Dispensas de Licitações

CAIRU
PREFEITURA MUNICIPAL

SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO

AVISO DE INTENÇÃO DE DISPENSA DE LICITAÇÃO Nº 014/2023

Nos termos do §3º do Art. 75 da Lei n. 14.133/2021, o **Município de Cairu,** Estado da Bahia, inscrito no CNPJ sob o n.º 14.235.907/0001-44, sito à Praça Marechal Deodoro, nº. 03, Centro, representado neste ato pelo Secretário, Senhor **ÂNGELO CÉSAR SANTIAGO FAHNING**, torna público o interesse da Secretaria Municipal de Administração na contratação de pessoas jurídicas objetivando a aquisição de 200 (duzentas) licenças do software Kaspersky Endpoint Security Corporativo, incluindo atualizações, garantia e suporte técnico pelo período de 24 (vinte quatro) meses para atender a demanda de segurança da informação, das diversas Secretarias do Município de Cairu, Arquipélago de Tinharé, no valor global de **R$ 31.478,00 (trinta e um mil quatrocentos e setenta e oito reais),** conforme planilha a seguir, podendo eventuais interessados apresentar proposta de preço no prazo de três dias úteis a contar desta publicação (acompanhada pela documentação elencada no item REQUISITOS DA CONTRATAÇÃO no Termo de Referência anexo), oportunidade em que a Administração escolherá a mais vantajosa.

Limite para apresentação da Proposta de Preços: **19/10/2023.**

O termo de referência da dispensa encontra-se anexo a este aviso.

A proposta deverá ser entregue na Diretoria de Compras, Contratos e Licitações, situada no Complexo Administrativo Diogo Magalhães Brandão - Praça Marechal Deodoro, nº 03, Centro, nesta cidade de Cairu – Bahia, CEP 45.420-000 das 8h às 17h, ou pelo email: licitacao@cairu.ba.gov.br até às 23:59h.

ITEM	ESPECIFICAÇÃO	UND	VLR. UNIT.	VLR. TOTAL
01	Fornecimento de licenças de uso do software de antivírus Kaspersky Endpoint Security For Business - ADVANCED, com suporte técnico, por 24 (vinte e quatro) meses.	200	R$ 157,39	R$ 31.478,00

Cairu - Bahia, 16 de outubro de 2023.

ÂNGELO CÉSAR SANTIAGO FAHNING
Secretário Municipal de Administração

CAIRU
PREFEITURA MUNICIPAL

SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO

TERMO DE REFERÊNCIA

1. OBJETO - Constitui presente termo a aquisição de 200 (duzentas) licenças do software Kaspersky Endpoint Security Corporativo, incluindo atualizações, garantia e suporte técnico pelo período de 24 (vinte quatro) meses para atender a demanda de segurança da informação, das diversas Secretarias do Município de Cairu, Arquipélago de Tinharé.

2. MOTIVAÇÃO / JUSTIFICATIVA - O Município possui um ambiente computacional formado por uma rede constituída por computadores de mesa (desktop) e notebook instalados nas diversas localidades (Boipeba, Gamboa, Morro de São Paulo e demais distritos) todos interconectados e à disposição nas diversas Secretarias Municipais, Escolas, Centros de Convivência, Unidade de Saúde entre outros ambientes.

Dispõe ainda de um Date Center constituído por 07 (sete) servidores (supercomputadores) responsáveis por diversos serviços necessários para a realização das atividades da administração pública municipal onde são gerados, trafegados e armazenados.

Em razão do conjunto de informações importantíssimas, atreladas a um sistema de informação que inclui vários sistemas como o de Recursos Humanos, Contabilidade, Arrecadação Municipal, movimentações bancárias e acesso à Rede Mundial de Computadores (Internet). Uma estrutura computacional que é essencial e obrigatório a implementação de medidas de segurança.

É fato que a vulnerabilidade das informações se tornou factível a qualquer rede que esteja conectada à Internet. Assim sendo, torna-se imprescindível desenvolver uma política de segurança, em virtude das valiosas informações trafegadas e armazenadas na rede de Computadores da Prefeitura de Cairu.

Baseado nestes fatos e cientes das consequências que podem advir à rede do Município, faz-se necessária a implementação de um sistema de proteção dos equipamentos servidores e estações de trabalho contra os vírus, *worms, Trojans, Rootkits e spywares e filtro de conteúdo web* que atue de forma simples, eficaz e integrada ao ambiente interno com console único de gerenciamento por meia da plataforma web, e possibilite a verificação de todos os produtos e até mesmo a instalação e manutenção por meio do mesmo console.

2.1 MANUTENÇÃO E PADRONIZAÇÃO PARA SOLUÇÃO DE ANTIVIRUS ATUAL - Atualmente o Município possuí em seu ambiente computacional, uma solução de segurança com política de controle para prevenção desses vírus e ataques vindos da grande rede de computadores mundial, configurado no console de gerenciamento centralizado em uma ferramenta desenvolvida pela Kaspersky.

A utilização da plataforma Kaspersky Endpoint Security for Business há mais de 5 anos, tem possibilitado o gerenciamento centralizado para a proteção dos endpoints (dispositivos como computadores, laptops, servidores) começou a ser utilizado em 2018 após com o processo de dispensa 005/2018, e continuou sendo utilizado desde 2020 por meio do processo de dispensa de licitação nº 015/2020, e vem atendendo as expectativas deste órgão, no que se refere a segurança da informação; e nesse período não registrou-se nenhuma ataque bem sucedido na rede de computadores no município. No entanto, para não sofrer problemas causados pela ausência de um antivírus ou pela descontinuidade ou até mesmo pela utilização de um antivírus desatualizado e incompatível com o ambiente já implementado; é necessária a manutenção dessa solução de software antivírus.

Além dessas razões destaca-se ainda o fato de dentre as soluções mais utilizadas no mercado, o software de antivírus da Kaspersky, apontando a superioridade constatada pelo mercado. Como apresentado em uma pesquisa realizada no site: https://www.oficinadanet.com.br/seguranca/30350-os-melhores-pagos, além de do site https://dpinet.com.br/qual-e-o-melhor-antivirus-para-minha empresa/; e do https://techinter.com.br/, fundamentado e certificado pelas empresas de teste de desempenho de software de antivírus, AV-Comparativos, https://www.av-comparatives.org/enterprise/comparison/# e AV-teste, https://www.av-test.org/en/antivirus/home-windows/.

Antivírus	Proteção RT	Performance	Proteção Malware	Falso Positivo	AV-TEST	MÉDIA
Kaspersky	99,70%	98,50%	99,96%	99,00%	100,00%	99,43%
Avira	99,80%	99,20%	99,98%	98,00%	100,00%	99,40%
Avast	100,00%	98,90%	100,00%	98,00%	100,00%	99,38%
BitDefender	99,70%	98,40%	99,98%	98,00%	100,00%	99,22%
Total AV	99,20%	99,10%	99,97%	100,00%	97,20%	99,09%
AVG	100,00%	98,80%	100,00%	98,00%	97,20%	98,80%
McAfee	99,80%	97,50%	100,00%	97,00%	97,20%	98,30%
Gdata	100,00%	99,10%	100,00%	91,00%	100,00%	98,02%
K7	99,50%	99,40%	99,97%	91,00%	97,20%	97,41%
Norton	99,90%	98,70%	99,99%	73,00%	97,20%	93,76%

CAIRU
PREFEITURA MUNICIPAL

SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO

Fonte: https://www.oficinadanet.com.br/seguranca/30350-os-melhores pagos

Nessa perspectiva, é essencial salvaguardar o ambiente computacional, permitindo preservar os ativos corporativos (hardware, software e, sobretudo, dados), garantindo a integridade, confiabilidade e segurança e a continuidade das atividades da organização; uma vez utilizando outra ferramenta, não se garante a interoperabilidade entre os ambientes e não se pode assegurar a segurança do ambiente de rede local corporativo desta instituição.

A padronização e manutenção da solução de antivírus da fabricante Kaspersky encontra-se baseada no período que essa instituição já vem utilizando essa solução, como já mencionado anteriormente. Além do atendimento ao princípio da padronização, trazida inclusive pela recente Lei Federal nº 14.133, de 1 de abril de 2021, no Art. 43, I e apresentado pelo doutrinador Justen Filho (2021, p. 567), ao salientar que:

> "A padronização é um instrumento de racionalização das atividades administrativa, com redução de custos e otimização da aplicação de recursos. A padronização elimina variações de produtos na fase de julgamento, na utilização, conservação entre outras vantagens". Há de se lembrar ainda que a Súmula/TCU nº 270: diz que "em licitações referentes a compras, inclusive de softwares, é possível a indicação de marca, desde que seja estritamente necessária para atender exigências de padronização e que haja prévia justificação".

Dessa forma em análise pode-se constatar que:

a) A solução de segurança e proteção Kaspersky, já homologada em nosso ambiente, atua na defesa contra vírus, ransowares e outras ameaças que surgem a cada segundo na rede mundial (Internet), além de permitir a utilização de software para controle de acesso, identificação, contingência e eliminação de códigos e limpeza de mensagens maliciosas via servidores de email, controle de detecção de intrusão, geração e emissão de relatórios e gerenciamento centralizado, além de nos proporcionar o bom funcionamento e proteção dos dados e informações sigilosas.

b) seria necessário demandar grandes recursos no intuito de traçar um novo estudo de implementação de plataforma diversa de antivírus gerando um consumo de tempo e recursos humanos, além da necessidade de gastos com treinamento de pessoal na nova tecnologia. Ou seja, a utilização de uma nova solução, demandaria a reconfiguração de um de nosso Servidores, para gerência a licenças, das estações, além do deslocamento dos técnicos para desinstalar a solução atual e instalar a nova, nas 200 estações. Já que todos as estações estão vinculadas a um Servidor de domínio, o qual gerencia toda a rede. Esse processo seria necessário, pois qualquer ataque bem-sucedido a uma das estações, afetaria toda a rede de computadores, servidores com danos aos arquivos e banco de dados do município. Ademais, há que se pesar a reescrita dos processos de gerenciamento da ferramenta.

c) Por fim, tendo em vista o fato do antivírus Kaspersky Endpoint Security for Business já estar implantado nesta instituição, esta fase (implantação de uma nova solução) não será necessária no contexto da ampliação do uso da ferramenta, não ensejando em adaptações do ambiente computacional, reconfigurações de rede, políticas de controle de tráfego e ajustes em regras de acesso. Desta forma, verifica-se que a opção pela manutenção da solução já implantada apresenta-se como a mais econômica para o Município.

Portanto, considerando as atividades e ações necessárias para o desenvolvimento dos serviços e das atividades, solicitamos a aquisição imediata de licenças de software antivírus Kaspersky Endpoint Security Corporativo, para continuar cobrindo com a presente solução a demanda de segurança da informação atendendo as necessidades das diversas Secretarias do Município de Cairu, Arquipélago de Tinharé.

2.2 ANÁLISE DAS VERSÃO PARA A SOLUÇÕES DE ANTIVÍRUS

A Prefeitura do Município de Cairu – BA, adquiriu em 2021, 200 (duzentas) licenças de antivírus Kaspersky Endpoint Security for Business na versão SELECT, a qual atendeu as demandas das estações de trabalho, notebooks e servidores da rede da instituição **naquele período**. No entanto essas licenças já expiraram (14 de maio de 2023) e com a constante diversificação e desenvolvimento de novas ameaças cibernéticas ao longo do tempo, torna-se mandatório o upgrade para uma melhor versão de antivírus, principalmente pelo crescimento dos ataques vindo da grande rede de computadores nos órgão públicos, por meio de ransomwere, o qual é um tipo de software malicioso (malware) que criptografa arquivos em um sistema infectado e que exige um resgate (ransom) para desbloquear os arquivos.

Esse tipo de malware é projetado para restringir o acesso aos dados de uma vítima, geralmente através da criptografia, e os cibercriminosos responsáveis pelo ataque exigem um pagamento em troca da chave de descriptografia. Além da implementação da proteção das informações e dados pessoais e corporativos, para atender às exigências da Lei geral de Proteção de Dados Pessoais (LGPD).

Dessa forma a versão atual não atende integralmente aos requisitos das necessidades desta instituição, sobretudo pela proteção com a utilização da tecnologia de criptografia, e a aquisição da renovação das licenças com o upgrade para a uma melhor versão do software antivírus. Pois **umas das funcionalidades**

CAIRU PREFEITURA MUNICIPAL

SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO

ausentes na versão em uso; como é visível na figura do comparativo das versões.

	Select	Advanced SAIBA MAIS	Total SAIBA MAIS
Defesa para PC, Linux, Mac, Android e IOS	✓	✓	✓
Defesa para aplicativos e servidores de terminal		✓	✓
Defesa para gateways da Web e servidores de e-mail			✓
Defesa contra ameaças em dispositivos móveis	✓	✓	✓
Detecção de comportamento, mecanismo de remediação	✓	✓	✓
Avaliação de vulnerabilidade e prevenção contra Exploit	✓	✓	✓
Permissões variáveis de ambiente e HIPS	✓	✓	✓
AMSI, Microsoft Active Directory, Syslog, RMM, PSA, EMM integration	✓	✓	✓
Gerenciamento de criptografia		✓	✓
Integração do Kaspersky Sandbox e Kaspersky EDR Optimum	✓	✓	✓
Proteções de ameaças da Web e de e-mails e controles para servidores		✓	✓
Controle adaptativo de anomalias e gerenciamento de correções		✓	✓
Criptografia e gerenciamento de criptografia integrado no SO		✓	✓
Integração de SIEM avançada, instalação de software de terceiros e de SO		✓	✓
Filtragem de conteúdo de entrada e saída			✓
Proteção anti-spam no nível de gateway			✓
Segurança de tráfego e controles da Web a nível de gateway			✓

MOSTRAR MENOS RECURSOS

Fonte:https://www.kaspersky.com.br/small-to-medium-business-security/endpoint-advanced

A figura 1 apresenta a diferença entre as versões SELECT, ADVANCED e TOTAL. **Dentre as características da versão ADVANCED, que interessam para as atuais necessidades da Prefeitura Municipal de Cairu**, as quais não se encontram na versão SELECT estão: integração de SIEM avançada, instalação de softwares de terceiros e de SO e o controle adaptativo de anomalias, gerenciamento de correções e utilização de tecnologia de criptografia no gerenciamento integrada no SO.

Deve-se observar que a versão TOTAL do Kaspersky também atende aos requisitos da demanda e ainda apresenta outras funcionalidades, mas essas funcionalidades exclusivas da versão TOTAL já são supridas por outras soluções já existentes do parque tecnológico do Município, o que justifica a sua exclusão como possível solução para este estudo técnico. Sendo assim é apresentada duas opções de versões de soluções:

Opção 1: a renovação das licenças Kaspersky Endpoint Security for Business SELECT É a versão em uso atualmente com as funções de segurança dos endpoints (dispositivos e pontos de comunicação). Renovar as licenças desta versão somente possibilita a manutenção das funcionalidades básicas já existentes e apresentadas na Figura 1 acima, não adicionando novas funcionalidades, tais como a instalação de sistema operacional e de softwares de terceiros, controle adaptativo de anomalias e gerenciamento de correções. Apesar de ser a de menor custo, não atende totalmente aos requisitos citados neste documento.

Opção 2: a renovação das licenças do software antivírus com upgrade para a versão Kaspersky Endpoint Security for Business ADVANCED. Esta versão tem todas as funcionalidades da versão SELECT e mais: gerenciamento de criptografia, proteção contra ameaças da Web e de e-mails, controles para servidores, controle adaptativo de anomalias, gerenciamento de criptografia e de criptografia integrado ao SO, Integração de SIEM avançada, atualização de path do sistema operacional e de softwares de terceiros e a verificação de vulnerabilidades de aplicativos. O que possibilita um melhor controle dos riscos

CAIRU
PREFEITURA MUNICIPAL

SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO

sobre os hardwares, softwares e dados, visando combater e prevenir riscos na operação e na utilização deles.

2.3 IDENTIFICAÇÃO DA VERSÃO PARA A SOLUÇÃO. - Após uma breve análise das três tabelas pode-se destacar o seguinte: A versão SELECT tem um custo unitário menor que a versão ADVANCED, mas devemos lembrar que a versão SELECT é menos provida de recursos que a versão ADVANCED e não atende à demanda deste estudo; O quantitativo de licenças adquiridas afeta o custo unitário, sendo que quanto mais licenças, menor o custo individual da licença, o que é um fator a justificar a aquisição de um número maior de licenças; O período de validade das licenças também influi no custo unitário, sendo que quanto maior o tempo, menor o valor unitário por ano de validade, sendo também um fator importante na escolha da melhor solução .Desse modo para atender as necessidade

A versão ADVANCED atende aos requisitos da demanda, dando maior segurança às operações no ambiente tecnológico da Prefeitura Municipal de Cairu.

Nesse sentido como relatado neste Termo de Referência, tal solução se enquadram como BENS COMUNS ou usuais de mercado. Conforme prevê o Parágrafo único do artigo 1º da Lei 10.520/2002: "Consideram-se bens e serviços comuns, para os fins e efeitos deste artigo, aqueles cujos padrões de desempenho e qualidade possam ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado".

Desse modo a Kaspersky oferece licenciamento desses produtos na modalidade de licença perpétua, onde o cliente compra a licença e junto com a aquisição adquire também o direito a suporte técnico da própria Kaspersky e manutenção das licenças (ex.: fazer o upgrade gratuito caso seja lançada uma nova versão do produto comprado). Este direito ao suporte e manutenção, também conhecido como "Termo" pode ser de 1, 2 ou 3 anos. Finalizado este prazo, o cliente deverá fazer a renovação deste "Termo", ou seja, pagará um valor menor do que a aquisição e continuará se beneficiando do acesso a suporte e manutenção das licenças.

Portanto, uma vez que parte dos equipamentos de informática já o tem devidamente instalados e em pleno funcionamento, tendo este processo a finalidade de atender integralmente ao parque tecnológico do município, visando a padronização e a manutenção por parte da equipe técnica, uso de software antivírus corporativo padronizado em seus diversos equipamentos é uma das várias ações tomadas ao longo do tempo para implantar ferramentas que possam viabilizar os processos de segurança objetivando a repercussão positiva na promoção da cultura da segurança.

Sendo assim é necessária a aquisição da renovação das licenças com o upgrade para a uma melhor versão do software antivírus com suporte técnico e garantia para continuidade do serviço prestado, uma vez que a solução é utilizada de forma padronizada no ambiente da prefeitura de Cairu.

Dessa forma o Município de Cairu busca uma solução de segurança que assegure a proteção dos seus dados e funcione de forma fácil e eficiente com os atuais hardwares, equipamentos e dispositivos da entidade. É uma solução que colabora com o aumento da produtividade, acrescentando fundamental segurança aos sistemas do Município, com proteção de dados em todos os dispositivos.

3. OBJETIVOS

- Proporcionar proteção centralizada para estações de trabalho da rede corporativa da Prefeitura Municipal de Cairu (PMC);
- Prevenir e proteger as estações de trabalho e servidores (Supercomputadores) da Prefeitura contra-ataques de usuários mal-intencionados e softwares maliciosos da rede mundial de computadores (internet);
- Proporcionar uma política de segurança para garantir a integridade dos dados e das informações do Município.
- Buscar a eliminação de gastos com manutenção de hardwares e softwares devido a danos causados por malwares e outros ataques virtuais;
- Buscar a elevação e melhoria nos níveis de segurança nos ativos protegidos.
- Proporcionar o uso de software com tecnologia moderna e atualizada.

4. BASE LEGAL - Lei nº 14.133/2021; e pela Lei Complementar nº 123/06.

5. ESPECIFICAÇÕES DOS MATERIAS

ITEM	PRODUTO	QUANT.	VALID. MINIMA DA LICENÇA
1	Fornecimento de licenças de uso do software de antivírus Kaspersky Endpoint Security For Business - ADVANCED, com suporte técnico, por 24 (vinte e quatro) meses.	200	2 ANO

5. 1 CARACTERÍSTICAS TÉCNICAS MÍNIMAS A SEREM ATENDIDAS:

1.Servidor de Administração e Console Administrativa

CAIRU PREFEITURA MUNICIPAL

SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO

1.1. Compatibilidade:

1.1.1. Microsoft Windows Server 2012/R2 (Todas as edições);
1.1.2. Microsoft Windows Small Business Server 2008 (Todas as edições);
1.1.3. Microsoft Windows Small Business Server 2011 (Todas as edições);
1.1.4. Microsoft Windows Server 2016 x64;
1.1.5. Microsoft Windows 7 SP1 Professional / Enterprise / Ultimate x86/x64;
1.1.6. Microsoft Windows 8 SP1 Professional / Enterprise x86/x64;
1.1.7. Microsoft Windows 8/8.1 Professional / Enterprise X86/x64;
1.1.8. Microsoft Windows 10 (Todas as edições);
1.1.9. Microsoft Windows 11; 1.2. Suporta as seguintes plataformas virtuais:
1.2.1. Vmware: Workstation 12.x pro vSphere 5.5, vSphere 6, vSphere 7;
1.2.2. Microsoft Hyper-V: 2008, 2008 R2, 2008 R2 SP1, 2012, 2012 R2;
1.2.3. Microsoft Virtual PC 6.0.156.0; 1.2.4. KVM integrado com: RHEL 5.4.;
1.2.5. Oracle VM VirtualBox 4.0.4-70112;
1.2.6. Citrix XenServer 6.2 e 6.5;
1.3.Características:
1.3.1. Console deve ser acessada via WEB (HTTPS) ou MMC;
1.3.2. Console deve ser baseada no modelo cliente/servidor;
1.3.3. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;
1.3.4. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;
1.3.5. Deve permitir incluir usuários do AD para logarem na console de administração;
1.3.6. Console deve ser totalmente integrada com as suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM;
1.3.7. As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;
1.3.8. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;
1.3.9. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;
1.3.10. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
1.3.11. Deve armazenar histórico das alterações feitas em políticas;
1.3.12. Deve 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;
1.3.13. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas;
1.3.14. A solução de gerência deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;
1.3.15. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;
1.3.16. Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS e Android;
1.3.17. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;
1.3.18. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os parâmetros KB/s e horário;
1.3.19. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução;
1.3.20. Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança;
1.3.21. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede;
1.3.22. Capacidade de gerar pacotes customizados (autoexecutáveis) contendo a licença e configurações do produto;
1.3.23. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;
1.3.24. Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;
1.3.25. A comunicação entre o cliente e o servidor de administração deve ser criptografada;
1.3.26. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;
1.3.27. Capacidade de aplicar atualizações do Windows remotamente nas estações e servidores;
1.3.28. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;
1.3.29. Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional;
1.3.30. Capacidade de monitorar diferentes subredes a fim de encontrar máquinas novas para serem adicionadas à proteção;

CAIRU
PREFEITURA MUNICIPAL

SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO

1.3.31. 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 à proteção;
1.3.32. Capacidade de, assim que detectar máquinas novas no Active Directory, subredes ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;
1.3.33. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos dois dias, etc.;
1.3.34. 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;
1.3.35. Deve fornecer as seguintes informações dos computadores: Se o antivírus está instalado; Se o antivírus está iniciado; Se o antivírus está atualizado; Minutos/horas desde a última conexão da máquina com o servidor administrativo; Minutos/horas desde a última atualização de vacinas; Data e horário da última verificação executada na máquina; Se é necessário reiniciar o computador para aplicar mudanças; Data e horário de quando a máquina foi ligada; Quantidade de vírus encontrados (contador) na máquina; Nome do computador; Domínio ou grupo de trabalho do computador; Data e horário da última atualização de vacinas; Sistema operacional com Service Pack; Quantidade de processadores; Quantidade de memória RAM; Usuário(s) logado(s) naquele momento, com informações de contato (caso disponível no Active Directory); Endereço IP; Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido; Atualizações do Windows Updates instaladas; Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD; Vulnerabilidades de aplicativos instalados na máquina;
1.3.36. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
1.3.37. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como: Alteração de Gateway Padrão; Alteração de subrede; Alteração de domínio; Alteração de servidor DHCP; Alteração de servidor DNS; Resolução de Nome; Disponibilidade de endereço de conexão SSL;
1.3.38. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
1.3.39. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
1.3.40. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
1.3.41. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
1.3.42. 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; 1.3.43. 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;
1.3.44. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML; 1.3.45. Capacidade de gerar traps SNMP para monitoramento de eventos;
1.3.46. Capacidade de enviar e-mails para contas específicas em caso de algum evento;
1.3.47. Listar em um único local, todos os computadores não gerenciados na rede;
1.3.48. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes;
1.3.49. Deve possuir compatibilidade com Cisco Network Admission Control (NAC),
1.3.50. Deve possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por exemplo).
1.3.51. Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente;
1.3.52. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc.), inclusive de máquinas que estejam em subredes diferentes do servidor;
1.3.53. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
1.3.54. Deve através de opções de otimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo, porém sem comprometer o desempenho do computador;
1.3.55. Deve 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);
1.3.56. 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;
1.3.57. Deve 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;
1.3.58. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;
1.3.59. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo: Nome do vírus; Nome do arquivo infectado; Data e hora da detecção; Nome da máquina ou endereço IP; Ação realizada;
1.3.60. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;
1.3.61. Capacidade de listar updates nas máquinas com o respectivo link para download
1.3.62. Deve criar um backup de todos os arquivos deletados em computadores para que possa ser restaurado através de comando na Console de administração;
1.3.63. Deve ter uma quarentena na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante;
1.3.64. Capacidade de realizar inventário de hardware de todas as máquinas clientes;
1.3.65. Capacidade de realizar inventário de aplicativos de todas as máquinas clientes;
1.3.66. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

2. Estações Windows

2.1. Compatibilidade:

2.1.1. Microsoft Windows 7 SP1 Professional/Enterprise/Ultimate x86/x64;
2.1.2. Microsoft Windows 8 Professional/Enterprise x86 /x64;
2.1.3. Microsoft Windows 8.1 Pro / Enterprise x86 /x64; 2.1.4. Microsoft Windows 10 Pro / Enterprise x86 /x64; Microsoft Windows 11 Pro/ Enterprise x86 /x64.
2.1.5. Microsoft Windows Server 2012 R2 Standard x64;
2.1.6. Microsoft Windows Server 2012 Foundation x64;
2.1.7. Microsoft Windows Server 2012 Standard x64;
2.1.8. Microsoft Small Business Server 2011 Standard x64;
2.1.9. Microsoft Windows Server 2016 x64.
2.2.Características:
2.2.1. Deve prover as seguintes proteções:
2.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;
2.2.1.2. Antivírus de Web (módulo para verificação de sites e downloads contra vírus);
2.2.1.3. Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
2.2.1.4. Antivírus de Mensagens Instantâneas (módulo para verificação de mensagens instantâneas, como ICQ, MSN, IRC, etc.);
2.2.1.5. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
2.2.1.6. Firewall com IDS; 2.2.1.7. Autoproteção (contra-ataques aos serviços/processos do antivírus); 2.2.1.8. Controle de dispositivos externos;
2.2.1.9. Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc; 2.2.1.10. Controle de acesso a sites por horário;
2.2.1.11. Controle de acesso a sites por usuários;
2.2.1.12. Controle de acesso a websites por dados, ex.: Bloquear websites com conteúdos de vídeo e áudio;
2.2.1.13. Controle de execução de aplicativos;
2.2.1.14. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
2.2.2. Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
2.2.3. 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);
2.2.4. Capacidade de automaticamente desabilitar o Firewall do Windows (caso exista) durante a instalação, para evitar incompatibilidade com o Firewall da solução;
2.2.5. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
2.2.6. 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;
2.2.7. 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
2.2.8. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
2.2.9. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
2.2.10. 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;
2.2.11. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas;
2.2.12. Capacidade de verificar somente arquivos novos e alterados;
2.2.13. Capacidade de verificar objetos usando heurística utilizando no mínimo as seguintes opções de nível: Alta, Média, Baixa;
2.2.14. Capacidade de agendar uma pausa na verificação;
2.2.15. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;
2.2.16. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
2.2.17. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI, assim como conexões criptografadas (SSL) para POP3 e IMAP (SSL);
2.2.18. Capacidade de verificar tráfego de ICQ, MSN, AIM e IRC contra vírus e links phishings;
2.2.19. Capacidade de verificar links inseridos em e-mails contra phishings;
2.2.20. Capacidade de verificar tráfego SSL nos browsers: Internet Explorer, Firefox, Google Chrome e Opera;
2.2.21. Capacidade de verificação de corpo e anexos de e-mails usando heurística;
2.2.22. Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;
2.2.23. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;
2.2.24. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;
2.2.25. Capacidade de verificação de tráfego HTTP/HTTPS e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc.), usando heurísticas;
2.2.26. Deve ter suporte total ao protocolo Ipv6;
2.2.27. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;
2.2.28. Na verificação de tráfego web, caso encontrado código malicioso o programa deve: Perguntar o que fazer, ou bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou permitir acesso ao objeto;
2.2.29. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador: Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo-real, ou Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação;
2.2.30. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;
2.2.31. 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;
2.2.32. Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;
2.2.33. 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;
2.2.34. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://www.antiphishing.org/);
2.2.35. Capacidade de distinguir diferentes subredes e conceder opção de ativar ou não o firewall para uma subrede específica;
2.2.36. 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;
2.2.37. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras: Filtragem de pacotes onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas; 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;
2.2.38. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo: Discos de armazenamento locais; Armazenamento removível; Impressoras; CD/DVD; Modems; Dispositivos de fita; Dispositivos multifuncionais; Leitores de smart card; Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc); Wi-Fi; Adaptadores de rede externos; Dispositivos MP3 ou smartphones; Dispositivos Bluetooth; Câmeras e Scanners.
2.2.39. Capacidade de liberar acesso a um dispositivo específico e usuários específico por um período de tempo específico, sem a necessidade de desabilitar a proteção, sem desabilitar o gerenciamento central ou de intervenção local do administrador na máquina do usuário;
2.2.40. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário; 2.2.41. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;
2.2.42. Capacidade de habilitar "logging" em dispositivos removíveis tais como Pendrive, Discos externos, etc.
2.2.43. Capacidade de configurar novos dispositivos por Class ID/Hardware ID;
2.2.44. Capacidade de limitar o acesso a sites da internet por categoria, por conteúdo (vídeo, áudio, etc), com possibilidade

de configuração por usuário ou grupos de usuários e agendamento.
2.2.45. 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);
2.2.46. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação: Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.
2.2.47. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
2.2.48. 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;
2.2.49. 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;
2.2.50. 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.
2.2.51. Capacidade de voltar ao estado anterior do sistema operacional após um ataque de malware. 2.2.52. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.
2.2.53. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).
2.2.54. Capacidade de integração com o Windows Defender Security Center.
2.2.55. Capacidade de integração com a Antimalware Scan Interface (AMSI).
2.2.56. Capacidade de detecção de arquivos maliciosos executados em Subsistema Windows para Linux (WSL).
2.2.57. Deve possuir módulo que monitora e bloqueia atividades potencialmente maliciosas, baseado no comportamento do usuário e Machine Learning.

3.Estações Mac OS X

3.1. Compatibilidade:

3.1.1. MasOS 10.14 ou posterior

4. Estações de trabalho Linux 32-64 bits

4.1. Compatibilidade:

4.1.1. Ubuntu 14.04.5 LTS,
4.1.2. Ubuntu 16.04.4 LTS
4.1.3. Ubuntu 17.10.1

5.Servidores Windows 32 ou 64 bits

5.1. Compatibilidade:

5.1.1.Windows Server 2008 Standard/Enterprise/Datacenter SP1 e posterior;
5.1.2. Windows Server 2022
5.1.3 Windows 10 Enterprise de várias sessões
5.1.4. Windows Server 2019, todas as versões
5.1.5.Windows Server 2016, todas as versões
5.1.6 Windows Server 2012, todas as versões
5.1.7.Windows Server 2008, todas as versões, Service Pack 2 ou posterior
5.1.8.Windows Server 2003, todas as versões, Service Pack 2 ou posterior
5.1.9. Windows Storage Server 2012 ou posterior
5.1.10. Hyper-V Server 2012 ou posterior
5.1.11.Windows MultiPoint Server 2011 ou posterior
5.1.12.Small Business Server 2008 ou posterior

5.2. Características:

5.2.1. Deve prover as seguintes proteções:
5.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;
5.2.1.2. Auto-proteção contra-ataques aos serviços/processos do antivírus;
5.2.1.3.Firewall com IDS; 5.2.1.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados; 5.2.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
5.2.3. 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);
5.2.4. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções: Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas); Gerenciamento de tarefa (criar ou excluir tarefas de verificação); Leitura de configurações; Modificação de configurações; Gerenciamento de Backup e Quarentena; Visualização de relatórios; Gerenciamento de relatórios; Gerenciamento de chaves de licença; Gerenciamento de permissões (adicionar/excluir permissões acima);

CAIRU PREFEITURA MUNICIPAL

SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO

5.2.5. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras: Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas; 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. 5.2.6. 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;
5.2.7. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede
5.2.8. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc);
5.2.9. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS);
5.2.10. Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;
5.2.11. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;
5.2.12. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;
5.2.13. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas; 5.2.14. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
5.2.15. 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;
5.2.16. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
5.2.17. 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;
5.2.18. Capacidade de verificar somente arquivos novos e alterados;
5.2.19. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.);
5.2.20. Capacidade de verificar objetos usando heurística;
5.2.21. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;
5.2.22. Capacidade de agendar uma pausa na verificação;
5.2.23. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
5.2.24. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve: Perguntar o que fazer ou bloquear acesso ao objeto; apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
5.2.24.1. Caso positivo de desinfecção restaurar o objeto para uso;
5.2.24.2. Caso negativo de desinfecção mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
5.2.25. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
5.2.26. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena; 5.2.27. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados; 5.2.28. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa;
5.2.29. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros
5.2.30. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning);
5.2.31. Capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeamento da pasta.
6.Servidores Linux 32 ou 64 bits
6.1. Compatibilidade:
6.1.1. Red Hat® Enterprise Linux®
6.9 Server
6.1.2. CentOS-6.9
6.1.3. Ubuntu 14.04.5 LTS
6.1.4. Ubuntu 16.04.2 LTS 6.1.5. Ubuntu 17.10.1
9. Criptografia
9.1. Compatibilidade
9.1.1. Microsoft Windows 7 Ultimate/Enterprise/Professional SP1 ou superior x86/x64;

CAIRU PREFEITURA MUNICIPAL

SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO

9.1.2. Microsoft Windows 8/8.1 Enterprise/Pro x86/x64;
9.1.3. Microsoft Windows 10 Enterprise x86/x64;
9.1.4. Microsoft Windows 10 Pro x86/x64;
9.1.5. Microsoft Windows 11;

9.2. Características

9.2.1. 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;
9.2.2. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;
9.2.3. Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;
9.2.4. Capacidade de utilizar Single Sign-On para a autenticação de pré-boot;
9.2.5. Permitir criar vários usuários de autenticação pré-boot;
9.2.6. Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;
9.2.7. Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:
9.2.7.1. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;
9.2.7.2. Criptografar todos os arquivos individualmente;
9.2.7.3. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;
9.2.7.4. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;
9.2.8. 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;
9.2.9. Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;
9.2.10. Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados; 9.2.11. Verificar compatibilidade de hardware antes de aplicar a criptografia;
9.2.12. Possibilita estabelecer parâmetros para a senha de criptografia;
9.2.13. Bloqueia o reuso de senhas;
9.2.14. Bloqueia a senha após um número de tentativas pré-estabelecidas;
9.2.15. Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;
9.2.16. Permite criar exclusões para não criptografar determinados "discos rígidos" através de uma busca por nome do computador ou nome do dispositivo
9.2.17. Permite criptografar as seguintes pastas pré-definidas: "meus documentos", "Favoritos", "Desktop", "Arquivos temporários" e "Arquivos do outlook";
9.2.18. Permite utilizar variáveis de ambiente para criptografar pastas customizadas;
9.2.19. Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de áudio, etc;
9.2.20. Permite criar um grupo de extensões de arquivos a serem criptografados;
9.2.21. Capacidade de criar regra de criptografia para arquivos gerados por aplicações;
9.2.22. Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.
9.2.23. Capacidade de deletar arquivos de forma segura após a criptografia;
9.2.24. Capacidade de criptografar somente o espaço em disco utilizado;
9.2.25. Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;
9.2.26. Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;
9.2.27. Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc;
9.2.28. Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft; 9.2.29. Deve ter a opção de utilização de TPM para criptografia através do BitLocker;
9.2.30. Capacidade de fazer "Hardware encryption".

10. Gerenciamento de Sistemas

10.1. Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores bare-metal;
10.2. Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;
10.3. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;
10.4. 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;

CAIRU PREFEITURA MUNICIPAL

SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO

10.5. Capacidade de gerenciar licenças de softwares de terceiros;
10.6. Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;
10.7. Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, etc);
10.8. Possibilita fazer distribuição de software de forma manual e agendada;
10.9. Suporta modo de instalação silenciosa;
10.10. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis; 10.11.Possibilita fazer a distribuição através de agentes de atualização;
10.12. Utiliza tecnologia multicast para evitar tráfego na rede;
10.13. Possibilita criar um inventário centralizado de imagens;
10.14. Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário; 10.15. Suporte a WakeOnLan para deploy de imagens;
10.16. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches; 10.17. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;
10.18. Capacidade de gerar relatórios de vulnerabilidades e patches;
10.19. Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;
10.20. Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;
10.21. Permite baixar atualizações para o computador sem efetuar a instalação;
10.22. Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;
10.23. Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;
10.24. Permite selecionar produtos a serem atualizados pela console de gerenciamento;
10.25. Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc;
10.26. Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;
10.27. Capacidade de instalar atualizações ou correções somente em computadores definidos ou em grupos definidos conforme selecionado pelo administrador;
10.28. Capacidade de configurar o reinício do computador após a aplicação das atualizações e correções de vulnerabilidades;
10.29. Deve permitir selecionar o idioma das aplicações que serão atualizadas;
10.30. Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes;
10.30.1. Capacidade de definir listas de tipos de objetos que não serão verificados;
10.30.2. Capacidade de definir listas de servidores que não terão o tráfego verificado;
10.30.3. Capacidade de definir grupos de usuários e aplicar regras de verificação por grupos.

6. RESPONSÁVEL PELO ACOMPANHAMENTO DOS SERVIÇOS

Os serviços executados deverão acontecer sob supervisão da Secretaria da Administração SEAD, através do Departamento de Tecnologia e Informação - DTI.

Técnico Responsável: Davi Boaventura da Silva Júnior
Tel.: (75) 3653-2151 / Ramal: 215
E-mail: dti@cairu.ba.gov.br

7. PRAZO, LOCAL E CONDIÇÕES DE ENTREGA

1. O objeto desta licitação deverá ser entregue de forma imediata em **até 10 (dez) dias** de acordo com as solicitações emitidas pela CONTRATANTE e o recebimento se dará de acordo com as quantidades descritas na Ordem de Fornecimento e deverá acontecer de segunda-feira a sexta-feira, das 08 às 17:00h.
2. A entrega do objeto desta licitação deverá ocorrer por meio de e-mail eletrônico do o Departamento de Tecnologia da Informação (DTI), ou também pelo correio, no seguinte endereço, onde está situado o Departamento: Complexo Administrativo Diogo Magalhães Brandão - Praça Marechal Deodoro, Nº 03, Centro - Cairu - Bahia.
3. Os pagamentos se darão em uma única parcela somente depois do recebimento definitivo dos produtos/serviços, que deverão ser atestados diretamente do fabricante;
4. A Administração rejeitará, no todo ou em parte, a entrega dos bens/serviços em desacordo com as especificações exigidas.

7.1 DAS LICENÇAS - Todas as licenças que compõem a solução devem contar com manutenções corretivas, sem ônus adicional para a Prefeitura Municipal de Cairu, durante o ciclo de vida do software indicado pelo fabricante, para o caso de vícios, defeitos ou falhas

CAIRU PREFEITURA MUNICIPAL

SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO

Não serão aceitas licenças provisórias. Somente serão aceitas licenças originais do fabricante do software.

As licenças, atualizações e o suporte técnico para o ITEM 01 terão duração de 36 (trinta e seis) meses, a contar de sua ativação.

O serviço de suporte técnico destinado às licenças em uso será realizado com os seguintes objetivos: Ativação das licenças, desinstalação, reconfiguração ou reinstalação, correção de problemas técnicos e esclarecimento de dúvidas sobre configuração, funcionamento e utilização das licenças;

Manutenção e atualização das licenças.

7.2 DA GARANTIA E DO SERVIÇO DE SUPORTE TÉCNICO

1. A garantia e o serviço de suporte técnico para as 200 (duzentas e cinquenta) licenças de uso do Software Antivírus, deverá ser prestado pelo período de 36 (trinta e seis) meses, contados a partir da instalação dos softwares, sem qualquer ônus adicional para a Prefeitura Municipal de Cairu.
2. A licitante vencedora deverá prestar suporte técnico e operacional durante o período de instalação da solução de antivírus, com atendimento através do serviço telefônico ou WEB, em língua portuguesa, para esclarecimento de dúvidas e abertura de chamados para a solução de problemas.
3. O fabricante da solução deverá manter site na internet em português ou inglês que contenha os manuais, atualizações para download, FAQs, instruções, contatos e quaisquer outras informações necessárias para o uso e permanente atualização dos mesmos;
4. O fabricante/fornecedor deverá manter suporte técnico (para resolução de dúvidas e problemas) em português, durante todo o prazo de vigência do contrato, através dos seguintes meios:
5. Telefones fixos em horário comercial (08:00 às 17:00);
6. On-line, via chat;
7. Web Site na Internet;
8. E-mail;
9. A garantia será total contra defeitos, mal funcionamento, atualizações e novas versões dos softwares constantes desta solução, durante todo o prazo de vigência das licenças, contados a partir da data de emissão do Termo de Recebimento Definitivo, a ser emitido pela contratante;
10. A garantia deverá ser acionada, através de comunicado formal de defeito, emitido pela contratante e, poderá ser solicitado através de site WEB ou e-mail indicado pelo fornecedor, para atendimento pela assistência técnica;
11. O fabricante/fornecedor fornecerá todas as atualizações e novas versões dos softwares constantes desta solução de antivírus, lançadas durante a vigência do contrato, sem ônus adicionais;
12. O fabricante fornecerá versões dos softwares constantes desta solução de antivírus, compatíveis com qualquer nova versão de sistema operacional lançada (nas plataformas windows e linux), assim que estas novas versões estejam disponíveis para uso, sem qualquer ônus adicional para a contratante;

8. CONDIÇÕES E PRAZOS DE PAGAMENTO

Os pagamentos devidos à Contratada serão efetuados através de ordem bancária ou crédito em conta corrente de pessoa jurídica em favor da empresa vencedora, no prazo de até 30 (trinta) dias contados da data da apresentação da Nota Fiscal, devidamente atestada à execução contratual, desde que não haja pendência a ser regularizada pelo contratado.

9. DA FISCALIZAÇÃO Todos as entregas e recebimentos serão acompanhados e fiscalizados pelo DTI (Departamento de Tecnologia da Informação) da Prefeitura de Cairu-Ba.

10.DAS RESPONSABILIDADES DA CONTRATADA

1. Fornecer os produtos nas quantidades, prazos e condições pactuadas, de acordo com as exigências constantes neste documento.
2. Emitir faturas no valor pactuado, apresentando-as ao CONTRATANTE para ateste e pagamento.
3. Atender prontamente as orientações e exigências inerentes à execução do objeto contratado.
4. Assegurar ao CONTRATANTE o direito de sustar, recusar, mandar desfazer ou refazer qualquer serviço/produto que não esteja de acordo com as normas e especificações técnicas recomendadas neste termo de referência.
5. Assumir inteira responsabilidade pela entrega dos materiais ou serviços, responsabilizando-se pelo transporte, acondicionamento e descarregamento dos materiais.
6. Responsabilizar-se pela garantia dos materiais e métodos empregados nos itens solicitados, dentro dos padrões adequados de qualidade, segurança, durabilidade e desempenho, conforme previsto na legislação em vigor e na forma exigida neste termo de referência.
7. Responsabilizar-se pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do objeto deste Termo de Referência.
8. Não transferir para o CONTRATANTE a responsabilidade pelo pagamento dos encargos estabelecidos no item anterior, quando houver inadimplência da CONTRATADA, nem onerar o objeto deste Termo de Referência.
9. Manter, durante toda a execução do objeto, em compatibilidade com as obrigações por ele assumidas, todas as condições de habilitação e qualificação exigidas na licitação.
10. Quando for o caso, manter preposto, aceito pela Administração, para representá-lo na execução do objeto contratado.

CAIRU
PREFEITURA MUNICIPAL

SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO

11. Responder pelos danos causados diretamente à CONTRATANTE ou aos seus bens, ou ainda a terceiros, decorrentes de sua culpa ou dolo na execução do objeto;
12. Comunicar ao **CONTRATANTE** qualquer anormalidade que interfira no bom andamento do fornecimento e sua assistência técnica;
13. Atender com presteza as reclamações sobre a qualidade dos serviços/ fornecimento executados, providenciando sua imediata correção, sem ônus para o **CONTRATANTE**;
14. Manter durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação; providenciar e manter atualizadas todas as licenças e alvarás junto às repartições competentes, necessários à execução dos serviços / fornecimento e sua assistência técnica;
15. Efetuar pontualmente o pagamento de todas as taxas e impostos que incidam ou venham a incidir sobre as suas atividades e/ou sobre a execução do objeto do presente, bem como observar e respeitar as Legislações Federal, Estadual e Municipal, relativas aos serviços prestados;
16. Adimplir os fornecimentos exigidos pelo Edital e pelos quais se obriga, visando à perfeita execução do contrato;

11. DAS RESPONSABILIDADES DA CONTRATANTE

1 - Acompanhar e fiscalizar os serviços, atestar nas notas fiscais/faturas o efetivo fornecimento do objeto deste Termo de Referência.

2 - Rejeitar, no todo ou em parte os itens entregues, se estiverem em desacordo com a especificação e da proposta de preços do Termo de Referência.

3 - Comunicar a CONTRATADA todas as irregularidades observadas durante o recebimento dos itens solicitados.

4 - Notificar a CONTRATADA no caso de irregularidades encontradas na entrega dos itens solicitados.

5 - Solicitar o reparo, a correção, a remoção ou a substituição dos materiais/serviços em que se verificarem vícios, defeitos ou incorreções.

6 - Conceder prazo de 03 (três) dias úteis, após a notificação, para a CONTRATADA regularizar as falhas observadas.

7 - Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA.

8 - Aplicar à CONTRATADA as sanções regulamentares.

9 - Exigir o cumprimento dos recolhimentos tributários, trabalhistas e previdenciários através dos documentos pertinentes.

10 - Após a disponibilização das licenças a Prefeitura de Cairu, autorizará a emissão de nota fiscal pela CONTRATADA, a qual deverá conter a discriminação detalhada dos itens fornecidos, momento em que será iniciado o prazo para pagamento.

11 - Caso as licenças ou os upgrades não estiverem em conformidade com o especificado, serão recusados e deverão ser substituídas dentro do prazo máximo de 2 (dois) dias, a contar da data da notificação encaminhada pela Prefeitura de Cairu à CONTRATADA.

12 - À Prefeitura de Cairu não caberá qualquer ônus pela rejeição das licenças ou dos upgrades considerados inadequados ou em desconformidade com as especificações exigidas neste Edital.

13 - A CONTRATADA deverá fornecer toda a documentação técnica original do fabricante, em língua portuguesa e que abranja configuração, instalação e gerenciamento das licenças.

12. REQUISITOS PARA A CONTRATAÇÃO

12.1 Relativos à Habilitação Jurídica:

a) Cédula de identidade do representante legal da empresa;

b) Registro comercial, no caso de empresa individual;

c) Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, para as sociedades comerciais e, no caso de sociedades por ações, acompanhado dos documentos comprobatórios de eleição de seus administradores;

d) Decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no país e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir.

e) Certidão de comprovação da condição de Microempresa ou Empresa de Pequeno Porte, expedida pela Junta Comercial nos termos do art. 8º, da Instrução Normativa nº 103, de 30 de abril de 2007, do Departamento Nacional de Registro do Comércio – DNRC.

12.2 Relativos à Regularidade Fiscal e Trabalhista:

a) Prova de inscrição no Cadastro Nacional de Pessoa Jurídica (CNPJ/MF);

b) Prova de regularidade perante a **Fazenda Federal**, mediante apresentação de Certidão Conjunta de Débitos Relativos a Tributos Federais e à Dívida Ativa da União, fornecida pela Secretaria da Receita Federal ou pela Procuradoria-Geral da Fazenda Nacional;

c) Prova de regularidade para com a **Fazenda Estadual** do domicílio ou sede da licitante, ou outra equivalente, na forma da lei, expedida de forma conjunta pela Procuradoria Geral do Estado do Bahia, nos termos do Decreto Estadual nº 28595 de 30/12/1981 (Certidão Negativa quanto a Dívida Ativa do Estado) e pela Secretaria da Fazenda do Estado do Bahia, com base na Lei Nº 3.956 de 11 de dezembro de 1981;

d) Prova de regularidade para com a **Fazenda Municipal** do domicílio ou sede da licitante, ou outra equivalente, expedida pela Prefeitura Municipal;

e) Prova de regularidade relativa ao **Fundo de Garantia por Tempo de Serviço (FGTS)**, emitida pela Caixa

CAIRU PREFEITURA MUNICIPAL

SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO

Econômica Federal;
f) **Certidão Negativa de Débitos Trabalhistas (CNDT)**, conforme o Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452/43, e Lei nº 12.440/2011.

RESPONSÁVEL PELA ELABORAÇÃO DO INSTRUMENTO.
SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO
Complexo Administrativo Diogo Magalhães Brandão
Praça Marechal Deodoro, S/N - Centro
Nome: Davi Boaventura da Silva Junior
Função: Assessor Técnico do Departamento de Tecnologia da Informação da SEAD
E-mail: dti@cairu.ba.gov.br
Telefone: (75) 3653-2151 Ramal 215

13. RESPONSÁVEL PELA APROVAÇÃO DO INSTRUMENTO.

SECRETARIA DE ADMINISTRAÇÃO
Coordenação: Ângelo César Santiago Fahning
E-mail: adm.geral@cairu.ba.gov.br
Telefone: 3653-2145 – Ramal 208

Cairu, 28 de setembro de 2023.

Davi Boaventura da Silva Júnior

Assessor Técnico