REQUISIÇÃO Nº 197805

1 - OBJETO

1.1. Constituir Ata de Registro de Preços, com vigência de 12 (doze) meses, para renovação de licenças de antivírus, Kaspersky Endpoint Security, pelo período de 1 (um) ano, a fim de suprir as necessidades do parque tecnológico do Sesc-DR/PE, com uma solução de software integrado de segurança e proteção contra spam de e-mail, vazamentos de dados, tentativas de phishing e hacking, AntiMalware - vírus, ransomware, cavalos de tróia, rootkits, backdoors, com criptografia de dados, segurança móvel, segurança da plataforma Office 365, gerenciamento de dispositivos móveis, gerenciamento de sistemas e treinamento de equipe técnica Sesc/DR-PE, com atualizações para 36 (trinta e seis) meses, serviço de implantação e manutenção, conforme especificações constantes neste Termo, a fim de garantir a proteção lógica dos computadores, servidores físicos e virtuais, MS Office 365, bem como, equipamentos móveis (laptops, smartphones, tablets) integrados a rede lógica de dados do Sesc-DR/PE e demais unidades da Instituição, contra a entrada e atuação de malwares e programas maliciosos, conforme condições, quantidades, exigências e estimativas, estabelecidas neste instrumento.

2 - JUSTIFICATIVA

2.1. A utilização de uma solução de AntiMalware é imprescindível à segurança de qualquer parque computacional, uma vez que os sistemas interconectados são altamente propensos à infecção de pragas digitais. Uma solução corporativa AntiMalware serve como mecanismo centralizado de gerência e decisões nesta área, permitindo que os analistas de rede atuem na prevenção e desinfecção de forma rápida, diminuindo o impacto no ambiente. Por sua vez, estas soluções têm seu correto funcionamento diretamente ligado à frequência e à qualidade das atualizações providas pelo fabricante e chamadas de assinaturas de vírus. As pragas eletrônicas propagam-se em números alarmantes, e não dispor de solução que acompanhe tal velocidade, é estar suscetível aos seus malefícios (roubos de dados, invasões, adulterações de informações).

2.2. O Sesc-DR/PE adquiriu em 2015 uma solução de segurança para as estações de trabalho, composta por antivírus, inventário de hardware e de software e proteção endpoint, através do **Pregão Eletrônico Sesc-DR/PE 04/2015**, contrato nº 030/2015, fabricante Kaspersky. As licenças adquiridas detêm no contrato a atualização e suporte de 01 ano.

A referida contratação de subscrição e suporte expirará no dia 15 de setembro de 2025. Com o fim do prazo do contrato, os softwares em questão perderão autorização de se atualizarem através da base de suporte do fabricante, bem como será suspenso o direito de acesso ao suporte da Kaspersky, que era mantido durante o prazo de contrato supramencionado.

A citada aquisição se faz necessária para que o software adquirido volte a poder acessar as áreas de atualizações e correções do fabricante, tendo acesso as atualizações de vacinas, atualizações recomendadas e críticas/segurança; bem como para que voltemos a ter acesso ao serviço de suporte do fabricante.

Lembramos ainda que a falta de atualização fará com que o software em curto e médio prazo esteja com tanta desatualização que correremos riscos de segurança e até mesmo

possibilidades de infecções de vírus em nossa rede, que podem inviabilizar o uso dos softwares, ocasionando uma possível perda de todo investimento realizado para a compra e a instalação da solução e a possível paralisação de serviços nas nossas estações de trabalho, além de ataques de vírus e outros Malwares; além de que não teremos acesso aos novos recursos e funcionalidades que surgirem para a ferramenta que forem disponibilizados pelo fabricante.
Além de economicidade, uma atualização custa bem menos do que uma aquisição de uma contratação de solução diferente que requer mais tempo em desinstalação de solução atual, treinamento, instalação e configuração.

A atual solução de antivírus utilizada pela instituição desempenha função fundamental na estratégia de continuidade de negócio, pois contribui fortemente na manutenção da segurança das informações contidas nos computadores utilizados no Sesc-DR/PE, sejam eles estações de trabalho e servidores de rede.

Após mais de 5 anos de utilização, a solução vem atendendo de maneira satisfatória as necessidades desta Instituição, de modo que desde a instalação da solução no parque do Sesc-DR/PE não ocorreu perda de dados ou infecção de computadores.

A decisão de adquirir licenças da solução atualmente utilizada no parque se dá pelos motivos abaixo explicitados:

- É a solução atualmente utilizada no Sesc-DR/PE, tendo atingido os objetivos das contratações anteriores;
- Já existe expertise técnica no Sesc-DR/PE quanto ao domínio do funcionamento e administração da solução, e desta forma, a instituição garante o retorno de todo o investimento em pesquisas e implementações já realizadas,
- Como a solução já está instalada, configurada e com funcionamento satisfatório, não haverá custo para implantação e treinamento de equipe de operação.
- Existem várias empresas no mercado que são revendedoras autorizadas da solução, o que descaracteriza qualquer direcionamento da solução.
- A Kaspersky está bem-posicionada entre as soluções de antivírus disponíveis no mercado, conforme gráfico da Empresa Gartner, líder mundial em consultoria de TI.

Diante do exposto, seria de extrema importância para o Sesc-DR/PE adquirir as licenças da solução vigente.

2.3. O julgamento por lote justifica-se em razão da natureza integrada da solução contratada, composta por licenças, suporte, atualizações, treinamento, implantação e manutenção, os quais devem operar de forma conjunta, interoperável e compatível entre si, garantindo a eficácia da proteção do ambiente tecnológico do Sesc-DR/PE.

A contratação de fornecedor único por lote assegura maior padronização tecnológica, simplificação da gestão contratual, redução de riscos operacionais, compatibilidade entre os componentes da solução e maior eficiência no suporte técnico e atendimento, além de facilitar a responsabilização contratual.

Ademais, a contratação por lote promove economicidade, uma vez que possibilita melhores condições comerciais, reduz custos administrativos e evita fragmentação do objeto, sem

prejuízo à competitividade, considerando que existem diversos fornecedores autorizados no mercado capazes de atender integralmente ao objeto pretendido.

3 – PLANILHA DE ESPECIFICAÇÃO TÉCNICA E QUANTITATIVOS

Item	Produto	Descrição	Previsão para Aquisição Imediata	U.M	Quantidade total a ser registrada
1	LICENÇAS DE ANTIMALWARE DESKTOP, COM DIREITO A TREINAMENTO, ATUALIZAÇÕES E SUPORTE TÉCNICO DE ACORDO COM O DETALHAMENTO E ESPECIFICAÇÕES TÉCNICAS DESCRITAS NESTE TERMO.	SOFTWARE DE SEGURANÇA ENDPOINT CORPORATIVO PARA ESTAÇÕES DE TRABALHO E ANTISPAM EM NUVEM – AQUISIÇÃO KASPERSKY NEXT EDR OPTIMUM BRAZILIAN EDITION COM PROTEÇÃO PARA ANTISPAM NA NUVEM O365, COM DIREITO A TREINAMENTO, ATUALIZAÇÕES E SUPORTE TÉCNICO, POR 01 ANO.	1100	Und.	1300
2	LICENÇAS DO ANTIMALWARE EM AMBIENTE FÍSICO E VIRTUALIZADO, COM DIREITO A TREINAMENTO ATUALIZAÇÕES E SUPORTE TÉCNICO, DE ACORDO COM O DETALHAMENTO E ESPECIFICAÇÕES TÉCNICAS DESCRITAS NESTE TERMO.	LICENÇAS DO ANTIMALWARE EM AMBIENTE FÍSICO E VIRTUALIZADO KASPERSKY HYBRID CLOUD SECURITY SERVER BRAZILIAN EDITION	120	Und.	130
3	KASPERSKY MANAGED DETECTION AND RESPONSE BRAZILIAN EDITION	KASPERSKY MANAGED DETECTION AND RESPONSE BRAZILIAN EDITION	150		1300

3.1 – Critério de Julgamento

O julgamento da licitação será realizado pelo critério de menor preço por lote, considerando a totalidade dos itens que compõem a solução, em conformidade com as especificações técnicas estabelecidas neste Termo de Referência.

4 – LOCAL DE ENTREGA

4.1. A solução de AntiMalware deverá ser entregue na UTD – Unidade de Tecnologia Digital do SESC-PE, situada à Avenida Visconde de Suassuna, 265 - Santo Amaro, Recife - PE, CEP 50.050-540.

4.2. Havendo a possibilidade de obter a solução de AntiMalware via download, deverá o FORNECEDOR realizar os procedimentos de instalação juntamente com o cliente.

5 – PRAZO DE ENTREGA

5.1. A entrega das licenças deverá ocorrer em até 10 (dez) dias úteis, contados a partir do PC (Pedido de Compra) ou documento equivalente.

5.2. O início do processo de instalação deverá ocorrer em até 05 (cinco) dias úteis após solicitação formal da UTD.

6 – PRAZO DE VIGÊNCIA

6.1. A Ata de Registro de Preços terá duração de 12 (doze) meses contados a partir da data de publicação da conclusão do certame, podendo ser prorrogado por igual período.

6.3. Independente do prazo de vigência do instrumento obrigacional, estendesse os efeitos ao prazo de suporte do(s) produto(s) adquiridos.

7 – DISPOSIÇÕES GERAIS / INFORMAÇÕES COMPLEMENTARES

7.1. REQUISITOS GERAIS DE GARANTIA E SUPORTE

7.1.1. O FORNECEDOR deverá fornecer garantia e suporte para todos os serviços que envolvem o funcionamento e uso da solução, sem que isso gere qualquer ônus para a GERENCIADOR.

7.1.2. O FORNECEDOR deverá garantir a atualização de versões do software e base de dados que compõem a solução, as quais incorporam correções de erros ou problemas registrados e melhorias nas funcionalidades implementadas pela Fabricante da Solução. Os procedimentos de atualização têm por finalidade assegurar a devida atualização da solução durante o período de suporte dos produtos.

7.2. REQUISITOS GERAIS DE TECNOLOGIA

7.2.1. Requisitos de arquitetura tecnológica (Requisitos de projeto e implementação)

7.2.1.1. Em até 10 (dez) dias úteis após o recebimento do PC, o FORNECEDOR deverá elaborar e disponibilizar para equipe técnica de fiscalização do GERENCIADOR, o Projeto de Implantação da Solução de Segurança e Proteção AntiMalware, de acordo com o ambiente tecnológico disponível no GERENCIADOR. O projeto deverá prever a implantação, em suas

respectivas fases, agrupando as atividades conforme cada uma das etapas e/ou subetapas, com detalhamento do cronograma, definições dos marcos de entrega, contemplando as fases de validação, aprovação e início de produção das etapas e/ou subetapas até que a solução esteja completamente operante no GERENCIADOR. A entrega deverá ser feita na forma arquivo digital e impressa, editável, devidamente encadernada, descrevendo cada uma das etapas e/ou subetapas, pré-requisitos, resultados previstos, cronograma e demais artefatos comuns em projetos de Tecnologia, Informação e Comunicação;

7.2.1.2. Após a implantação de toda a solução, devidamente validadas e aprovadas em todas as etapas pela equipe técnica da Sesc/DR-PE, responsável pela fiscalização da Ata), o FORNECEDOR deverá elaborar e disponibilizar o Projeto em sua versão final, de acordo com o que fora executado. A entrega deverá ser feita no arquivo digital e impressa, editável, devidamente encadernada, descrevendo cada uma das etapas e/ou subetapas, pré-requisitos, resultados previstos e alcançados, cronograma e demais artefatos comuns em projetos de Tecnologia, Informação e Comunicação;

7.2.1.3. Tendo em vista que a solução atenderá a todo o parque tecnológico do SESC-PE, esta deverá manter a compatibilidade com as seguintes distribuições de sistemas operacionais de 32 bits e 64 bits, devendo atender, também, com versões superiores destas distribuições:

a) GNU Linux e seus derivados;
b) Windows 10 ou superior;
c) Windows server 2008;
d) Windows server 2012;
e) Windows server 2016 ou superior
f) MAC OS X 10.4 ou superior;

7.2.1.4. SISTEMAS OPERACIONAIS X SERVIDORES FÍSICOS E VIRTUAIS

SISTEMA OPERACIONAL	SERVIDORES FÍSICAS	SERVIDORES VIRTUAIS	QUANTIDADE
Windows Server 2008 R2		X	1
Windows Server 2008 R2	X		2
Windows Server 2012 Standard		X	1
Windows Server 2012 Standard	X		1
Windows Server 2012 R2	X		3
Windows Server 2012 R2		X	12
Windows Server 2012 R2 Standard		X	2
Windows Server 2012 R2 Standard	X		1
Windows Server 2012 Datacenter		X	1
Windows Server 2016 Standard	X		16
Windows Server 2016 Standard		X	70
Windows Storage Server 2012 R2 Standard		X	1

7.2.1.5. SISTEMAS OPERACIONAIS X DESKTOPS

SISTEMA OPERACIONAL	QUANTIDADE DESKTOPS
Windows 10 Professional	907
Windows 11	175

7.2.1.6. A solução deverá ser capaz de bloquear atividades de malware, explorando vulnerabilidades em software de terceiros;

7.2.1.7. A solução deverá ser capaz de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina;

7.2.1.8. A solução deverá ser capaz de identificar processo malicioso de criptografia não autorizado antes de ser iniciado, realizando backup dos dados automaticamente e possibilitando volta ao estado inicial;

7.2.1.9. A solução deverá ser capaz de limitar a execução de aplicativos por hash MD5, nome de arquivo, versão do arquivo, nome do aplicativo, fabricante/desenvolvedor, categoria (ex.: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc);

7.2.1.10. A solução deverá ser capaz de habilitar automaticamente uma política, sempre que ocorrer uma epidemia na rede, baseado em quantidade de malware encontrados em determinado intervalo de tempo;

7.2.1.11. A solução deverá ser capaz de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e regras de acesso à internet;

7.2.1.12. A solução deverá ser capaz de gerenciar todos os recursos da solução através de uma única console;

7.2.2. Requisitos Gerais do Suporte Técnico

7.2.2.1. Deverá funcionar em regime de horário **24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, inclusive feriados, para chamados de Nível 1 (Serviços Indisponíveis/Epidemia)**. Casos excepcionais serão estabelecidos pela UTD. **Para chamados de Nível 2 e Nível 3, o suporte poderá ocorrer em regime de horário administrativo, das 08:00 às 17:00 horas, de segunda à sexta.**

7.2.2.2. Os métodos para abertura de chamado deverão ser via telefone ou portal Web;

7.2.2.3. A equipe de suporte deverá prestar toda assistência remota necessária até a resolução dos problemas, tais como:

I. Nível 1: Serviços Indisponíveis

a) Interrupção dos negócios ou rede inoperante;
b) Epidemia de vírus por toda a rede;
c) Serviços críticos gravemente afetados;
d) Servidores que não estão se comunicando com a console de gerenciamento;
e) Ou similar;

II. Nível 2: Serviços Parcialmente Indisponíveis

a) Detecção de falsos positivos que afetam serviços críticos;
b) Suporte para upgrade de versões e releases do software;
c) Ou similar;

III. Nível 3: Serviços disponíveis com ocorrência de falhas ou alertas

a) Máquinas que não estão se comunicando com a console de gerenciamento;
b) Análise e correção de eventos relacionados à segurança e à performance do software e do ambiente;
c) Ou similar;

Níveis de Severidade	
Nível	**Descrição**
1	Serviços indisponíveis
2	Serviços parcialmente indisponíveis ou com degradação dos serviços.
3	Serviços disponíveis com ocorrência de falhas ou alertas. Dúvidas geral sobre equipamentos

7.2.2.4. Para efeito dos atendimentos técnicos aos chamados, o FORNECEDOR deverá observar os níveis de severidade e respectivos prazos máximos fixados:

Prazo máximo para Início de Atendimento				
Tipo	**Prazo**	**Nível de Severidade**		
		1	**2**	**3**
Remoto	Tempo	2 horas	6 horas	24 horas

7.2.2.5. O FORNECEDOR arcará com todas as despesas decorrentes dos serviços de garantia e suporte técnico.

7.2.2.6. Após a prestação de cada serviço de garantia/suporte técnico, o FORNECEDOR deverá emitir o relatório correspondente, no qual deverão constar todos os dados relevantes sobre a data e hora do chamado, do diagnóstico, o nome do técnico que realizou os serviços, a hora de início e de término do atendimento.

8 – DETALHAMENTO E ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO

ITEM 1: LICENÇAS DE ANTIMALWARE

SERVIDOR DE ADMINISTRAÇÃO E CONSOLE ADMINISTRATIVA

1. A console deverá ser acessada via WEB (HTTPS) ou MMC;
2. Console deverá ser baseada no modelo cliente/servidor;
3. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;
4. Deverá permitir a atribuição de perfis para os administradores da Solução de AntiMalware;
5. Deverá permitir incluir usuários do AD para logarem na console de administração;
6. Console deverá ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM;
7. As licenças deverão ser por subscrição anual (12 meses), ou seja, expirado a validade do produto as funcionalidades de atualização e acesso ao serviço de inteligência de ameaças (Kaspersky Security Network) serão desativadas, sendo necessária a renovação para manter a proteção eficaz.
8. Capacidade de remover remotamente e automaticamente qualquer solução de AntiMalware (própria ou de terceiros) que estiver presente nas estações e servidores;
9. Capacidade de instalar remotamente a solução de AntiMalware nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;
10. Deverá registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
11. Deverá armazenar histórico das alterações feitas em políticas;
12. Deverá permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada;
13. Deverá ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas;
14. A solução de gerência deverá permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;
15. Através da solução de gerência, deverá ser possível verificar qual licença está aplicada para determinado computador;
16. Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS, Android e Windows;
17. Capacidade de instalar remotamente qualquer app em smartphones e tablets de sistema iOS;
18. A solução de gerência centralizada deverá permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;
19. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário;
20. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução AntiMalware;
21. Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança;
22. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede;

23. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;
24. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;
25. Capacidade de fazer distribuição remota de qualquer software, ou seja, deverá ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de AntiMalware para que seja instalado nas máquinas clientes;
26. A comunicação entre o cliente e o servidor de administração deverá ser criptografada;
27. Capacidade de desinstalar remotamente, através da console de gerenciamento, qualquer software instalado nas máquinas clientes;
28. Deverá permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

    a) Nome do computador;
    b) Nome do domínio;
    c) Range de IP;
    d) Sistema Operacional;
    e) Máquina virtual.

29. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;
30. Deverá permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional;
31. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;
32. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção;
33. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o AntiMalware instalado. Caso não possuir, deverá instalar o AntiMalware automaticamente;
34. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o AntiMalware instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias, etc.;
35. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;
36. Deverá fornecer as seguintes informações dos computadores:

    a) Se o AntiMalware está instalado;
    b) Se o AntiMalware está iniciado;
    c) Se o AntiMalware está atualizado;
    d) Minutos/horas desde a última conexão da máquina com o servidor administrativo;
    e) Minutos/horas desde a última atualização de vacinas;
    f) Data e horário da última verificação executada na máquina;

g) Versão do AntiMalware instalado na máquina;
h) Se é necessário reiniciar o computador para aplicar mudanças;
i) Data e horário de quando a máquina foi ligada;
j) Quantidade de vírus encontrados (contador) na máquina;
k) Nome do computador;
l) Domínio ou grupo de trabalho do computador;
m) Data e horário da última atualização de vacinas;
n) Sistema operacional com Service Pack;
o) Quantidade de processadores;
p) Quantidade de memória RAM;
q) Usuário (s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);
r) Endereço IP;
s) Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;
t) Atualizações do Windows Updates instaladas;
u) Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;
v) Vulnerabilidades de aplicativos instalados na máquina;

37. Deverá permitir bloquear as configurações do AntiMalware instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
38. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:

a) Alteração de Gateway Padrão;
b) Alteração de subrede;
c) Alteração de domínio;
d) Alteração de servidor DHCP;
e) Alteração de servidor DNS;
f) Alteração de servidor WINS;
g) Resolução de Nome;
h) Disponibilidade de endereço de conexão SSL;
i) Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;

39. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
40. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de AntiMalware;
41. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
42. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor

administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;

43. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;
44. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;
45. Capacidade de gerar traps SNMP para monitoramento de eventos;
46. Capacidade de enviar e-mails para contas específicas em caso de algum evento;
47. Listar em um único local, todos os computadores não gerenciados na rede;
48. Deverá encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes;
49. Capacidade de baixar novas versões do AntiMalware direto pela console de gerenciamento, sem a necessidade de importá-los manualmente
50. Deverá possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por exemplo).
51. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc.), inclusive de máquinas que estejam em subnets diferentes do servidor;
52. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
53. Deverá através de opções de optimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o AntiMalware ativo, porém sem comprometer o desempenho do computador;
54. Deverá permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, (ex: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint);
55. Permitir fazer uma verificação rápida ou detalhada de um dispositivo removível assim que conectado no computador, podendo configurar a capacidade máxima em GB da verificação;
56. Deverá ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do Windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros;
57. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;
58. Deverá armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:

    a) Nome do vírus;
    b) Nome do arquivo infectado;
    c) Data e hora da detecção;
    d) Nome da máquina ou endereço IP;
    e) Ação realizada.

59. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;

60. Capacidade de listar updates nas máquinas com o respectivo link para download;
61. Deverá criar um backup de todos arquivos deletados em computadores para que possa ser restaurado através de comando na Console de administração;
62. Deverá ter uma quarentena na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante;
63. Capacidade de realizar inventário de hardware de todas as máquinas clientes;
64. Capacidade de realizar inventário de aplicativos de todas as máquinas clientes;
65. Capacidade de diferenciar máquinas virtuais de máquinas físicas.
66. Possuir as seguintes características de CRIPTOGRAFIA:

a) O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação;
b) Utilizar, no mínimo, algoritmo AES com chave de 256 bits;
c) Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;
d) Capacidade de utilizar Single Sign-On para a autenticação de pré-boot;
e) Permitir criar vários usuários de autenticação pré-boot;
f) Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento; g)
g) Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:

g.1) Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;
g.2) Criptografar todos os arquivos individualmente;
g.3) Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;
g.4) Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;

h) Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente. Nesta modalidade, os arquivos devem estar acessíveis para todas as máquinas gerenciadas pela mesma console de maneira transparente para os usuários;
i) Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;
j) Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;
k) Verifica compatibilidade de hardware antes de aplicar a criptografia;
l) Possibilita estabelecer parâmetros para a senha de criptografia;
m) Bloqueia o reuso de senhas;
n) Bloqueia a senha após um número de tentativas pré-estabelecidas;
o) Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;

p) Permite criar exclusões para não criptografar determinados discos rígidos através de uma busca por nome do computador ou nome do dispositivo;
q) Permite criptografar as seguintes pastas pré-definidas: meus documentos, Favoritos, Desktop, arquivos temporários e arquivos do outlook;
r) Permite utilizar variáveis de ambiente para criptografar pastas customizadas;
s) Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de áudio etc.;
t) Permite criar um grupo de extensões de arquivos a serem criptografados;
u) Capacidade de criar regra de criptografia para arquivos gerados por aplicações;
v) Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento;
w) Capacidade de deletar arquivos de forma segura após a criptografia;
x) Capacidade de criptografar somente o espaço em disco utilizado;
y) Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;
z) Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;
aa) Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc.;
bb) Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;
cc) Deve ter a opção de utilização de TPM para criptografia através do BitLocker;
dd) Capacidade de fazer Hardware encryption;

67. Deverá possui as seguintes características para o gerenciamento do sistema:

a) Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;
b) Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários;
c) Capacidade de gerenciar licenças de softwares de terceiros;
d) Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;
e) Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc.), informando data de compra, local onde se encontra, service tag, número de identificação e outros;
f) Possibilita fazer distribuição de software de forma manual e agendada;
g) Suporta modo de instalação silenciosa;
h) Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;
i) Possibilita fazer a distribuição através de agentes de atualização;
j) Utiliza tecnologia multicast para evitar tráfego na rede;
k) Possibilita criar um inventário centralizado de imagens;
l) Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;

m) Suporte a WakeOnLan para deploy de imagens;
n) Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;
o) Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;
p) Capacidade de gerar relatórios de vulnerabilidades e patches;
q) Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;
r) Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;
s) Permite baixar atualizações para o computador sem efetuar a instalação;
t) Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;
u) Capacidade de instalar correções de vulnerabilidades de acordo com a Severidade;
v) Permite selecionar produtos a serem atualizados pela console de gerenciamento;
w) Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc.;
x) Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;
y) Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador;
z) Capacidade de configurar o reinício do computador após a aplicação das atualizações e correções de vulnerabilidades;
aa) Deve permitir selecionar o idioma das aplicações que serão atualizadas;
bb) Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes;

68. Compatibilidade:

a) Microsoft Windows Server 2012 (Todas edições);
b) Microsoft Windows Server 2012 R2 (Todas edições);
c) Microsoft Windows Server 2016 x64 ou superior;
d) Microsoft Windows 10 todas as edições x32 e x64 ou superior;
e) Microsoft Windows 11 todas edições ou superior.

69. Suportar as seguintes plataformas virtuais:

a) Vmware: Workstation 12.x Pro ou superior, vSphere 5.5, vSphere 6 e vShere 6.5 ou superior;
b) Microsoft Hyper-V: 2008, 2008 R2, 2008 R2 SP1, 2012, 2012 R2, 2016;
c) Microsoft VirtualPC 6.0.156.0;
d) Parallels Desktop 7 e 11;
e) Oracle VM VirtualBox 4.0.4-70112 (Somente logon como convidado);
f) Citrix XenServer 6.2, 6.5, 7.0 e 7.2
g) Citrix XenDesktop 7.14
h) Citrix Provisioning Services 7.14 DOS SERVIDORES

SISTEMA OPERACIONAL WINDOWS:

1. Deve prover as seguintes proteções:

   a) Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
   b) Autoproteção contra-ataques aos serviços/processos do antivírus;
   c) Firewall com IDS;
   d) Controle de vulnerabilidades do Windows e dos aplicativos instalados;

2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
3. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
4. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

   a) Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
   b) Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
   c) Leitura de configurações;
   d) Modificação de configurações;
   e) Gerenciamento de Backup e Quarentena;
   f) Visualização de relatórios;
   g) Gerenciamento de relatórios;
   h) Gerenciamento de chaves de licença;
   i) Gerenciamento de permissões (adicionar/excluir permissões acima);

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

   a) Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
   b) Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso à rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados;

6. Capacidade de, separadamente, selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total;
7. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede;
8. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc);
9. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply UPS);
10. Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;
11. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;

12. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;
13. apacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;
14. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
15. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: Win32.Trojan.banker) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
16. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
17. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
18. Capacidade de verificar somente arquivos novos e alterados;
19. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos autodescompressores, .PST, arquivos compactados por compactadores binários, etc.);
20. Capacidade de verificar objetos usando heurística;
21. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;
22. Capacidade de agendar uma pausa na verificação;
23. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
24. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

    a) Perguntar o que fazer, ou;
    b) Bloquear acesso ao objeto;
    c) Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração preestabelecida pelo administrador);
    d) Caso positivo de desinfecção, restaurar o objeto para uso;
    e) Caso negativo de desinfecção, mover para quarentena ou apagar (de acordo com a configuração preestabelecida pelo administrador);

25. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
26. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
27. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
28. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa;
29. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros;
30. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).
31. Compatibilidade:

a) Microsoft Windows Storage Server SP2 Workgroup Edition;
b.) Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter;
c.) Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter;
d.) Microsoft Windows Server 2012 Core Essentials / Standard / Foundation / Datacenter;
e.) Microsoft Windows Server 2012 R2 Core Essentials / Standard / Foundation / Datacenter;
f.) Microsoft Windows Storage Server 2012 (Todas edições);
g.) Microsoft Windows Storage Server 2012 R2 (Todas edições);
h.) Microsoft Windows Hyper-V Server 2012;
i.) Microsoft Windows Hyper-V Server 2012 R2 ou superior;
j.) Windows Server 2016 Essentials/Standard/Datacenter/Core ou posterior;
k.) Windows Storage Server 2016 ou posterior;
l.) Windows Hyper-V Server 2016.

MS OFFICE 365

1. Características Gerais

1.1 A solução deve ser entregue no modelo de “Software as a Service”, onde servidor e console administrativa são hospedados na nuvem.
1.2 Acesso a console administrativa via HTTPS.
1.3 A integração com o Office 365 deve ser realizada via API.
1.4 A autenticação da integração deve ser realizada via protocolo seguro OAuth 2.0.
1.5 A solução deve prover módulos de proteção para a suíte Microsoft Office 365 (Exchange Online, OneDrive, SharePoint e Teams).
1.6 A console deve prover painel de informações exibindo as informações principais da operação e do estado dos componentes de proteção.
1.7 Capacidade de geração de relatórios em no mínimo formato “.pdf”.
1.8 Capacidade de geração de relatório instantâneo;
1.9 Capacidade de agendamento automático de relatórios.
1.10 A solução deve verificar o tráfego de e-mails inbound e outbound.
1.11 Deve possuir quarentena para armazenar artefatos detectados como maliciosos.
1.12 A quarentena deve possuir no mínimo as seguintes opções:

1.12.1 Exibir detalhes do item;
1.12.2 Excluir item;
1.12.3 Liberar item;
1.12.4 Filtrar itens;
1.12.5 Salvar item em disco;

1.13 A gestão da solução deve ser realizada por usuário com perfil de administrador.
1.14 Deve ser possível atribuir perfil de administrador para um usuário na console de administração.

2. **Módulos de Proteção**

2.1 Anti-malware

2.1.1 Deve proteger as caixas de correio contra vírus, worms, trojans, entre outras ameaças que podem ser enviadas via e-mail.
2.1.2 Análise das ameaças deve ser realizada por no mínimo as seguintes tecnologias:
2.1.2.1. Assinaturas;
2.1.2.2. Heurística;
2.1.2.3. Comportamento;
2.1.2.4. Consulta ao repositório de inteligência do fabricante.
2.1.3 Capacidade de detectar ataques conhecidos e desconhecidos.
2.1.4 Ao detectar um malware, a solução deve tomar uma ou mais ações de acordo com a configuração do administrador, possibilitando no mínimo:
2.1.4.1. Excluir a mensagem e coloca-la em quarentena;
2.1.4.2. Excluir anexo infectado e colocá-lo em quarentena;
2.1.4.3. Colocar tag no assunto;
2.1.4.4. Substituir arquivo por mensagem personalizada;
2.1.5 Notificar ao administrador sobre novas ameaças encontradas
2.1.6 Notificar ao proprietário da caixa sobre mensagens excluídas.
2.1.7 Deve analisar arquivos nas seguintes aplicações:
2.1.7.1. Exchange Online
2.1.7.2. OneDrive
2.1.7.3. SharePoint
2.1.7.4. Teams

2.2 Anti-phishing

2.2.1 Deve proteger as caixas de correio contra phishing e links maliciosos enviados em mensagens de e-mail, evitando assim infecção por malware, roubo de dados pessoas e acesso a sites fraudulentos.
2.2.2 Deve validar o conteúdo das mensagens para detectar phishing, utilizando as seguintes tecnologias:
2.2.2.1. SPF (Sender Policy Framework)
2.2.2.2. DKIM (Domain-based Message Authentication)
2.2.2.3. DMARC (Domain-based Message Authentication, Reporting and Conformance)
2.2.2.4. Consulta ao repositório de inteligência do fabricante.
2.2.3 Capacidade de detectar ataques conhecidos e desconhecidos.
2.2.4 Ao detectar um link de phishing, a solução deve tomar uma ou mais ações de acordo com a configuração do administrador, possibilitando no mínimo:
2.2.4.1. Excluir a mensagem e coloca-la em quarentena;
2.2.4.2. Permitir;
2.2.4.3. Mover para pasta “Lixo eletrônico”;
2.2.4.4. Colocar tag no assunto;
2.2.5 Notificar ao administrador sobre novas mensagens encontradas.

2.2.6 Notificar ao proprietário da caixa sobre mensagens excluídas.
2.2.7 Permitir a criação de exclusões por e-mail completo ou máscara.

2.3 Anti-spam / Mass Mail

2.3.1 Deve proteger as caixas de correio contra e-mail não solicitados "SPAM" e e-mails enviados em massa.
2.3.2 A verificação deve ser realizada através dos seguintes métodos:

2.3.2.1. Verificação de cabeçalho, conteúdo, anexos e elementos de design;
2.3.2.2. Algoritmos linguísticos e heurísticos;
2.3.2.3. Consulta ao repositório de inteligência do fabricante;

2.3.3 Ao detectar um SPAM, a solução deve tomar uma ou mais ações de acordo com a configuração do administrador, possibilitando no mínimo:

2.3.3.1. Permitir;
2.3.3.2. Mover para a pasta "Lixo eletrônico";
2.3.3.3. Colocar tag no assunto;

2.3.4 Notificar ao administrador sobre novas ameaças encontradas
2.3.5 Notificar ao proprietário da caixa sobre mensagens excluídas.
2.3.6 Permitir a criação de exclusões por e-mail completo ou máscara.

2.4 Filtro de conteúdo

2.4.1 Deve possibilitar a filtragem de anexos em mensagens de e-mail.
2.4.2 Capacidade de detectar anexos pelos seguintes parâmetros:

2.4.2.1. Formato do arquivo;
2.4.2.2. Nome completo do arquivo;
2.4.2.3. Nome do arquivo com máscara;
2.4.2.4. Arquivos MS Office com macro;

2.4.3 Ao detectar um anexo que se encaixe em uma das regras, a solução deve possibilitar as seguintes ações:

2.4.3.1. Excluir mensagem e coloca-la em quarentena;
2.4.3.2. Excluir anexo e colocá-lo em quarentena;
2.4.3.3. Permitir
2.4.3.4. Colocar tag no assunto;
2.4.3.5. Substituir arquivo por mensagem personalizada;

2.4.4 Notificar ao administrador sobre novas ameaças encontradas
2.4.5 Notificar ao proprietário da caixa sobre mensagens excluídas.
2.4.6 Permitir a criação de exclusões por e-mail completo ou máscara.

DOS SERVIDORES

SISTEMA OPERACIONAL LINUX:

1. Deve prover as seguintes proteções:

a) Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
b) As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

2. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

a) Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
b) Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;
c) Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
d) Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados;

3. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;
4. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
5. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
6. Capacidade de verificar objetos usando heurística;
7. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
8. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
9. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).
10. Compatibilidade:

a) Plataforma 32-bits:

a.1) Red Hat Enterprise Linux 6.7;
a.2) Red Hat Enterprise Linux 6.8 ou posterior;
a.3) CentOS-6.7;
a.4) CentOS-6.8 ou posterior;
a.5) Ubuntu 14.04 LTS;

a.6) Ubuntu 16.04 LTS;
a.7) Ubuntu 16.10 LTS ou posterior;
a.8) Debian GNU/Linux 7.10;
a.9) Debian GNU/Linux 7.11;
a.10) Debian GNU/Linux 8.6;
a.11) Debian GNU/Linux 8.7 ou posterior;

b) Plataforma 64-bits:

b.1) Red Hat Enterprise Linux 6.7;
b.2) Red Hat Enterprise Linux 6.8;
b.3) Red Hat Enterprise Linux 7.2;
b.4) Red Hat Enterprise Linux 7.3 ou posterior;
b.5) CentOS-6.7;
b.6) CentOS-6.8;
b.7) CentOS-7.2;
b.8) CentOS-7.3 ou posterior;
b.9) Ubuntu 14.04 LTS;
b.10) Ubuntu 16.04 LTS;
b.11) Ubuntu 16.10 LTS ou posterior;
b.12) Debian GNU/Linux 7.10;
b.13) Debian GNU/Linux 7.11;
b.14) Debian GNU/Linux 8.6;
b.15) Debian GNU/Linux 8.7 ou posterior;
b.16) OpenSUSE 42.2;
b.17) SUSE Linux Enterprise Server 12 ou posterior;
b.18) OracleLinux 7.3 ou posterior;
b.19) Novell Open Enterprise Server 11 SP3;
b.20) Novell Open Enterprise Server 2015 SP1 ou posterior;

DAS ESTAÇÕES DE TRABALHO

SISTEMA OPERACIONAL WINDOWS:

1. Deve prover as seguintes proteções:

a) AntiMalware de Arquivos residente (anti-spyware, anti-trojan, antimalware, etc) que verifique qualquer arquivo criado, acessado ou modificado; b) AntiMalware de Web (módulo para verificação de sites e downloads contra vírus);
b) AntiMalware de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
c) AntiMalware de Mensagens Instantâneas;
d) O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
e) Firewall com IDS;
f) Autoproteção (contra-ataques aos serviços/processos do AntiMalware);
g) Controle de dispositivos externos;

h) Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc;
i) Controle de acesso a sites por horário;
j) Controle de acesso a sites por usuários;
k) Controle de acesso a websites por dados, ex: Bloquear websites com conteúdos de vídeo e áudio;
l) Controle de execução de aplicativos;
m) Controle de vulnerabilidades do Windows e dos aplicativos instalados;

2. Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
3. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
4. Capacidade de detecção de presença de AntiMalware de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
5. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do AntiMalware, (ex: Win32.Trojan.banker) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
6. Capacidade de adicionar aplicativos a uma lista de aplicativos confiáveis, onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;
7. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
8. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
9. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O AntiMalware deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
10. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas;
11. Capacidade de verificar somente arquivos novos e alterados;
12. Capacidade de verificar objetos usando heurística;
13. Capacidade de agendar uma pausa na verificação;
14. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;
15. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
16. O AntiMalware de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

a) Perguntar o que fazer, ou;
b) Bloquear acesso ao objeto;
c) Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
d) Caso positivo de desinfecção:
e) Restaurar o objeto para uso;

f) Caso negativo de desinfecção, mover para quarentena ou apagar (de acordo com a configuração pré- estabelecida pelo administrador);

17. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o AntiMalware deve realizar um backup do objeto;
18. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, IMAP, NNTP, SMTP e MAPI;
19. Capacidade de verificar links inseridos em e-mails contra phishings;
20. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox e Opera;
21. Capacidade de verificação de corpo e anexos de e-mails usando heurística;
22. O AntiMalware de e-mail, ao encontrar um objeto potencialmente perigoso, deve:

a) Perguntar o que fazer, ou;
b) Bloquear o e-mail;
c) Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
d) Caso positivo de desinfecção, restaurar o e-mail para o usuário;
e) Caso negativo de desinfecção, mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);

24. Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;
25. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;
26. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeandoos de acordo com a configuração feita pelo administrador;
27. Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurísticas;
28. Deve ter suporte total ao protocolo Ipv6;
29. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;
30. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:

a) Perguntar o que fazer, ou;
b) Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;
c) Permitir acesso ao objeto;

31. O AntiMalware de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:

a) Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo-real, ou;
b) Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação;

32. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo AntiMalware de web;
33. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;

34. Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;
35. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas;
36. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://www.antiphishing.org/);
37. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;
38. Deve possuir módulo IDS (Intrusion Detection System) para proteção contra port scans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas;
39. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

a) Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
b) Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

40. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:

a) Discos de armazenamento locais;
b) Armazenamento removível;
c) Impressoras;
d) CD/DVD;
e) Drives de disquete;
f) Modems;
g) Dispositivos de fita;
h) Dispositivos multifuncionais;
i) Leitores de smart card;
j) Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc);
k) Wi-Fi;
l) Adaptadores de rede externos;
m) Dispositivos MP3 ou smartphones;
n) Dispositivos Bluetooth;
o) Câmeras e Scanners.

41. Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário;
42. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;

43. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;
44. Capacidade de habilitar logging em dispositivos removíveis tais como Pendrive, Discos externos, etc.
45. Capacidade de configurar novos dispositivos por Class ID/Hardware ID;
46. Capacidade de limitar a execução de aplicativos por hash MD5, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc);
47. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
48. Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo;
49. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web;
50. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

51. **Compatibilidade:**

a) Microsoft Windows 10 Pro / Enterprise x86 / x64;
b) Microsoft Windows 11 todas as edições;
e) Microsoft Windows Server 2012 R2 Standard x64;
f) Microsoft Windows Server 2012 Foundation x64;
g) Microsoft Windows Server 2012 Standard x64;
h) Microsoft Small Business Server 2011 Standard x64;
i) Microsoft Windows Server 2008 R2 Standard/Enterprise x64 SP1;
j) Microsoft Windows Server 2008 Standard/Enterprise x86/x64 SP2;
k) Microsoft Windows Server 2016 Standard/Enterprise/datacenter 4 ou posterior;

SISTEMA OPERACIONAL MAC OS X:

1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
2. Possuir módulo de web-AntiMalware para proteger contra ameaças durante navegação na internet com possibilidade de analisar endereços https; 3. Possuir módulo de bloqueio á ataques na rede;
4. Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador;
5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio à ataques na rede;
6. Possibilidade de importar uma chave no pacote de instalação;
7. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

8. A instalação e a primeira execução do produto deve ser feita sem a necessidade de reinicialização do computador, de modo que, o produto funcione com toda sua capacidade;
9. Deve possuir suportes a notificações utilizando o Growl;
10. As vacinas devem ser atualizadas pelo fabricante e disponibilizadas aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
11. Capacidade de voltar para a base de dados de vacina anterior;
12. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;
13. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do AntiMalware, (ex: Win32.Trojan.banker) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
14. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
15. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O AntiMalware deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
16. Capacidade de verificar somente arquivos novos e alterados;
17. Capacidade de verificar objetos usando heurística;

a) Capacidade de agendar uma pausa na verificação;
b) O AntiMalware de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
c) Perguntar o que fazer, ou;
d) Bloquear acesso ao objeto;
e) Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
f) Caso positivo de desinfecção, restaurar o objeto para uso;

18. Caso negativo de desinfecção, mover para quarentena ou apagar (de acordo com a configuração pré- estabelecida pelo administrador);
19. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o AntiMalware deve realizar um backup do objeto;
20. Capacidade de verificar arquivos de formato de email;
21. Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o AntiMalware e iniciar o AntiMalware pela linha de comando;
22. Capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento.
23. Compatibilidade:

a) Mac OS X 10.11 (El Capitan);
b) Mac OS X 10.10 (Yosemite);
c) Mac OS X 10.9 (Mavericks);
d) Mac OS X 10.8 (Mountain Lion);
e) Mac OS X 10.7 (Lion);
f) Mac OS Sierra 10.12;

SISTEMA OPERACIONAL LINUX:

1. Deve prover as seguintes proteções:

a) AntiMalware de arquivos residente (anti-spyware, anti-trojan, antimalware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
b) As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
c) Capacidade de configurar a permissão de acesso às funções do AntiMalware;
d) Capacidade de criar exclusões por local, máscara e nome da ameaça;
e) Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
f) Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;
g) Dectectar aplicações que possam ser utilizadas como vetor de ataque por hackers;
h) Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:

h.1) Alta;
h.2) Média;
h.3) Baixa;
h.4) Recomendado;

i) Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
j) Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.
k) Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;
l) Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
m) Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O AntiMalware deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

GERENCIAMENTO DE SISTEMAS:

1. Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores bare-metal;
2. Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;
3. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;

4. Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários;
5. Capacidade de gerenciar licenças de softwares de terceiros;
6. Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;
7. Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc), informando data de compra, local onde se encontra, service tag, número de identificação e outros;
8. Possibilita fazer distribuição de software de forma manual e agendada;
9. Suporta modo de instalação silenciosa;
10. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;
11. Possibilita fazer a distribuição através de agentes de atualização;
12. Utiliza tecnologia multicast para evitar tráfego na rede;
13. Possibilita criar um inventário centralizado de imagens;
14. Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;
15. Suporte a WakeOnLan para deploy de imagens;
16. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;
17. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;
18. Capacidade de gerar relatórios de vulnerabilidades e patches;
19. Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;
20. Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;
21. Permite baixar atualizações para o computador sem efetuar a instalação;
22. Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;
23. Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;
24. Permite selecionar produtos a serem atualizados pela console de gerenciamento;
25. Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc;
26. Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;
27. Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador;
28. Capacidade de configurar o reinício do computador após a aplicação das atualizações e correções de vulnerabilidades;
29. Deve permitir selecionar o idioma das aplicações que serão atualizadas;
30. Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes;

a) Capacidade de verificar objetos usando heurística;
b) Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

c) Deve possuir função para? escolha da pasta? onde arquivos restaurados de backup deverão ser salvos em local definido pelo cliente; de administração remota através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

31. Compatibilidade:

a) Plataforma 32-bits:

a.1) Red Hat Enterprise Linux 6.7;
a.2) Red Hat Enterprise Linux 6.8;
a.3) CentOS-6.7;
a.4) CentOS-6.8;
a.5) Ubuntu 14.04 LTS;
a.6) Ubuntu 16.04 LTS;
a.7) Ubuntu 16.10 LTS;
a.8) Debian GNU/Linux 7.10;
a.9) Debian GNU/Linux 7.11;
a.10) Debian GNU/Linux 8.6;
a.11) Debian GNU/Linux 8.7.

b) Plataforma 64-bits:

b.1) Red Hat Enterprise Linux 6.7;
b.2) Red Hat Enterprise Linux 6.8;
b.3) Red Hat Enterprise Linux 7.2;
b.4) Red Hat Enterprise Linux 7.3 e versões superiores;
b.5) CentOS-6.7;
b.6) CentOS-6.8;
b.7) CentOS-7.2;
b.8) CentOS-7.3 e versões superiores;
b.9) Ubuntu 14.04 LTS;
b.10) Ubuntu 16.04 LTS;
b.11) Ubuntu 16.10 LTS e versões superiores;
b.12) Debian GNU/Linux 7.10;
b.13) Debian GNU/Linux 7.11;
b.14) Debian GNU/Linux 8.6;
b.15) Debian GNU/Linux 8.7 e versões superiores;
b.16) OpenSUSE 42.2 e versões superiores;
b.17) SUSE Linux Enterprise Server 12 e versões superiores;
b.18) OracleLinux 7.3 e versões superiores;
b.19) Novell Open Enterprise Server 11 SP3 e versões superiores;
b.20) Novell Open Enterprise Server 2015 SP1 e versões superiores

DOS DISPOSITIVOS MÓVEIS TABLETS E SMARTPHONES:

1. Deve prover as seguintes proteções:

a) Proteção em tempo real do sistema de arquivos do dispositivo e interceptação e verificação de:

a.1) Proteção contra adware e autodialers;
a.2) Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser;
a.3) Arquivos abertos no smartphone;
a.4) Programas instalados usando a interface do smartphone;
a.5) Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;
a.6) Deverá isolar em área de quarentena os arquivos infectados;
a.7) Deverá atualizar as bases de vacinas de modo agendado;
a.8) Deverá bloquear spams de SMS através de Black lists;
a.9) Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado com mensagem de aviso ao utilizador do dispositivo;
a.10) Capacidade de desativar por política:
a.11) Wi-fi;
a.12) Câmera;
a.13) Bluetooth.

b) Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;
c) Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha;
d) Deverá ter firewall pessoal (Android);
e) Capacidade de tirar fotos quando a senha for inserida incorretamente;
f) Possibilidade de instalação remota utilizando o Microsoft System Center Mobile Device Manager 2008 SP1;
g) Capacidade de enviar comandos remotamente de:

g.1) Localizar;
g.2) Bloquear.

h) Capacidade de detectar Jailbreak em dispositivos iOS;
i) Capacidade de bloquear o acesso a site por categoria em dispositivos;
j) Capacidade de bloquear o acesso a sites phishing ou malicioso;
k) Capacidade de criar containers de aplicativos, separando dados corporativos de dados pessoais;
l) Capacidade de bloquear o dispositivo quando o cartão ?SIM? for substituído;
m) Capacidade de configurar White e blacklist de aplicativos;
n) Capacidade de localizar o dispositivo quando necessário;
o) Permitir atualização das definições quando estiver em roaming;
p) Capacidade de selecionar endereço do servidor para buscar a definição de vírus;
q) Deve permitir verificar somente arquivos executáveis;
r) Deve ter a capacidade de desinfectar o arquivo se possível;
s) Capacidade de agendar uma verificação;

t) Capacidade de enviar URL de instalação por e-mail;
u) Capacidade de fazer a instalação através de um link QRCode;
v) Capacidade de executar as seguintes ações caso a desinfecção falhe:

v.1) Deletar;
v.2) Ignorar;
v.3) Quarentena;
v.4) Perguntar ao usuário.

2. Compatibilidade:

a) Apple iOS 9.0-10.3 ou superior;
b) Android 4.1 ? 7.1.1 ou superior;

ITEM 2: AQUISIÇÃO DE LICENÇAS DO ANTIMALWARE EM AMBIENTE FÍSICO E VIRTUALIZADO

SERVIDOR DE ADMINISTRAÇÃO E CONSOLE ADMINISTRATIVA

1. **Requerimentos Gerais**

a) O software de segurança para ambientes virtuais deve incluir:
a.1) Software AntiMalware sem agente para ambientes virtuais;
a.2) Software AntiMalware baseado em agente para ambientes virtuais;
a.3) Gerenciamento, monitoramento e atualização de software e vacinas centralizados;
a.4) Capacidade de atualizar definições de vírus e padrões de ataques;
a.5) Documentação do administrador;
a.6) Compatibilidade com a rede a ser protegida.

2. Requerimentos para o AntiMalware sem agente:

a) O software de AntiMalware sem agente para ambientes virtualizados deve funcionar com as seguintes versões do VMWARE:

a.1) VMWARE ESXi Hypervisor 6.0 update 2;
a.2) VMWARE ESXi Hypervisor 5.5 update 3b;
a.3) VMWARE NSX para Vsphere 6.2.4;
a.4) VMWARE vCenter 6.0.0a Server ou superior;
a.5) VMWARE vCenter 6.0 Update 2 ou superior;
a.6) VMWARE vCenter 5.5. update 3e;
a.7) VMWARE vShield Endpoint do VMware vCloud Networking and Security 5.5.4.3 suite;
a.8) VMWARE vShield Manager do VMware vCloud Networking and Secruity 5.5.4.3 suite;

b) Requerimentos para o componente de integração ao Servidor:

b.1) Windows Server 2016 Datacenter / Standard x64 ou superior;
b.2) Windows Server 2012 R2 Datacenter / Standard x64;
b.3) Windows Server 2012 R2 Essentials x64;
b.4) Windows Server 2012 Datacenter x64;
b.5) Windows Server 2012 Essentials x64;
b.6) Windows Server 2008 R2 Datacenter / Enterprise / Standard Service Pack 1 x64;
b.7) b.7) Windows Server 2008 Datacenter / Enterprise / Standard Service Pack 2 x86 e x64;

c) Software de AntiMalware sem agente para ambientes virtuais deve proteger os seguintes sistemas operacionais para desktops:

c.1) Windows 10 32/64 bits ou superior;
c.2) Windows 11 todas as edições.

d) Software de AntiMalware sem agente para ambientes virtuais deve proteger os seguintes sistemas operacionais para servidores:

d.1) Windows Server 2008 R2 (x64);
d.2) Windows Server 2012 R2;
d.3) Windows Server 2012 sem ReFS (Resilient File system) suporte (x64);
d.4) Windows Server 2012 R2 (x64) quando utilizado com o VMware vSphere 5.5 update 2 ou posterior;
d.5) Windows Server 2016 Datacenter x64 ou superior;

3. O AntiMalware sem agente para ambientes virtuais deve prover as seguintes funcionalidades:

a) Proteção contra malware em tempo real e durante a verificação agendada sem a necessidade de qualquer agente instalado no computador convidado;
b) Integração com a tecnologia Vmware vShield Manager para proteger o sistema de arquivos do computador;
c) Integração com a tecnologia Vmware Network Extensibility SDK para prover proteção no nível de rede, implementado para monitorar e bloquear atividade maliciosa na rede bem como endereços de URL com a habilidade de notificar o usuário sobre os bloqueios efetuados;
d) Possuir integração com Vmware NSX;
e) Deve possuir IPS;
f) Possuir integração com as etiquetas de segurança NSX;
g) Adicionar automaticamente novas máquinas virtuais ao escopo de proteção, sem a necessidade de qualquer instalação adicional;
h) Deve automatizar a instalação se baseando em políticas de segurança identificadas pelo VMware NSX;
i) Fazer scan em máquinas virtuais mesmo desligadas;
j) Verificar os dispositivos removíveis tais como (Pendrive, Cartões, etc);
k) O produto deve permitir parar o scan após x (minutos) da inicialização da verificação;
l) O produto deve ser capaz de ser configurado até três níveis de segurança sendo eles: Recomendado, alto ou baixo;

m) Provê as seguintes opções caso encontre uma ameaça:

m.1) Escolher a ação automaticamente;
m.2) Desinfectar ou bloquear caso a desinfecção falhe;
m.3) Desinfectar ou deletar caso a desinfecção falhe;
m.4) Deletar ou bloquear caso a deleção falhe;
m.5) Bloquear;

n) A solução deve permitir configurar um tamanho máximo de um arquivo para ser verificado. Ex: Caso o arquivo compactado tenha mais de 10 MB não verificar;
o) Permitir configurar o tempo máximo de scan em um arquivo;
p) Verificar os malwares do tipo trojans, auto-dialers, adware, etc;
q) Permitir verificar drives de rede;
r) Permitir verificar todos os arquivos do sistema com a exceção dos arquivos selecionados pelo administrador;
s) Fazer a verificação dos arquivos que possuem somente as extensões definidas pelo administrador;
t) Permitir a criação de exceções por pastas ou arquivos podendo incluir subpastas;
u) Permitir a criação de perfis de políticas diferentes para cada grupo de máquinas virtuais;
v) Possuir a integração com SNMP;
w) Capacidade de bloquear ataques vindos pela rede;
x) Verificar os endereços da web por possíveis ameaças;
y) Permitir a criação de exceções para URLs que não devem ser verificadas;
z) Permitir enviar uma mensagem de bloqueio caso colaborador acesse um site malicioso;
aa) Proteção baseada em nuvem contra novas ameaças, permitindo a aplicação se comunicar com a fabricante do software para poder dar um veredito a um arquivo tanto na proteção em tempo real como na verificação agendada;
bb) Atualizações centralizadas no sistema com a proteção especializada para virtualização sem a necessidade de distribuir atualizações para cada máquina convidada;
cc) Possibilidade de verificação sob demanda ou manual nas máquinas virtuais selecionadas;
dd) Verificação de: arquivos selecionados, pastas ou todo o sistema na verificação agendada de todas as máquinas virtuais;
ee) Capacidade de implementar a solução de segurança sem a necessidade de reiniciar o Hypervisor ou entrar no modo de manutenção; ff) Tecnologia que previne a verificação do mesmo arquivo mais de uma vez;
gg) Prevenir múltipla verificação em arquivos iguais mesmo que estejam em máquinas virtuais diferentes; hh) Bloquear, isolar e remover os vírus notificando o usuário e o administrador;
ii) Possuir uma única console de gerenciamento para todos os componentes de proteção;
jj) Uma única console de gerenciamento tanto para o ambiente virtual como para o ambiente físico;
kk) Capacidade de ver a estrutura de administração tanto física como lógica assim como é apresentado no Vmware vCenter;
ll) Informações detalhadas sobre os eventos e tarefas de implementação nas máquinas virtuais;

mm) Capacidade de aplicar configurações de segurança diferentes para cada grupo de máquinas virtuais;
nn) Criar exceções pelo nome do arquivo, pelo endereço dos arquivos e pela máscara dos arquivos;
oo) Permitir exportar e importar listas com exceções;
pp) Criar listas com exceções frequentes de acordo com as recomendações da Microsoft;
qq) Permitir verificar drives de rede conectados na máquina virtual se necessário;
rr) Capacidade de excluir drives de rede do escopo de proteção;
ss) Suporta o Vmware vMotion, se uma máquina é transferida de um ESXi para outro a proteção não é interrompida; tt) Criar backup de arquivos deletados pela proteção;
uu) Suportar esquema de licenciamento pela quantidade de máquinas virtuais protegidas e de acordo com o número de CPU cores;
vv) Componente dedicado para integração centralizada com o ambiente virtual para evitar carga no Vmware vCenter e impedir chamadas de soluções de AntiMalware; ww) Suporte para ativar o software utilizando um código sob subscrição; xx) Providenciar informações sobre números de objetos verificados; yy) Providenciar informações sobre detalhes da definição de AntiMalware;
zz) Suportar verificação de certificados SSL para comunicação entre o mecanismo de antimalware, servidor de gerenciamento e Componentes de infraestrutura do VMware;
aaa) Importar ou exportar a lista de exclusões e verificações nas tarefas de verificação e perfis de proteção.

4. Requerimentos para AntiMalware em ambientes virtualizados baseado em agente (conector);

a) Para ser instalado em uma infraestrutura virtualizada, um dos seguintes hypervisors devem ser instalados:

a.1) Vmware ESXi 5.1 com os últimos updates;
a.2) Vmware ESXi 5.5 com os últimos updates;
a.3) Vmware ESXi 6.0 com os últimos updates;
a.4) Vmware ESXi 6.5 com os últimos updates;
a.5) Vmware vCenter 5.1, 5.5, 6.0 ou 6.5 com todos os patches instalados;
a.6) Microsoft Windows Server 2012 R2 Hyper-V (no modo instalação completa ou modo core) com todos os updates disponíveis;
a.7) Microsoft Windows Server 2016 Hyper-V (no modo instalação completa ou core) com todos os updates disponíveis;
a.8) Citrix XenServer 6.5 SP1;
a.9) Citrix XenServer 7;
a.10) Citrix XenDesktop 7.9 ou 7.11;
a.11) Citrix Provisioning Services 7.9 ou 7.11;
a.12) Vmware Orizon View 7
a.13) KVM (Kernel-based Virtual Machine) executando sistema operacional Ubuntu Server 14.04 LTS;
a.14) KVM CentOS 7.2;
a.15) Red Hat Enterprise Linux Server 7 patch 1

b) O AntiMalware baseado em agente deve prover proteção para as máquinas virtuais no Vmware hypervisor nos seguintes sistemas operacionais para Desktop:

b.1) Windows 10 Pro/Enterprise/Enterprise LTSB/RS1 x86/x64;
b.2) Windows 11 todas as edições.

c) O AntiMalware baseado em agente deve prover proteção para máquinas virtuais no Vmware Hypervisor com os seguintes sistemas operacionais para servidores:

c.1) Windows Server 2008 Service Pack 2 Todas edições x64;
c.2) Windows Server 2008 R2 SP1 Todas edições x64;
c.3) Windows Server 2012 R2 Todas edições (X64);
c.4) Windows Server 2012 Todas edições (x64);
c.5) Windows Server 2016 todas edições x64.

d) A Suite VMware tools deve ser instalada para prover integração entre o Hypervisor, máquinas virtuais e o conector;

e) O AntiMalware baseado em agente deve prover proteção para máquinas virtuais no Microsoft Hyper-V Hypervisor com os seguintes sistemas operacionais para Desktop;

e.1) Windows 10 Pro/Enterprise x86/x64;
e.2) Windows 11 todas as edições.

f) O AntiMalware baseado em agente deve prover proteção para máquinas virtuais no Microsoft Hyper-V Hypervisor com os seguintes sistemas operacionais para Servidores;

f.1) Windows Server 2012 R2 x64;
f.2) Windows Server 2012 x64;
f.3) Windows Server 2008 R2 todas edições SP1 x64;
f.4) Windows Server 2008 SP2 Todas edições;
f.5) Windows Server 2016 Todas edições x64.
f.6) Um serviço de integração deve ser instalado na máquina virtual executada pelo Microsoft Hyper-V

g) O AntiMalware baseado em agente deve prover proteção para máquinas virtuais no Citrix Hypervisor com os seguintes sistemas operacionais para Desktop:

g.1) Microsoft Windows 10 Pro/Enterprise x86/x64;
g.2) Microsoft Windows 11 todas as edições.

h) O AntiMalware baseado em agente deve prover proteção para máquinas virtuais no Citrix Hypervisor com os seguintes sistemas operacionais para Servidores;

h.1) Windows Server 2012 R2 x64;
h.2) Windows Server 2012 x64;
h.3) Windows Server 2008 R2 Todas edições SP1 x64;
h.4) Windows Server 2016 Todas edições x64;

i) O AntiMalware baseado em agente deve suportar a proteção das seguintes máquinas virtuais Linux:

i.1) Debian GNU/Linux 8.5 32/64 bits;
i.2) Ubuntu Server 14.04 LTS 32/64 bits;
i.3) Ubuntu Server 16.04 LTS x64;
i.4) CentOS 6.8 x64;
i.5) CentOS 7.2 x64;
i.6) Red hat Enterprise Linux Server 6.7 x64;
i.7) Red Hat Enterprise Linux Server 7.2 x64;
i.8) SUSE Linux Enterprise Server 12 SP1 x64;

j) O AntiMalware baseado em agente deve ser compatível com as soluções usadas para criar e gerenciar um a infraestrutura de máquinas virtuais VDI:

j.1) Citrix Provisioning Services 7.1;
j.2) Citrix XenDesktop 7.5

k) O AntiMalware baseado em agente deve prover proteção para máquinas virtuais no KVM Hypervisor com os seguintes sistemas operacionais Linux:

k.1) Ubuntu Server 14.04 LTS;
k.2) CentOS 7;

l) O AntiMalware baseado em agente deve prover proteção para máquinas virtuais no KVM com os seguintes sistemas operacionais para servidores:

l.1) Windows Server 2012 R2 x64;
l.2) Windows Server 2012 x64;
l.3) Windows Server 2008 R2 Standard SP1 x64;
l.4) Ubuntu Server 14.04 LTS;
l.5) CentOS 7;

m) O AntiMalware baseado em agente deve prover as funcionalidades abaixo;

m.1) AntiMalware e monitoramento residente;
m.2) Proteção contra rootkits e auto dialers a sites pagos;
m.3) Verificação por heurística para detectar e bloquear malwares desconhecidos;
m.4) Transferir a verificação de malware e as tarefas intensivas para uma única máquina virtual responsável pela proteção;
m.5) Garantir a continuidade da proteção de arquivos durante pequenas indisponibilidades na máquina de proteção logando todas as operações de arquivos nas máquinas protegidas durante o período de indisponibilidade, e faz a verificação automática de todas alterações após a restauração do acesso;
m.6) Proteção baseada em nuvem contra ameaças novas, permitindo a aplicação acessar recursos especializados da fabricante para obter vereditos durante a verificação em tempo real ou agendada;

m.7) Deve atender HIPPA e SOX;
m.8) Proteção de e-mail contra malwares verificando tráfego de entrada e saída nos protocolos IMAP, SMTP, POP3, MAPI e NNTP independente do cliente de e-mail;
m.9) Proteção de tráfego Web: verificação de objetos enviados para os computadores dos usuários via HTTP e FTP, com a possibilidade de adicionar sites confiáveis;
m.10) Bloqueia banners e pop-ups nas páginas web;
m.11) Capacidade de detectar e bloquear sites de phishing;
m.12) Proteção contra ameaças não conhecidas baseadas no comportamento;
m.13) Capacidade de determinar comportamento anômalo de uma aplicação analisando a sequência de execução. Capacidade de reverter operações de malware durante o tratamento do arquivo;
m.14) Capacidade de restringir o privilégio de programas executáveis tal como escrita no registro ou acesso a arquivos e pastas. Detecção automática de nível de detecção baseado na reputação do programa;
m.15) O Firewall deve permitir a criação de regras para pacotes de rede em protocolos específicos (TCP, UDP) e portas;
m.16) Permitir a criação de regras de rede para programas específicos;
m.17) Proteção contra-ataques de hackers utilizando o firewall com IDS/IPS e regras de atividade de rede para as aplicações mais conhecidas;
m.18) Criação de regras especiais para bloquear a instalação e/ou execução de uma aplicação. Deve ter a capacidade de controlar a aplicação utilizando o caminho, metadado, MD5, checksum, e categorias predefinidas de aplicações providenciadas pelo fabricante;
m.19) Não carregar nenhum módulo de segurança na máquina virtual e sim no appliance virtual;
m.20) Permitir a verificação em máquinas linux;
m.21) Deve ser capaz de usar o Microsoft System Center Virtual Machine Manager (SCVMM) para fazer deploy dos appliances virtuais;
m.22) Os virtuais appliances responsáveis pela verificação devem ser baseados em Linux;
m.23) Capacidade de desativar a interface local na inicialização do sistema para diminuir consumo de memória;
m.24) Permitir selecionar a forma de conexão ao appliance virtual de três formas diferentes:

i. Utilizando Multicast;
ii. Selecionando Servidor de integração;
iii. Utilizando uma lista de appliances virtuais

m.25) Deve ser capaz de verificar vírus, worms, trojans, toolkits, adware, autodialers e outros tipos de ameaças em máquinas Linux;
m.26) Deve ser capaz de criar exclusões em máquinas linux por nome ou pasta;
m.27) Capacidade de verificar arquivos por formato ou extensão em máquinas Linux;

m.28) Permitir configurar limite de tempo de verificação em um arquivo tanto para máquinas Linux como Windows;
m.29) Permitir alterar o modo de scan para no mínimo três opções diferentes:

i. Verificação automática;
ii. Verificar os arquivos no acesso ou na modificação;
iii. Somente no acesso;

m.30) Monitorar as atividades de I/O do usuário na utilização de dispositivos externos pelo tipo de dispositivo e/ou BUS usado incluindo a capacidade de criar uma lista de dispositivos confiáveis através do ID;
m.31) Capacidade de garantir privilégios na utilização de dispositivos externos para usuários específicos do AD;
m.32) Monitorar as atividades do usuário na internet incluindo o bloqueio ou a permissão de acesso a certos recursos bem como a capacidade de bloquear certos tipos de informação (audio, video, etc);
m.33) Capacidade de controlar acesso na internet por horário e por usuário do AD;
m.34) Atualizações centralizadas permitindo que parte do banco de dados de definições seja armazenado na máquina de proteção (SVM);
m.35) Habilidade de executar tarefas de detecção de vulnerabilidades em aplicações instaladas nos computadores incluindo opção de submeter um relatório de qualquer vulnerabilidade encontrada;
m.36) Integração com o Windows Update para instalar patches de acordo com as vulnerabilidades encontradas;
m.37) Capacidade de instalar e distribuir remotamente componentes do antivirus em todas as máquinas protegidas sem utilização de ferramentas de terceiros;
m.38) Armazenar as informações de arquivos verificados para evitar um novo scan sobre o arquivo e aumentar consumo de recursos;
m.39) Bloquear, neutralizar e remover os malwares com a opção de notificar os administradores;
m.40) Console de gerenciamento única para todos os componentes de proteção;
m.41) Console de gerenciamento única tanto para ambientes físicos como virtuais;
m.42) Console única para administração de máquinas virtuais Linux e Windows;
m.43) Provê informações detalhadas sobre os eventos e execução de tarefas;
m.44) Capacidade de aplicar configurações de segurança diferentes para cada grupo de máquinas virtuais;
m.45) Salvar o backup dos arquivos deletados;

5. Suporta as seguintes tecnologias Vmware: vMotion, Distributed resource Scheduler;
6. Suporta as seguintes tecnologias Citrix: Virtual User Drive, Citrix Receiver, Multi-stream ICA, XenMotion Live Migration, Automated VM protection and recovery, Dynamic memory control;
7. Suportar as seguintes tecnologias Hyper-V: Live migration, Cluster shared volumes, Dynamic memory, Live backup;
8. Suportar rollback do banco de dados de definições;
9. Suportar o esquema de licença de acordo com o número de máquinas virtuais protegidas e de acordo com o número de hardware CPU cores;

10. Requerimentos para administração centralizada, monitoramento e update do software para ambientes virtualizados:

a) A administração centralizada, monitoramento e atualização de softwares deve funcionar em computadores executando os seguintes sistemas operacionais:

a.1) Microsoft Windows 10 Education RS1;
a.2) Microsoft Windows 10 Education 32/64 bits;
a.3) Microsoft Windows 10 Enterprise RS1 e Professional RS1 32/64 bits;
a.4) Microsoft Windows 10 Enterprise e Professional 32/64 bits;
a.5) Microsoft Windows 11 todas as edições;
a.6) Microsoft Windows Small Business Server 2008 Standard x64;
a.7) Microsoft Windows Small Business Server 2008 Premium x64;
a.8) Microsoft Windows Server 2008 Todas edições 32/64 bits;
a.9) Microsoft Windows Server 2008 R2 Todas edições 32/64 bits;
a.10) Microsoft Windows Server 2012 Todas edições 32/64 bits;
a.11) Microsoft Windows Server 2012 R2 Todas edições 32/64 bits;
a.12) Microsoft Windows Server 2016 x64;

11. Banco de dados Suportados pela console de administração centralizada:
a) Microsoft SQL Server Express 2008;
b) Microsoft SQL Server Express 2008 R2;
c) Microsoft SQL Server Express 2008 R2 Service Pack 2;
d) Microsoft SQL Server 2005;
e) Microsoft SQL Server 2008;
f) Microsoft SQL Server 2008 R2;
g) Microsoft SQL Server 2012;
h) Microsoft SQL Server 2014 Todas as edições x64
i) MySQL Enterprise versions 5.0.67, 5.0.77, 5.0.85, 5.087 Service Pack 1, 5.091;
j) MySQL Enterprise versions 5.0.60 Service Pack 1, 5.0.70, 5.0.82 Service Pack 1, 5.0.90;

12. Requerimentos Console de administração instalada em ambientes virtualizados:

a) Vmware: Workstation 9.x, Workstation 10.x;
b) Microsoft Hyper-V: 2008, 2008 R2, 2012, 2012 R2
c) Microsoft Virtual PC 2007 (6.0.156.0)
d) Parallels Desktop 7;
e) Citrix XenServer 6.1 e 6.2;
f) Oracle VM VirtualBox 4.0.4-70112

13. O console de administração centralizada deve prover as seguintes funcionalidades:

a) Deve ser compatível com Microsoft SCVMM;
b) Capacidade de desativar a interface local do agente (conector) para diminuir uso de memória;
c) Instalação do AntiMalware a partir de uma única distribuição;

d) Seleção de instalação dependendo do número de pontos protegidos;
e) Capacidade de ler informações do AD para obter dados que some com as contas dos computadores na organização;
f) Capacidade de fazer a instalação automática através dos grupos gerenciados;
g) Capacidade de realocar computadores de acordo com endereço IP, tipo do sistema operacional e localização no AD;
h) Instalação centralizada;
i) Remoção centralizada (manual ou automática) de aplicações incompatíveis através do servidor de administração;
j) Capacidade de instalar o AntiMalware de diferentes formas: RPC, GPO, agente de administração;
k) Capacidade de atualizar pacotes de instalação com as últimas atualizações;
l) Atualizar de forma automática a versão do AntiMalware e as definições;
m) Procurar automaticamente por vulnerabilidades nas aplicações e sistemas operacionais presentes da rede;
n) Capacidade de proibir instalação/execução de aplicações;
o) Capacidade de gerenciar I/O de dispositivos externos;
p) Gerenciar a atividade do usuário na internet;
q) Capacidade de testar as atualizações antes de aplicar para o ambiente;
r) Capacidade de executar instalações automáticas baseado no sistema de proteção dedicado, tais como: Vmware ESXi, Microsoft Hyper-V, Citrix XenServer virtualization ou hypervisor;
s) Criar os usuários baseados em RBAC;
t) Criar a hierarquia dos servidores de administração e tem capacidade de gerenciar cada um deles através de uma única console de gerenciamento;

9. TREINAMENTO HANDS-ON DA SOLUÇÃO E SUPORTE - DETALHAMENTO E ESPECIFICAÇÃO

9.1 SERVIDOR DE ADMINISTRAÇÃO E CONSOLE ADMINISTRATIVA

1. A capacitação deverá contemplar, no mínimo, os seguintes tópicos:

a) Criação de pacotes de instalação;
b) Configuração de AntiMalware;
c) Configuração de proteção para arquivos compactados, e-mails navegação e discos removíveis.
d) Gerenciamento centralizado das funções via console;
e) Atualização de softwares e vacinas.
f) Instalação e atualização em ambientes físicos (servidores, estações de trabalho, laptops, smartphones, tablet) e virtuais (servidores);
g) Instalação e atualização em sistemas virtuais e operacionais windows, linux, android, iOS;
h) Criação de pacotes de instalação;

2. O FORNECEDOR deverá transmitir conhecimento à equipe da UTD do SESC-PE, contemplando o uso da solução objeto deste Termo.

3. O treinamento será feito para a equipe técnica da UTD, com vistas a capacitá-los para o uso das funcionalidades da solução, com carga horária de 16 horas, para até 15 (quinze) técnicos, no formato remoto.
4. O instrutor do FORNECEDOR deverá possuir pleno conhecimento no uso de todas as ferramentas que integram a referida solução.
5. O instrutor do FORNECEDOR deverá possuir certificado fornecido por centro de treinamento oficial do Fabricante que o credencie a ministrar a capacitação da solução.

9.1.1 INFORMAÇÕES SOBRE OS TREINAMENTOS

9.1.1.1. Treinamento da solução implementada - Hands-on (para todos os itens constantes na tabela de especificações):

a) A vencedora fica responsável em ofertar treinamento (Hands-on) sobre a instalação, configuração e gerenciamento da solução de antivirus / antimalware, com carga horária mínima de 24hs, a ser realizada na sede do Sesc-DR/PE (podendo ser on-line), utilizando o ambiente da solução ofertada e instalada, provendo este treinamento prático para equipe composta de até 10 (dez) colaboradores indicados pela UTD do Sesc-DR/PE.

a.1) A exigência apresentada na alínea anterior está subordinada ao pedido mínimo (acumulativo) de 1.000 (mil) licenças para o item 01 e uma licença do item 02 do unico lote.
a.2) O treinamento HANDS-ON deverá ocorrer juntamente com a instalação e configuração dos produtos (itens 01 e 02 constantes no item 3 deste Termo de Referência).
a.3) A contratada deverá ser responsável por todos os custos, referente a este treinamento.

9.1.1.2. Treinamento Oficial para o AntiMalware ofertado:

a) A vencedora fica responsável em ofertar treinamento presencial em Centro de Treinamento Oficial do AntiMalware ofertado, para 03 (três) funcionários da UTD do SESC-PE.

a.1) O treinamento deverá ser presencial e possuir o conteúdo programático oficial, contendo no mínimo: instalação e configuração em desktops e servidores; e gerenciamento em servidores.
a.2) O treinamento deverá ter carga horária mínima de 20 (vinte) horas. A Contratada deverá arcar com todo o ônus e custos dos mesmos, tais como material didático, translados, hospedagem, treinamento.
a.3) A exigência apresentada na alínea anterior está subordinada ao pedido mínimo (acumulativo) de 1.500 (hum mil e quinhentas) licenças para o item 01 e 100 (cem) licenças do item 02 do único lote.
a.4) O prazo máximo de realização do treinamento presencial Oficial para o AntiMalware será de até 90 (noventa) dias, contados a partir do Pedido de Compra (PC) que totalize os quantitativos mínimos estabelecidos.

9.2. SUPORTE

SERVIDOR DE ADMINISTRAÇÃO E CONSOLE ADMINISTRATIVA

Nível 1: Serviços indisponíveis

a) Interrupção de serviços ou rede inoperante causado por vírus;
b) Epidemia de vírus por toda a rede;
c) Serviços críticos gravemente afetados;
d) Servidores que não estão se comunicando com a console de gerenciamento;

Nível 2: Serviços parcialmente indisponíveis
a) Detecção de falsos positivos que afetam serviços críticos;
b) Suporte para upgrade de versões e releases do software;

Nível 3: Serviços disponíveis com ocorrência de falhas ou alertas
a) Máquinas que não estão se comunicando com a console de gerenciamento;
b) Análise e correção de eventos relacionados à segurança e à performance do software e do ambiente;
c) O suporte inicial se dará de forma remota, em casos mais graves que o suporte remoto não seja suficiente, será realizado o atendimento de forma presencial.

ITEM 3: KASPERSKY MANAGED DETECTION AND RESPONSE BRAZILIAN EDITION

a. Detecção e Resposta Gerenciada

a.1. Do monitoramento, identificação e investigação dos eventos de segurança cibernética

a.1.1. O serviço de monitoramento deverá utilizar informações extraídas de registros gerados pelos sistemas monitorados.
a.1.2. Deverá ser instalado agentes específicos nos servidores e desktops, objetivando coletar informações mais detalhadas para o serviço de monitoramento, desde que seja plenamente compatível com o sistema onde será instalado e não afete o desempenho dos serviços.
a.1.3. A análise das informações correlacionadas deve ser realizada com auxílio de bases globais de inteligência cibernética em conjunto com a expertise dos profissionais do fabricante, com vistas a reduzir ao máximo os falsos positivos.
a.1.4. É obrigatório que a comunicação entre equipamentos e soluções do fabricante instalados nos dispositivos e qualquer infraestrutura onde esses dados sejam processados ocorra de forma segura, utilizando algoritmos criptográficos para preservar o sigilo das informações.
a.1.5. Deverá ser feita a investigação e a classificação dos eventos monitorados, aplicando os principais frameworks de gestão de incidentes de segurança cibernética bem como boas práticas de mercado na detecção e triagem dos eventos de segurança, objetivando minimizar a presença de falsos positivos na abertura de incidentes de segurança.
a.1.6. O serviço de monitoramento deverá ser capaz de coletar e realizar a correlação de eventos dos sistemas e ativos monitorados, permitindo uma visão mais abrangente do alcance das ações maliciosas, bem como de possível movimentação lateral do atacante dentro da rede.
a.1.7. O monitoramento deverá ser capaz de identificar as principais ameaças, bem como táticas, técnicas e procedimentos de ataque descritos na base de conhecimento MITRE ATT&CK, sem prejuízo do uso de outras

bases de conhecimento ou serviços de inteligência de ameaças, para complementação da capacidade de identificação de atividades maliciosas.
a.1.8. Deverá monitorar e avaliar criticamente os serviços, traçando curvas de comportamento, definindo a volumetria média e identificando comportamentos anômalos, visando antecipar a identificação de incidentes de segurança.
a.1.9. A solução deverá prover inteligência de proteção contra ataques cibernéticos a nível global, sendo responsável por pesquisar novos tipos de ataques, vírus, malwares, botnets, vulnerabilidades e afins com intuito de melhoria contínua de detecção e mitigação destes males dentro dos serviços e ativos de segurança monitorados.
a.1.10. O fabricante deverá utilizar solução para registro de incidente de segurança, acessível pela equipe técnica do GERENCIDOR, para indicar ações de contenção, comunicar à equipe do GERENCIADOR sobre o andamento do tratamento dos incidentes.

b. Compatibilidade:

b.2. É suportada por qualquer um dos seguintes navegadores:

b.2.1. Apple Safari versões mais recentes
b.2.2. Google Chrome versões mais recentes
b.2.3. Microsoft Edge
b.2.4. Mozilla Firefox versões mais recentes

c. Requisitos de rede:

c.1. Em condições médias de carga: um canal full-duplex com largura de banda de pelo menos 1,7 Kbps para cada ativo.
c.2. Em condições de carga máxima: um canal full-duplex com largura de banda de pelo menos 2,7 Kbps para cada ativo.
c.3. Compatibilidade de sensor de endpoint
c.4. O agente de endpoint deve ser compatível com os seguintes sistemas operacionais, para no mínimo a coleta e envio dos dados/telemetria ao SOC do fabricante:
c.5. Microsoft Windows 7 e superiores;
c.6. macOS 10.14-11;
c.7. CentOS 6.7 ou superior;
c.8. Debian GNU / Linux 9.4 ou superior;
c.9. Linux Mint 19 ou superior;
c.10. Oracle Linux 7.3 ou superior;
c.11. Red Hat Enterprise Linux 6.7 ou superior;
c.12. SUSE Linux Enterprise Server 12 SP5 ou superior;
c.13. Ubuntu 18.04 LTS ou superior.

d. **Capacidades técnicas**

d.1. Deve possuir console web própria do serviço, além de integração nativa com a console do "software de segurança e antivírus para servidores físicos, microcomputadores e smartphones/tablets"
d.2. A console deve possuir dashboards com as informações principais, apresentando no mínimo:
d.3. Número de incidentes e status
d.4. Quantidade de dispositivos monitorados
d.5. Deve possuir mecanismo de notificações, com no mínimo as seguintes opções:
d.6. E-mail
d.7. Telegram
d.8. Deve permitir o envio de relatórios.
d.9. O agente deve enviar a telemetria em tempo real para o SoC do fabricante;
d.10. O serviço deve compreender monitoramento dos dados enviados e alertas gerados em um regime 24x7x365.
d.11. O envio e armazenamento da telemetria, devem respeitar as principais legislações de proteção de dados, como GDPR e LGPD.
d.12. O SoC do fabricante deve possuir datacenters em pelo menos duas localidades em diferentes países.
d.13. O SoC do fabricante deve possuir equipes de analistas em pelo menos 3 regiões (países) incluindo Brasil.
d.14. Os dados coletados devem passar por no mínimo:
d.15. Modelos de Machine Learning/Inteligência Artificial;

e. Análise humana;

e.1. Correlação com IoA's (indicadore de ataque);
e.2. Emulação em sandbox (quando necessário);
e.3. Após análise, informações sobre atividades potencialmente maliciosas, devem ser apresentadas no portal como "Incidentes"
e.4. O Incidente deve possuir no mínimo as seguintes informações:
e.5. Resumo
e.6. Prioridade (Baixa, Média e Alta)
e.7. Recomendação
e.8. Data de criação e data de atualização
e.9. Correlacionamento com táticas/técnicas do Framewok MITRE ATT&CK
e.10. Dispositivos afetados
e.11. IoC's de host e de rede
e.12. Descrição completa em linha do tempo

f. **O incidente pode receber ações de resposta recomendada disparadas pela equipe de SoC, compreendendo no mínimo as seguintes ações:**

f.1. Transferir arquivo para o SoC;
f.2. Isolar um dispositivo;
f.3. Desabilitar isolamento de dispositivo;
f.4. Deletar chave de registro;
f.5. Dump de memória;

f.6. As ações devem ser aprovadas no portal por profissional do gerenciador, com a opção de habilitar aprovação automática.
f.7. Deve possuir console mult-tenant com a possibilidade de separar ativos.
f.8. Deve possuir campos para o mult-tenant para melhor visualização: f.9. Name;
f.10. Status;
f.11. Descrição;
f.12. Criado em;
f.13. Agente de endpoint

g. **As funcionalidades relacionadas a detecção e resposta solicitadas nesse item, devem ser operadas na mesma console de gerenciamento da solução de endpoint;**

g1. A solução deve oferecer módulo focado em capacidades de EDR "Endpoint Detection and Response", incluindo no mínimo as seguintes capacidades:
g2. O agente deve ter capacidade de coletar e processar dados relacionadas ao veredito e ao contexto da ameaça;
g3. Deve fornecer graficamente a visualização da cadeia do ataque;
g4. Deve possuir a capacidade de varredura, para identificar a presença de um artefato detectado em outros dispositivos na rede, através de indicadores de comprometimento (IoC).
g5. A varredura deve oferecer opções de resposta automatizada (sem intervenção do administrador), para serem executadas caso o IoC seja encontrado em outro dispositivo, com no mínimo as seguintes opções:

- Isolar o host;
- Iniciar uma varredura nas áreas críticas;
- Quarentenar o objeto;

h. **A solução deve criar um report detalhado sobre o incidente, tendo a capacidade de incluir no mínimo os seguintes dados:**

h.1. Detecções provenientes da solução de endpoint;
h.2. Processos;
h.3. Alterações de registro;
h.4. Conexões remotas;
h.5. Criação de arquivos;
h.6. Varredura por todos os dispositivos executada a partir de indicador de comprometimento (IoC) gerado através da solução e importado pelo administrador.
h.7. Possibilidade de exportar os indicadores de comprometimento (IoC) gerados a partir da solução.

i. **A solução deve oferecer no mínimo as seguintes opções de resposta:**

i.1. Prevenir a execução de um arquivo;
i.2. Quarentenar um arquivo;
i.3. Iniciar uma varredura por IoC;
i.4. Parar um processo;

i.5. Executar um processo;

j. **Ferramenta que possibilite o isolamento do host infectado com no mínimo as características abaixo:**

j.1. A opção de isolamento deve estar disponível junto a visualização do incidente;
j.2. Na configuração padrão, o isolamento deve ser feito de forma granular, permitindo o controle do dispositivo pela console administrativa mesmo após ativação da regra;

10. AVALIAÇÃO DA QUALIDADE E TERMO DE ACEITE

O Gerenciamento Técnico da Ata será de responsabilidade da equipe de fiscalização da Ata designada pelo GERENCIADOR, que estará acompanhando e avaliando a execução dos serviços prestados pelo FORNECEDOR. Será utilizada como metodologia de avaliação da qualidade e aceite dos serviços o cumprimento a todas as exigências, obrigações e especificações descritas neste Termo de referência e demais anexos e conteúdos que integrarem o Edital, durante a execução da Ata. O recebimento provisório ou definitivo não exclui a responsabilidade civil, nem a ético-profissional pela perfeita execução da Ata, dentro dos limites estabelecidos pela lei.

11. EXECUÇÃO DAS ATIVIDADES

O início da execução dos serviços deverá ser realizado mediante a emissão do PC. Serão emitidas solicitações para as atividades de TREINAMENTO. O envio das solicitações será realizada pelo Gestor da Ata, por meio dos instrumentos formais de comunicação.

A obrigação de execução dos serviços por parte do FORNECEDOR iniciará declarada na autorização de fornecimento ou documento equivalente. O FORNECEDOR deverá apresentar justificativa prévia e formal sobre eventuais atrasos ou paralisação dos serviços, cabendo ao Gestor acatar ou não a justificativa. A fiscalização promoverá a avaliação da qualidade dos serviços realizados e justificativas, de acordo com os Critérios de Aceitação e demais requisitos definidos neste Termo de Referência.

12. MANUTENÇÃO DE SIGILO E NORMAS DE SEGURANÇA

O FORNECEDOR deverá manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse do GERENCIADOR ou de terceiros de que tomar conhecimento em razão da execução da Ata, respeitando todos os critérios estabelecidos, aplicáveis aos dados, informações, documentos, entre outros pertinentes.

O FORNECEDOR deverá manter sigilo absoluto sobre quaisquer dados e informações, que venha a ter conhecimento durante a prestação dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo GERENCIADOR a tais documentos.

13. OBRIGAÇÕES DO GERENCIADOR

a) Acompanhar e fiscalizar a execução da Ata, atestar as notas fiscais/faturas relativo à entrega do objeto e o seu aceite.
b) Efetuar o pagamento ao FORNECEDOR de acordo com o preço, os prazos e as condições estipuladas na Ata.
c) Rejeitar, no todo ou em parte, serviço ou fornecimento realizado em desacordo com o Termo de Referência.
d) Informar ao FORNECEDOR toda e qualquer irregularidade constatada na execução do objeto, ou problemas que venham a interferir, direta ou indiretamente, na execução da Ata.
e) Providenciar o acesso do FORNECEDOR aos locais necessários para o levantamento das informações que a execução dos serviços requeira.
f) Permitir o acesso dos técnicos da empresa FORNECEDORA, para execução dos serviços previstos, desde que previamente identificados e credenciados, assim como acompanhá-los na execução dos serviços quando ocorrer in loco.
g) Assegurar que os preços contratados estão compatíveis com aqueles praticados no mercado.
h) Serão permitidas subcontratações desde que haja autorização/anuência do gerenciador;
i) Documentar as ocorrências decorrentes de sua fiscalização, verificar o cumprimento das obrigações da Empresa Fornecedora, aplicando-lhe as penalidades cabíveis quando do descumprimento daquelas, ressalvados os casos de força maior, justificados e aceitos pela Administração;
j) Proporcionar todas as condições e prestar as informações necessárias para que o FORNECEDOR possa cumprir com suas obrigações, dentro das normas e condições contratuais.
k) Registrar e oficializar ao FORNECEDOR, as ocorrências de desempenho ou comportamento insatisfatório, irregularidades, falhas, insuficiências, erros e omissões constatados, durante a execução da Ata, para as devidas providências.

14. OBRIGAÇÕES DO FORNECEDOR

a) Executar fielmente a Ata, de acordo com as cláusulas avençadas. A ação ou omissão, total ou parcial do GERENCIADOR não eximirá o FORNECEDOR de total responsabilidade quanto à execução dos serviços.

b) Fornecer o objeto deste Termo de Referência dentro dos padrões e requisitos estabelecidos e realizar entrega dos itens, estritamente de acordo com as especificações.

c) Manter, durante toda a execução da Ata, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na contratação.

d) Assumir a responsabilidade por todos os encargos previdenciários e obrigações sociais previstos na legislação social e trabalhista em vigor, obrigando-se a saudá-los na época própria, uma vez que os seus empregados não manterão nenhum vínculo empregatício com o GERENCIADOR.

e) Assumir a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho, quando, em ocorrência da espécie, forem vítimas os seus empregados quando da execução do serviço ou em conexão com ele, ainda que acontecido em dependência do GERENCIADOR, inclusive por danos causados a terceiros.

f) Assumir todos os encargos de possível demanda trabalhista, cível ou penal, relacionados à execução do serviço, originariamente ou vinculada por prevenção, conexão ou contingência, incluindo atendimento às normas regulamentadoras da Medicina e Segurança do Trabalho.

g) Promover a execução do serviço dentro dos parâmetros e rotinas estabelecidos, em observância às normas legais e regulamentares aplicáveis e às recomendações aceitas pela boa técnica.

h) Responder integralmente pelos danos causados, direta ou indiretamente, ao patrimônio da União em decorrência de ação ou omissão de seus empregados ou prepostos, não se excluindo ou reduzindo essa responsabilidade em razão da fiscalização ou do acompanhamento realizado pelo GERENCIADOR.

i) Providenciar que seus empregados portem crachá de identificação quando da execução do serviço em ambiente do GERENCIADOR.

j) Atender às solicitações do GERENCIADOR, por intermédio de funcionários ou técnicos por ele credenciados, relacionados com a execução dos serviços.

k) Comunicar ao GERENCIADOR qualquer ocorrência que venha a interferir na execução dos serviços.

l) Respeitar, durante a execução dos serviços, todas as leis, normas e posturas Federais, Estaduais, Distritais e Municipais pertinentes e vigentes.

m) Atender às solicitações do GERENCIADOR, de acordo com as especificações técnicas, procedimentos de controle administrativo e cronogramas físicos que venham a ser estabelecidos, ou quaisquer outras solicitações inerentes ao objeto da Ata.

n) Facilitar à equipe de fiscalização o pleno exercício de suas funções, prestando-lhe todos os esclarecimentos e informações administrativas e/ou técnicas que lhe forem solicitadas, exibindo-lhe todos os documentos e dados de interesse para acompanhamento e fiscalização da execução do instrumento contratual ou instrumento equivalente.

o) O exercício das funções da equipe de fiscalização não desobriga o FORNECEDOR de sua própria responsabilidade, quanto à adequada, pronta e fiel execução do objeto contratado.

p) Ter pleno conhecimento de todas as condições e peculiaridades inerentes ao objeto não podendo invocar posteriormente desconhecimento para cobrança de serviços extras.

q) Proibir a veiculação de publicidade ou qualquer outra informação acerca do objeto da Ata, salvo se houver prévia autorização da Administração do GERENCIADOR.

r) Executar os serviços por intermédio de profissionais qualificados, com experiência e conhecimento compatíveis com os serviços a serem realizados.

s) O FORNECEDOR é responsável por realizar a supervisão e acompanhamento da qualidade e dos níveis de serviço alcançados com vistas a efetuar eventuais ajustes e correções para o atendimento dos níveis de serviço.

t) Durante a fase da execução do serviço a interrupção na prestação do serviço, em desacordo com a Ata, sujeita o FORNECEDOR às penalidades previstas no Edital e seus anexos, salvo por motivo formalmente encaminhado ao GERENCIADOR, justificado e aceito por esta.

u) Se o GERENCIADOR houver disponibilizado recursos (documentos, equipamentos ou outros) ao FORNECEDOR, estes deverão ser devolvidos ao GERENCIADOR durante a transição contratual.

v) O FORNECEDOR deverá reparar, corrigir, remover ou reconstruir, às suas expensas, no total ou em parte, os serviços efetuados referentes ao objeto em que se verifiquem vícios, defeitos ou incorreções resultantes da execução, ou ainda aqueles que não satisfaçam aos níveis de qualidade previstos.

w) Solicitar, previamente e formalmente, autorização à equipe de fiscalização sempre que necessitar executar atividades especiais ou não previstas.

x) Cumprir todas as obrigações e exigências previstas no Termo de Referência e em seus anexos.

y) Não é permitido a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos; nem a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre.

z) Os serviços excepcionais realizados em horário noturno, e aos sábados, domingos e feriados no ambiente do GERENCIADOR ou do FORNECEDOR não implicarão em nenhuma forma de acréscimo ou majoração nos valores dos serviços e produtos, razão pela qual será improcedente a reivindicação de restabelecimento de equilíbrio econômico-financeiro.

aa) O representante do FORNECEDOR deverá apresentar, na reunião inicial, carta de formalização do PREPOSTO, contendo indicação de nome e contato do funcionário que exercerá as atividades de preposto do FORNECEDOR, no âmbito da Ata.

bb) Prestar todos os esclarecimentos que forem solicitados pela fiscalização do GERENCIADOR acerca da situação dos serviços contratados, em até 8 (oito) horas úteis, a contar do encaminhamento formal do pedido.

cc) Deverão ser entregues junto com a solução de AntiMalware:

cc.1) Todos os manuais necessários à instalação do software de AntiMalware e seus componentes em mídia digital;
cc.2) Todas as licenças de utilização definitivas para os softwares fornecidos, em suas últimas versões disponíveis considerando a data de entrega do software, em nome do SESC PERNAMBUCO. As licenças do software deverão ser ofertadas na modalidade de licenciamento perpétua;

dd) O FORNECEDOR deverá possibilitar a conferência das características da Solução descrita neste Termo, através dos canais de comercialização do fabricante no Brasil (site, folder, dentre outros meios).

15. QUALIFICAÇÃO TÉCNICA

Para Habilitação:

Apresentação de Atestados(s) de capacidade técnica, conforme a seguir:

a) Comprovação de capacidade técnico-operacional: pelo menos 01 (um) atestado em nome da licitante, fornecido por pessoa jurídica de direito público ou privado, para desempenho de atividade pertinente e compatível com o objeto da licitação.

a.1) O(s) atestado(s) deverá(ão) ser apresentado(s) constando as seguintes informações da emitente: papel timbrado, CNPJ, endereço, telefone, data de emissão, nome e cargo/função de quem assina o documento, bem como conter objeto, atividades desenvolvidas e período da contratação.

a.2) Não serão aceitos atestados emitidos por empresas do mesmo grupo empresarial da Concorrente ou pela própria Concorrente e/ou emitidos por empresas, das quais participem sócios ou diretores da Concorrente.

16. CRITÉRIOS PARA ASSINATURA DA ATA DE REGISTRO DE PREÇOS

Como critério de adjudicação de proposta, a licitante deverá apresentar, as exigências constantes nas tabelas abaixo:

ITEM	EXIGÊNCIA (CONFORME TABELA LEGENDA DO CAMPO EXIGÊNCIA)
01	A, B, C
02	A, B, C

LEGENDA DO CAMPO EXIGÊNCIA	
A	Comprovação através de Carta do Fabricante (nominal ao processo) que sua empresa é revenda/distribuidor autorizado a comercializar os produtos;
B	Declaração do fabricante comprovando que possui em seu quadro funcional ao menos um profissional autorizado e com capacitação técnica para realizar treinamentos oficiais de implantação, configuração e operação da solução ofertada
C	Declaração do fabricante garantindo que o produto terá atualização e suporte pelo período mínimo de 36 (trinta e seis) meses

17. FISCALIZAÇÃO

A fiscalização da Ata será realizada pela equipe técnica a ser designada pela UTD – Unidade de Tecnologia Digital do SESC PERNAMBUCO.

O GERENCIADOR designará uma comissão de servidores para acompanhamento e fiscalização da execução do objeto deste Termo de Referência, que registrará, em relatório, todas as ocorrências relacionadas com sua execução, determinando o que for necessário à regularização das falhas ou defeitos observados, bem como a emissão de documentos de atesto, validações e aprovações;

Os esclarecimentos solicitados pela fiscalização deverão ser prestados imediatamente, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de 8 (oito) horas úteis;

18. FORMA DE PAGAMENTO

O pagamento será realizado pela unidade de suprimentos, em até 30 (trinta) dias úteis, contados a partir do recebimento definitivo do objeto, mediante a apresentação dos documentos fiscais legalmente exigíveis e devidamente atestados pelo servidor/comissão de recebimento.

19. ELABORAÇÃO DO TERMO DE REFERÊNCIA

São responsáveis pela elaboração deste Termo de Referência: DIEGO LILIOSO VIEIRA DE LUCENA E ANSELMO WILLIAM BRAZ, ambos da Unidade de Tecnologia Digital.

Diego Lilioso
Gerente da GEINF
SESC ADM. REGIONAL - PE

Diego Lilioso

Anselmo William Braz
COORDENADOR
DA GEINF
SESC ADM. REGIONAL - PE

Anselmo William Braz