração e boas práticas do software de antivírus a ser fornecido.

7.2 Todo o material do treinamento deverá ser em português (Brasil), incluindo apostilas em formato digital e arquivos, os quais terão de ser fornecidos pela contratada.

7.3 O serviço de suporte especializado deverá englobar todos os elementos de software da solução, incluindo a prestação de serviços de manutenção e assistência técnica, compreendendo a substituição de módulos, componentes, acessórios, mídias ópticas e aplicativos que apresentarem defeito durante este período, sem qualquer ônus adicional para a JUCEPA, obrigando-se a contratada a manter todo o ambiente de antivírus corporativo permanentemente em perfeitas condições de funcionamento para a finalidade a que se destina, na forma estabelecida neste contrato.

7.4 Os serviços de manutenção do software antivírus deverão prover suporte aos componentes (licenças de uso); orientações sobre uso, configuração e instalação; orientações para identificação de causas de falhas de software; fornecimento de informações conhecidas sobre defeitos conhecidos e envio de informações sobre falhas não conhecidas para tratamento do fabricante do software.

7.5 Durante a vigência da licença, a empresa contratada deverá realizar no mínimo,

01 (uma) visita técnica por semestre para realização de manutenção preventiva, incluindo: mão de obra e deslocamento, atualizações dos softwares, testes, medição e fornecimento de relatório.

7.6 O serviço de suporte técnico especializado deverá ser realizado das seguintes formas:

a) Suporte remoto: serviço de atendimento aos chamados técnicos executados por meio telefônico (discagem direta gratuita 0800) ou contato telefônico efetuado pela contratada, web e e-mail, ferramentas de acesso remoto monitorado, via central de help desk, que possibilite a abertura de chamados técnicos e ocorrências relativas à solução, assim como o acompanhamento online da resolução do chamado.

b) Suporte on-site: quando necessários devem ser realizados em Belém-Pa (prédio-sede da JUCEPA) por corpo técnico especializado da própria fabricante, parceiro licenciado ou da própria contratada com credenciamento da fabricante.

7.7 A contratada deverá prestar o serviço de suporte técnico durante 48 (quarenta e oito) meses, na modalidade 24x7 (vinte quatro horas por dia e sete dias por semana), disponibilizando central de atendimento (Idioma Português do Brasil) para abertura de chamados.

7.8 Os chamados serão abertos pela equipe técnica da JUCEPA e somente serão encerrados após o restabelecimento do serviço por completo quando apresentar condições normais de operação e com autorização para o encerramento pela Contratante.

7.9 Em todo atendimento técnico solicitado deve ser fornecido o número do chamado na sua abertura, o responsável pela abertura, o nome do atendente e os motivos ou problemas referentes ao chamado.

7.10 A contratada, no momento da assinatura do contrato, deverá fornecer os meios de comunicação (contato telefônico, endereço de site, e-mail etc.) para abertura de chamados.

7.11 Todos os chamados, inclusive os que podem resultar em manutenção de natureza corretiva, bem como o fluxo de resolução de problemas, deverão ser documentados. Esta documentação, bem como outras geradas em processos de atendimento, auditorias, manutenção ou configurações, deverá ser entregue à JUCEPA através de relatórios (impressos e/ou em mídia digital) mediante solicitação.

7.12 O atendimento de suporte on-site, quando necessário, será solicitado via telefone, e-mail, site na internet etc. e deverá contemplar os problemas que não foram possíveis de ser solucionados através do suporte remoto.

7.13 Ao final de cada visita, o técnico da contratada deverá entregar à equipe técnica da JUCEPA um relatório circunstanciado do atendimento mencionando: data e hora de abertura do chamado técnico, número do chamado técnico, data e hora do atendimento, o nome do responsável pela abertura, o nome do atendente, os problemas verificados, as providências adotadas, as recomendações e orientações técnicas.

7.14 A contratada deverá disponibilizar mensalmente um relatório consolidado das ordens de serviços geradas.

7.15 O relatório deverá ser enviado via e-mail ou disponibilizado via página web da contratada.

7.16 Quanto ao prazo para solução do problema após a abertura de chamado:

a) Para solução dos problemas em que o software se encontrar inoperante, estando completamente indisponível para qualquer tipo de operação, o tempo de solução deverá ser de até 8 h (oito horas), podendo seron-site, a depender da solicitação por esta JUCEPA.

b) No caso de perda parcial de uma função crítica da solução, porém que apresente uma solução temporária que permita a continuidade do serviço, o tempo de solução deverá ser de até 16 h (dezesseis horas).

c) Quando para consultas técnicas, perda parcial de funções não críticas, sugestão de configurações ou documentações, o prazo para solução deverá ser de até 36 h (trinta e seis horas).

7.17 Ainda poderão ser executadas as seguintes tarefas em relação à prestação de suporte: Resolução de dúvidas sobre as licenças; Discussão de melhorias na configuração; Resolução de pequenos problemas e ajustes na solução; Solicitação de relatórios gerenciais contendo informações sobre incidentes e ações recomendadas para tratar o incidente; Solicitação de análise de segurança em ativos gerenciados pela solução.

CLÁUSULA 8

DA GARANTIA CONTRA DEFEITOS DE EXECUÇÃO DOS SERVIÇOS

8.1 O período de garantia contra defeitos de execução dos serviços, complementar à garantia legal prevista no código de defesa do consumidor, deverá ser de, no mínimo, 03 (três) meses, ou pelo prazo fornecido pelo fabricante, se superior, abrangendo a substituição da(s) licença(s) que apresentar(em) defeito(s) decorrente(s) do processo de fabricação.

8.2 O prazo de garantia será contado a partir da data da emissão do Termo de Recebimento Definitivo.

8.3 A justificativa para a estipulação do prazo de garantia citado acima tem como principal finalidade, assegurar a qualidade das licenças de software antivírus corporativo a serem adquiridas, bem como as suas possíveis substituições e o refazimento do(s) serviço(s) de instalação, configuração e/ou ativação das licenças que apresentem eventuais defeitos detectados na utilização e/ou na instauração.

CLÁUSULA 9

Preço

O valor total da despesa advinda da aquisição é de R$ 49.000,00 (quarenta e nove mil reais).

CLÁUSULA 10

Dotação orçamentária

As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria do orçamento do Estado do Pará, para o exercício de **2023**, na classificação abaixo:

Gestão/Unidade	72000/720201
Unidade Orçamentária	72201
Fonte	01501000061/02501000061 Rec da Adm Indireta (próprios)
Programa de Trabalho	23.126.15088238 Gestão de Tecnologia da Informação e Comunicação
Elemento de Despesa	339040.00 Serv de Tecno da Infor e Comun - PJ
Plano Interno	4120008238c

CLÁUSULA 11

Reajuste

11.1 O contrato não sofrerá reajuste.

CLÁUSULA 12

Pagamento

12.1 O pagamento será realizado em até 30 dias corridos, a contar do recebimento da nota fiscal ou fatura atestada pelo fiscal do contrato. A contratada deverá enviar junto à nota fiscal ou fatura, os comprovantes de regularidade fiscal (municipal, estadual e federal), trabalhista e previdenciária

12.2 O pagamento será efetuado por ordem bancária para conta de titularidade da CONTRATADA, cujos dados são:

BANCO	**077 (Inter)**
CONTA	14346428-0
AGÊNCIA	0001

12.3 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 adote as medidas para saneamento das pendências.

12.4 Na hipótese do item 12.3, o prazo para pagamento começará a correr depois da comprovação da regularização da pendência, sem ônus à CONTRATANTE.

12.5 A data do efetivo pagamento será considerada aquela que constar da ordem bancária emitida para quitação da nota fiscal ou fatura.

12.6 A regularidade fiscal da CONTRATADA deve ser verificada pela CONTRATANTE por ocasião do pagamento por meio de consulta ao Sistema de Cadastramento Unificado de Fornecedores (SICAF) ou, na impossibilidade de acesso a ele, devem ser consultados sítios eletrônicos oficiais ou, ainda, ser solicitada a documentação física listada no art. 68 da Lei Federal nº 14.133/21.

12.7 A constatação de irregularidade fiscal da CONTRATADA não impede o pagamento do que foi executado, mas constitui falta contratual, a ser sancionada em procedimento de inexecução contratual.

12.8 Antes da instauração do procedimento de inexecução contratual a que faz menção o item 12.7, a CONTRATADA deve ser notificado para regularizar a pendência no prazo de 5 dias úteis. Não sendo regularizada, deve-se instaurar o procedimento de inexecução contratual, ofertando contraditório e ampla defesa à CONTRATADA.

12.9 A instauração do procedimento de inexecução contratual não impede o pagamento dos bens que já foram entregues.

12.10 Diante da gravidade do caso concreto e para proteger o Erário e o interesse público, a autoridade competente pode decidir pela suspensão do contrato, ocasião em que somente serão pagos os bens já entregues.

12.11 Caso ao final do procedimento a que faz menção a parte final do item 12.8 a autoridade decida pela rescisão contratual, o pagamento será sustado automaticamente.

12.12 A inadimplência do CONTRATADA junto ao SICAF é causa de rescisão contratual, exceto se a autoridade máxima da CONTRATANTE justificar a necessidade de manutenção do contrato por motivo de economicidade, segurança estadual ou outro de interesse público de alta relevância.

12.13 A CONTRATANTE efetuará a retenção tributária prevista na legislação aplicável por ocasião do pagamento.

12.14 A CONTRATADA optante do Simples Nacional não sofrerá retenção tributária em relação aos impostos e contribuições abrangidos por aquele regime, mas o pagamento ficará condicionado à comprovação, por documento oficial, de que a CONTRATADA é beneficiário do tratamento tributário previsto na Lei Complementar Federal nº 123/06.

CLÁUSULA 13

Garantia de cumprimento contratual

13.1 Não há exigência de prestação de garantia de cumprimento deste contrato.

CLÁUSULA 14

Obrigações das partes

As PARTES tem a obrigação de:

Contratante	Contratada
a. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com este contrato, Termo de	**a.** Entregar o objeto no prazo constante no contrato, acompanhado do manual do usuário com uma versão em português e da relação da rede de assistência técnica autorizada.

Referência e anexos.	
b. Receber o objeto no prazo e condições estabelecidas no contrato.	**b.** Aceitar acréscimos ou supressões unilaterais impostos pela CONTRATANTE de até 25% do valor atualizado do contrato, nas mesmas condições pactuadas inicialmente.
c. Notificar a CONTRATADA sobre vícios, defeitos ou incorreções verificadas no objeto fornecido para que ele seja substituído, reparado ou corrigido às suas expensas.	**c.** Responsabilizar-se pelos vícios e danos do objeto, nos termos dos arts. 12, 13 e 17 a 27, da Lei Federal nº 8.078/90.
d. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações da CONTRATADA.	**d.** Comunicar à CONTRATANTE, no prazo de até 24 horas antes da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação.
e. Efetuar o pagamento do objeto fornecido no prazo, forma e condições aqui estabelecidos.	**e.** Atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior e prestar esclarecimentos ou informações por eles solicitados.
f. Aplicar à CONTRATADA as sanções decorrentes da inexecução total ou parcial do contrato.	**f.** No prazo fixado pelo fiscal do contrato, reparar, corrigir, remover, reconstruir ou substituir às suas expensas os bens nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução contratual ou dos materiais empregados.
g. Decidir sobre as solicitações e reclamações relacionadas à execução do contrato, ressalvados os requerimentos meramente protelatórios, manifestamente impertinentes ou de nenhum interesse à boa execução do ajuste.	**g.** Responsabilizar-se pelos vícios e danos decorrentes do cumprimento deste contrato e de todo dano causado à CONTRATANTE ou a terceiros, cuja responsabilidade não será reduzida pela fiscalização ou acompanhamento da execução contratual pela CONTRATANTE, o qual ficará autorizado a descontar o valor dos danos sofridos dos pagamentos devidos ou da garantia.
	h. Na hipótese do item 12.6, parte final, quando solicitado a CONTRATADA deverá entregar à CONTRATANTE os seguintes documentos: 1. Prova de regularidade relativa à Seguridade Social. 2. Certidão conjunta relativa aos tributos federais e à Dívida Ativa da União. 3. Certidões que comprovem a regularidade perante a Fazenda Estadual ou Distrital da sede da CONTRATADA. 4. Certidão de Regularidade do FGTS. 5. Certidão Negativa de Débitos Trabalhistas. 6. Nota fiscal atestada pelo fiscal do contrato.

i. Responsabilizar-se pelo cumprimento das obrigações previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade à CONTRATANTE.
j. Comunicar ao fiscal do contrato, no prazo de 24 horas, qualquer ocorrência anormal que se verifique no local da execução do objeto contratual.
k. Manter durante a vigência do contrato todas as condições exigidas para habilitação na licitação ou para qualificação, na contratação direta.
l. Cumprir durante todo o período de execução do contrato a reserva de cargos para pessoa com deficiência, reabilitado da Previdência Social, aprendiz e outras reservas de cargos previstas na legislação.
m. Comprovar o cumprimento da alínea acima no prazo fixado pelo fiscal do contrato, indicando os empregados que preencheram as referidas vagas.
n. Arcar com o ônus decorrente de eventual equívoco no dimensionamento do quantitativo de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos do art. 124, II, d, da Lei Federal nº 14.133/21.
o. Cumprir as normas de segurança da CONTRATANTE, além da legislação vigente em âmbito federal, estadual e municipal.

CLÁUSULA 15

Responsabilidade por danos

15.1 A responsabilidade pelos danos causados por ato da CONTRATADA, de seus empregados, prepostos ou subordinado, é exclusivamente do CONTRATADA.

15.2 A responsabilidade pelos compromissos assumidos pela CONTRATADA com

terceiros é exclusivamente sua.

15.3 A CONTRATANTE não responderá pelos compromissos assumidos pela CONTRATADA com terceiros, ainda que vinculados à execução deste contrato, ou por qualquer dano causado por ato da CONTRATADA, de seus empregados, prepostos ou subordinados.

CLÁUSULA 16

Infrações e sanções administrativas

16.1 Constituem infrações administrativas da CONTRATADA a serem punidas com as seguintes sanções:

Infração	Penalidade
	Advertência*
a. Dar causa à inexecução parcial do contrato.	* Exceto quando se justificar a imposição de penalidade mais grave, ocasião em que poderá ser aplicada a sanção de "*Impedimento de licitar e contratar*".
b. Dar causa à inexecução parcial do contrato que cause grave dano à CONTRATANTE ou ao funcionamento dos serviços públicos ou ao interesse coletivo. **c.** Dar causa à inexecução total do contrato. **d.** Deixar de entregar a documentação exigida para o certame. **e.** Deixar de manter sua proposta, salvo em decorrência de fato superveniente devidamente justificado. **f.** Ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado.	**Impedimento de licitar e contratar*** * Exceto quando se justificar a imposição de penalidade mais grave, ocasião em que poderá ser aplicada a sanção de "*Declaração de inidoneidade para licitar e contratar*".

g. Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a dispensa eletrônica ou execução do contrato.	**Declaração de inidoneidade para licitar e contratar**
h. Fraudar a contratação ou praticar ato fraudulento na execução do contrato.	
i. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza.	
j. Praticar atos ilícitos com vistas a frustrar os objetivos do certame.	
k. Praticar ato lesivo previsto no art. 5º da Lei Federal nº 12.846/13.	

16.2 O atraso superior a 30 **dias corridos** autoriza a rescisão do contrato por seu descumprimento, nos termos do art. 137, I, da Lei Federal n° 14.133/21.

16.3 A aplicação das sanções previstas neste contrato *não exclui* a obrigação de reparação integral do dano causado à CONTRATANTE.

16.4 As sanções podem ser *cumuladas* com as seguintes multas:

Multa	
Moratória	***Compensatória***
a. **0,5%** sobre o valor da parcela inadimplida por dia de atraso injustificado até o limite de **30 dias corridos**.	**0,5%** sobre o valor total do contrato, no caso de inexecução total do seu objeto.
b. 0,5**%** sobre o valor total do contrato por dia de atraso injustificado até o limite de 45 **dias corridos** pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia.	

16.5 Antes da aplicação das sanções, A CONTRATADA será notificada para apresentar defesa no prazo de **15 dias úteis**, contado de sua intimação.

16.6 Se a multa aplicada e as indenizações cabíveis forem superiores ao valor devido à CONTRATADA, além da perda deste valor, a diferença será descontada da garantia prestada e/ou será cobrada judicialmente.

16.7 Antes do ajuizamento da cobrança, a multa poderá ser recolhida administrativamente em até **15 dias úteis**, a contar do trânsito em julgado da decisão administrativa.

16.8 A aplicação das sanções será precedida de processo administrativo em que seja assegurado o contraditório e a ampla defesa à CONTRATADA, observando o *rito especial* previsto no art. 158 da Lei Federal nº 14.133/21 para as penalidades de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar.

16.9 A aplicação das sanções deve observar:

a. A natureza e gravidade da infração.

b. As peculiaridades do caso.

c. As circunstâncias agravantes e/ou atenuantes.

d. Os danos causados à CONTRATANTE.

e. A implantação ou aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

16.10 As infrações administrativas tipificadas como atos lesivos na Lei Federal nº 12.846/13 serão apuradas e julgadas em conjunto com as infrações previstas neste contrato, nos mesmos autos.

16.11 A personalidade jurídica da CONTRATADA poderá ser desconsiderada quando for utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste contrato ou para provocar confusão patrimonial e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com a CONTRATADA, observados o contraditório, ampla defesa e a obrigatoriedade de análise jurídica prévia.

16.12 No prazo de **15 dias úteis**, a contar da data de aplicação da sanção, à CONTRATANTE informará e manterá atualizados os dados relativos às sanções aplicadas por ela, para publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e no Cadastro Nacional de Empresas Punidas (CNEP), instituídos no âmbito do Poder Executivo Federal.

16.13 As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação, na forma do art. 163 da Lei Federal nº 14.133/21.

CLÁUSULA 17

Alterações do contrato

17.1 As alterações contratuais serão disciplinadas pelo art. 124 e seguintes da Lei Federal nº 14.133/21.

17.2 Caso haja interesse público, a CONTRATANTE pode alterar unilateralmente o contrato para impor acréscimos ou supressões de até **25%** do valor atualizado do contrato, mantidas as mesmas condições pactuadas inicialmente.

17.3 As PARTES podem acordar suprimir o objeto do contrato em percentual superior a 25% do valor inicial atualizado do contrato.

17.4 Os acréscimos ou supressões não podem transfigurar o objeto da contratação.

17.5 Registros que não caracterizem alteração do contrato podem ser realizados por *simples apostila*, dispensada a celebração de termo aditivo, conforme art. 136 da Lei Federal nº 14.133/21.

CLÁUSULA 18

Extinção do contrato

18.1 O contrato se extingue quando todas as obrigações de ambas as PARTES forem cumpridas.

18.2 Se as obrigações não forem cumpridas no prazo estipulado, a vigência ficará prorrogada até a conclusão do objeto, caso em que a CONTRATANTE deverá providenciar a readequação do cronograma fixado para cumprimento do contrato.

18.3 Se a não conclusão do contrato decorrer de culpa da CONTRATADA, ele ficará constituído em mora, devendo ser instaurado procedimento de inexecução contratual para a aplicação das sanções administrativas cabíveis.

18.4 Na hipótese do item 18.3, a CONTRATANTE poderá optar, ainda, pela extinção do contrato e adotar as medidas previstas em lei para a continuidade da execução do objeto.

CLÁUSULA 19

Interpretação

As dúvidas interpretativas sobre as cláusulas deste contrato deverão ser suscitadas à CONTRATANTE e serão decididas por ele, de acordo com a Lei Federal nº 14.133/21, seus regulamentos, Lei Estadual n° 8.972/20 e observando a jurisprudência dos Tribunais sobre o assunto.

CLÁUSULA 20

Tratamento adequado dos conflitos de interesse

Observado o disposto na Cláusula 19, permanecendo o conflito de interesse, as PARTES se comprometem a submeter a disputa *preferencialmente* à CÂMARA DE NEGOCIAÇÃO, CONCILIAÇÃO, MEDIAÇÃO E ARBITRAGEM DA ADMINISTRAÇÃO PÚBLICA ESTADUAL para dirimir os conflitos decorrentes deste contrato de maneira consensual, conforme Lei Complementar Estadual n° 121/19.

CLÁUSULA 21

Divulgação e publicação

21.1 A CONTRATANTE divulgará este contrato no Portal Nacional de Contratações Públicas (PNCP) em até **20 dias úteis** e o publicará no Diário Oficial do Estado em forma de extrato, no prazo de **10 dias úteis**.

21.2 Os prazos contidos no item 21.1 são contados da data da assinatura do contrato.

CLÁUSULA 22

Vigência

22.1 O contrato terá vigência de 48 meses, com início em dd/mm/aa e término em dd/mm/aa.

22.2 Quando o objeto não for concluído no período acima fixado, o prazo de vigência do contrato será *automaticamente prorrogado*, sem prejuízo da aplicação dos itens 18.3 e 18.4, quando a não conclusão decorrer de culpa da CONTRATADA.

22.3 Antes da prorrogação da vigência do contrato, a CONTRATANTE deverá verificar a regularidade fiscal da CONTRATADA, consultar o CEIS e o CNEP, emitir as certidões negativas de inidoneidade, de impedimento e de débitos trabalhistas e juntá-las ao respectivo processo.

CLÁUSULA 23

Foro

As PARTES elegem o foro da Comarca de Belém-PA para resolver os litígios oriundos deste contrato, observado o disposto na Cláusula 20.

Belém (PA), _____ DE _____ DE 2023

CILENE MOREIRA SABINO DE OLIVEIRA:16656476805
Assinado de forma digital por CILENE MOREIRA SABINO DE OLIVEIRA:16656476805
Dados: 2023.08.28 13:42:55 -03'00'

CILENE MOREIRA SABINO DE OLIVEIRA
Presidente da JUCEPA
Contratante

TIAGO FARIAS DE BRITO:00497682206

EMETH CONTABILIDADE E SERVIÇOS LTDA
Tiago Farias de Brito
Contratada