CETESB

COMPANHIA AMBIENTAL DO ESTADO DE SÃO PAULO

DIVISÃO DE SUPRIMENTOS
SETOR DE APOIO AOS GESTORES DE CONTRATOS E DE CADASTRO DE PRODUTOS E FORNECEDORES

COTAÇÃO DE PREÇOS Nº 13/2026/326

OBJETO: Cotação de preços para prestação de serviço de solução de proteção de endpoint e servidores com suporte e gerenciamento da solução, conforme Planilha de Quantidades e Preços – Anexo "1" e Termo de Referência – Anexo "2".

ENCERRAMENTO: 17/04/2026 às 17:00 hs

CONDIÇÕES GERAIS:

1 - PROPOSTA: Apresentar a proposta de preço de acordo com o disposto nesta Cotação e seus anexos, redigida em português, salvo quanto às expressões técnicas de uso corrente. Devendo estar considerado, além do lucro, todos os custos diretos e indiretos, bem como os encargos, benefícios e despesas indiretas (BDI) e demais despesas de qualquer natureza, relacionadas com a prestação dos serviços.

a) Condição de Pagamento – **30 DDL**

b) **VALIDADE DA PROPOSTA**: A validade da proposta não deverá ser inferior a **60 dias.**

c) **PRAZO**: Prazo de Execução: **12 (doze) meses.**

d) A proposta deverá ter o nome do responsável por sua formulação, bem como os dados cadastrais da empresa, **CNPJ, Razão Social, Endereço e Telefone** para contato.

e) A proposta deverá ser encaminhada em formato.**pdf**, Word.**doc**. ou .Excel **.xls**, por e-mail para proposta_cetesb@sp.gov.br ou gboliveira@sp.gov.br até a data e horário de **ENCERRAMENTO**.

f) A proponente deverá possuir cadastro SICAF – Sistema de Cadastramento Unificado de Fornecedores.

CRITÉRIO DE AVALIAÇÃO: A avaliação será feita por **VALOR GLOBAL**

São Paulo, 10 de abril de 2026.

Gabriela Bleker de Oliveira
Fone: (11) 3019-6712
gboliveira@sp.gov.br

CETESB

COMPANHIA AMBIENTAL DO ESTADO DE SÃO PAULO

DIVISÃO DE SUPRIMENTOS
SETOR DE APOIO AOS GESTORES DE CONTRATOS E DE CADASTRO DE PRODUTOS E FORNECEDORES

COTAÇÃO DE PREÇOS Nº 13/2026/326

ANEXO "1"
PLANILHA DE QUANTIDADES E PREÇOS

Item	Descrição do Produto	Unidade	Quantidade (A)	Valor Unit. R$ (B)	Valor Total R$ (C) = (A) x (B)
1	Suíte para proteção de estações de trabalho e servidores, com garantia e suporte técnico pelo período de 12 meses	Licença	2.300		
2	Serviço de implantação e migração da solução de proteção para endpoints e servidores	Serviço	1		
3	Serviço Gerenciado e suporte técnico nas soluções ofertadas	Mensal	12		
				Total Geral (R$)	

Obrigatoriamente a suíte para proteção de estações de trabalho e servidores deverá ser do fabricante Trellix, solução atual utilizada pela CETESB e composta pelos itens abaixo:

Part Number	Descrição	Quantidade
MV6ECE-AA	Trellix Protect Plus EDR for Endpoint	2.300
IVXECE-AA	IVX Enterprise Cloud	2.300
PL1ECE-AA	Trellix Protect Plus EDR for Endpoint	1

IMPORTANTE: DEVERÃO CONSTAR NA PLANILHA DE PROPOSTA OS VALORES UNITÁRIOS E TOTAIS.

Data _____/_____/_____

_____
Assinatura com carimbo da empresa

CETESB

COMPANHIA AMBIENTAL DO ESTADO DE SÃO PAULO

DIVISÃO DE SUPRIMENTOS
SETOR DE APOIO AOS GESTORES DE CONTRATOS E DE CADASTRO DE PRODUTOS E FORNECEDORES

COTAÇÃO DE PREÇOS Nº 13/2026/326

ANEXO "2"

TERMO DE REFERÊNCIA

ESPECIFICAÇÃO TÉCNICA

1. Solução para proteção de estações de trabalho e servidores

1.1. Características gerais

1.1.1. Deve possuir capacidade de instalação e pleno funcionamento dos módulos solicitados em estações de trabalho com no mínimo 3 (três) GB de memória RAM.
1.1.2. Deve suportar as seguintes plataformas clientes:
  1.1.2.1. Windows 8 e superior;
  1.1.2.2. Catalina 10.15.6 e superior;
1.1.3. Deve suportar as seguintes plataformas de servidores:
  1.1.3.1. Windows Server 2012 e superior, inclusive Server Core;
1.1.4. Deve suportar, pelo menos as funções de antivírus e firewall de host, nas seguintes distribuições de Linux:
  1.1.4.1. Oracle Linux 7.x 64 bits e superior;
  1.1.4.2. Red Hat Enterprise 7.x 64 bits e superior;
  1.1.4.3. CentOS 7.x 64 bits e superior;
1.1.5. Deve suportar a instalação de agente nos sistemas operacionais acima virtualizados nas seguintes plataformas:
  1.1.5.1. Microsoft Hyper-V 2012 R2 e superior;
  1.1.5.2. VMware ESXi e superior;
1.1.6. Todas as funcionalidades deverão ser geridas por uma console única com as capacidades mínimas de:
  1.1.6.1. Relatórios;
  1.1.6.2. Dashboards;
  1.1.6.3. Políticas;
  1.1.6.4. Configuração;
  1.1.6.5. Instalação/Desinstalação;
1.1.7. O cliente deve ser capaz de operar em modo autônomo (self-managed) e permitir que as configurações sejam aplicadas diretamente no cliente.
1.1.8. O cliente deve ser capaz de atualizar as definições para detecção de ameaças, patches e hotfixes a partir de um servidor definido pelo administrador ou diretamente nos servidores do fabricante.
1.1.9. A solução deve possuir múltiplas camadas de proteção, não sendo aceitas soluções baseadas apenas em assinaturas;

1.2. Características de proteção para clientes Windows

1.2.1. Módulo Antimalware
  1.2.1.1. Características da prevenção contra exploração
    1.2.1.1.1. Deve ser possível selecionar, no mínimo, dois modos de proteção (Padrão/Máximo).
    1.2.1.1.2. Deve ser possível ativar/desativar a proteção contra escalonamento de privilégios genéricos.
    1.2.1.1.3. Deve ser possível ativar/desativar a prevenção de execução de dados do Windows.

CETESB

COMPANHIA AMBIENTAL DO ESTADO DE SÃO PAULO

DIVISÃO DE SUPRIMENTOS
SETOR DE APOIO AOS GESTORES DE CONTRATOS E DE CADASTRO DE PRODUTOS E FORNECEDORES

COTAÇÃO DE PREÇOS Nº 13/2026/326

1.2.1.1.4. Deve ser possível selecionar dentre as ações de apenas bloquear ou apenas relatar ou bloquear e relatar;
1.2.1.1.5. Deve ser possível bloquear contra falsificação de IP (IP Spoofing).
1.2.1.1.6. Deve ser possível incluir exclusões por:
1.2.1.1.6.1. Processo
1.2.1.1.6.2. Módulo chamador
1.2.1.2. Características da Proteção de acesso
1.2.1.2.1. Deve fornecer regras de proteção de maneira nativa, ou seja, pré-definidas pelo fabricante da solução, no mínimo, para:
1.2.1.2.1.1. Alteração políticas de direitos dos usuários;
1.2.1.2.1.2. Criar ou modificar remotamente arquivos ou pastas;
1.2.1.2.1.3. Executar arquivos das pastas do usuário;
1.2.1.2.1.4. Execução de scripts pelo host de script do Windows;
1.2.1.2.1.5. Modificar processos principais do Windows;
1.2.1.2.2. As regras especificadas devem permitir o:
1.2.1.2.2.1. Bloqueio, ou
1.2.1.2.2.2. Evento de informação, ou
1.2.1.2.2.3. Bloqueio e evento de informação;
1.2.1.2.3. Deve permitir ao administrador criar regras de customizadas com no mínimo os seguintes parâmetros:
1.2.1.2.3.1. Processos;
1.2.1.2.3.2. Usuário;
1.2.1.2.3.3. Arquivos;
1.2.1.2.3.4. Chave de registro;
1.2.1.2.3.5. Valor de registro;
1.2.1.2.4. Deve permitir a configuração de exclusões;
1.2.1.3. Características da varredura ao acessar
1.2.1.3.1. A Varredura deve ser passível de habilitação/desativação por opção do administrador;
1.2.1.3.2. Deve iniciar a proteção durante a inicialização do sistema operacional;
1.2.1.3.3. Deve ser capaz de realizar análise no setor de boot;
1.2.1.3.4. O administrador da solução deve especificar o tempo máximo de análise para um único arquivo;
1.2.1.3.5. Deve analisar os processos durante inicialização do serviço e na atualização de conteúdo;
1.2.1.3.6. Deve possibilitar ao administrador a análise de instaladores confiáveis;
1.2.1.3.7. Deve realizar análise durante cópia entre pastas locais;
1.2.1.3.8. A solução deve possuir conexão com Centro de Inteligência do fabricante, passível de ativação ou desativação por parte do administrador;
1.2.1.3.9. Deve permitir a configuração do nível de agressividade da análise.
1.2.1.3.10. Deve possibilitar aplicar as configurações a todos os processos do sistema operacional ou a uma lista específica criada pelo administrador;
1.2.1.3.11. Deve realizar varredura quando o processo:
1.2.1.3.11.1. Ler o disco e/ou gravar no disco;
1.2.1.3.12. Deve possibilitar análise em:
1.2.1.3.12.1. Unidades de rede;
1.2.1.3.12.2. Arquivos compactados;
1.2.1.3.13. Deve detectar programas indesejados, ameaças em programas desconhecidos e ameaças em macro desconhecidas;
1.2.1.3.14. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar uma ameaça:

CETESB

COMPANHIA AMBIENTAL DO ESTADO DE SÃO PAULO

DIVISÃO DE SUPRIMENTOS
SETOR DE APOIO AOS GESTORES DE CONTRATOS E DE CADASTRO DE PRODUTOS E FORNECEDORES

COTAÇÃO DE PREÇOS Nº 13/2026/326

1.2.1.3.14.1. Limpar o arquivo;
1.2.1.3.14.2. Excluir o arquivo;
1.2.1.3.14.3. Negar acesso ao arquivo;
1.2.1.3.15. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar um programa indesejado:
1.2.1.3.15.1. Limpar o arquivo;
1.2.1.3.15.2. Excluir o arquivo;
1.2.1.3.15.3. Permitir acesso ao arquivo;
1.2.1.3.15.4. Negar acesso ao arquivo;
1.2.1.3.16. Deve possibilitar ao administrador a gestão de uma lista de exclusões;
1.2.1.3.17. Deve possuir módulo capaz de interceptar scripts (Javascript e VBScript) destinados ao Windows Host Scripting e analisá-lo para indicar se é malicioso ou não;
1.2.1.3.18. Deve permitir a criação de listas de exclusão de URLs que não sofrerão interceptação e análise de scripts;
1.2.1.3.19. Ao detectar uma ameaça o agente deverá emitir uma notificação ao usuário com uma mensagem a ser customizada pelo administrador da solução.
1.2.1.4. Características da Varredura sob demanda
1.2.1.4.1. Deve ser possível realizar varreduras agendadas com periodicidade diária ou semanal;
1.2.1.4.2. Deve permitir a criação de repetição da tarefa;
1.2.1.4.3. Deve permitir definir a hora da execução da tarefa de análise;
1.2.1.4.4. Deve permitir a criação da tarefa de varredura de maneira aleatória;
1.2.1.4.5. Deve permitir a realização de varreduras agendadas após logon do usuário ou durante inicialização do sistema operacional.
1.2.1.4.6. Deve permitir escolher (um ou mais) os alvos da varredura, dentre eles:
1.2.1.4.6.1. Os locais da varredura:
1.2.1.4.6.1.1. Memória;
1.2.1.4.6.1.2. Processos em execução;
1.2.1.4.6.1.3. Todas as unidades fixas;
1.2.1.4.6.1.4. Todas as unidades removíveis;
1.2.1.4.6.1.5. Todas as unidades mapeadas;
1.2.1.4.6.1.6. Pasta de perfil do usuário;
1.2.1.4.6.1.7. Pasta temporária;
1.2.1.4.6.1.8. Arquivo ou pasta especificada pelo administrador;
1.2.1.4.6.2. Os tipos de arquivos que serão analisados;
1.2.1.4.6.3. Opções adicionais, como por exemplo detecção de programas indesejados, ameaças em programas desconhecidos e ameaças em macro desconhecidas.
1.2.1.4.6.4. Áreas de exclusão que não deverão ser varridas;
1.2.1.4.7. Deve permitir a integração com o Centro de Inteligência do fabricante durante a varredura agendada.
1.2.1.4.8. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar uma ameaça:
1.2.1.4.8.1. Limpar o arquivo;
1.2.1.4.8.2. Excluir o arquivo;
1.2.1.4.8.3. Continuar varredura;
1.2.1.4.9. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar um programa indesejado:
1.2.1.4.9.1. Limpar o arquivo;
1.2.1.4.9.2. Excluir o arquivo;

CETESB

COMPANHIA AMBIENTAL DO ESTADO DE SÃO PAULO

DIVISÃO DE SUPRIMENTOS
SETOR DE APOIO AOS GESTORES DE CONTRATOS E DE CADASTRO DE PRODUTOS E FORNECEDORES

COTAÇÃO DE PREÇOS Nº 13/2026/326

1.2.1.4.9.3. Continuar varredura;
1.2.1.4.10. Para minimizar o impacto ao usuário, a solução deve permitir:
1.2.1.4.10.1. Utilização de cache, ou seja, arquivos que já foram analisados e não tiveram seu conteúdo alterado não serão novamente analisados;
1.2.1.4.10.2. Iniciar a varredura apenas quando o sistema estiver ocioso ou diminuir a agressividade conforme o uso de memória;
1.2.1.4.10.3. Permitir ao usuário retomar varreduras pausadas;
1.2.1.4.11. Deve permitir ao administrador inserir uma conta de domínio para realizar a análise de dispositivos de rede;

1.2.2. Módulo de Firewall de Host
1.2.2.1. Deve permitir a ativação/desativação do módulo de Firewall através da console;
1.2.2.2. Deve ser capaz de prevenir intrusões e proteger os endpoints garantindo cobertura para ataques dia zero;
1.2.2.3. Deve possuir um firewall de estação stateful bloqueando tráfego de entrada e controlando o tráfego de saída;
1.2.2.4. Deve permitir o tráfego de saída somente após os serviços de Firewall estiverem iniciados;
1.2.2.5. Deve ser possível bloquear tráfego bridge;
1.2.2.6. O módulo deve permitir a criação de regras de maneira adaptativa, ou seja, em uma estação modelo definida pelo administrador deve ser capaz de criar as regras de maneira automática;
1.2.2.7. Deve ser possível bloquear o tráfego de todos os processos identificados como não confiáveis;
1.2.2.8. Deve permitir a criação de uma lista de processos identificados como confiáveis por meio de uma ou mais das seguintes informações:
1.2.2.8.1. Nome;
1.2.2.8.2. Nome do arquivo ou caminho;
1.2.2.8.3. Hash MD5;
1.2.2.8.4. Assinador digital;
1.2.2.9. Deve permitir integração com o Centro de Inteligência do próprio fabricante para bloqueio de ameaças advindas por meio de conexões maliciosas;
1.2.2.10. Deve ser possível registrar os eventos de conexões bloqueadas e permitidas pelo módulo;
1.2.2.11. Deve permitir inspeção do protocolo FTP;
1.2.2.12. Deve ser possível permitir tráfego de protocolos não suportados;
1.2.2.13. O módulo de Firewall deve vir com regras pré-indicadas pelo próprio fabricante.
1.2.2.14. O módulo de Firewall deve permitir a criação de regras customizadas, com no mínimo os seguintes parâmetros:
1.2.2.14.1. Ação:
1.2.2.14.1.1. Bloquear;
1.2.2.14.1.2. Permitir;
1.2.2.14.2. Direção:
1.2.2.14.2.1. Ambas;
1.2.2.14.2.2. Entrada;
1.2.2.14.2.3. Saída;
1.2.2.14.3. Protocolo:
1.2.2.14.3.1. Protocolo IP;
1.2.2.14.3.2. IPv4;
1.2.2.14.4. Especificação da Rede:
1.2.2.14.4.1. Endereço IP;
1.2.2.14.4.2. Subnet;
1.2.2.14.4.3. Range;

CETESB

COMPANHIA AMBIENTAL DO ESTADO DE SÃO PAULO

DIVISÃO DE SUPRIMENTOS
SETOR DE APOIO AOS GESTORES DE CONTRATOS E DE CADASTRO DE PRODUTOS E FORNECEDORES

COTAÇÃO DE PREÇOS Nº 13/2026/326

1.2.2.14.4.4. FQDN;
1.2.2.14.5. Protocolo de Transporte:
1.2.2.14.5.1. ICMP;
1.2.2.14.5.2. ICMPv6;
1.2.2.14.5.3. TCP;
1.2.2.14.5.4. UDP;
1.2.2.14.6. Agendamento:
1.2.2.14.6.1. Dias da semana;
1.2.2.14.6.2. Hora de início e fim;
1.2.2.14.7. Aplicações;

1.2.3. Módulo de Filtragem Web
1.2.3.1. Deve permitir o controle de browsers suportados, dentre eles:
1.2.3.1.1. Chrome;
1.2.3.1.2. Firefox;
1.2.3.1.3. Edge;
1.2.3.2. Deve ser capaz de utilizar lista de categorias para bloqueio de sites relacionados ao conteúdo não autorizado;
1.2.3.3. Deve possuir, no mínimo, duas das seguintes categorias:
1.2.3.3.1. Browser Exploits;
1.2.3.3.2. Download maliciosos;
1.2.3.3.3. Sites maliciosos;
1.2.3.3.4. Phishing;
1.2.3.3.5. Pornografia;
1.2.3.3.6. Hacking/Computer Crime;
1.2.3.3.7. Spyware/Adware/Keyloggers;
1.2.3.3.8. Anonymizer;
1.2.3.4. Deve ser possível bloquear um site conforme a sua classificação de risco;
1.2.3.5. Deve ser possível bloquear um site quando este nunca foi visto pelo Centro de Inteligência do Fabricante;
1.2.3.6. Deve ser possível bloquear páginas de phishing, mesmo que o conteúdo tenha acesso permitido;
1.2.3.7. Deve permitir a varredura de arquivos baixados da internet;
1.2.3.8. Deve ser possível excluir endereços IP da análise;
1.2.3.9. Deve permitir a busca segura para buscadores;
1.2.3.10. Deve bloquear links que direcionem para sites com alto risco;
1.2.3.11. Deve permitir a customização das mensagens apresentadas para o usuário;
1.2.3.12. O módulo deve ter a capacidade de detecção da presença da solução de proxy em uso no ambiente da CONTRATANTE para que seja desativado no endpoint, e posteriormente reativado caso o proxy não seja detectado.

1.2.4. Módulo de Ameaças Avançadas
1.2.4.1. A solução deve permitir o a análise de comportamento de aplicativos e arquivos executáveis com indícios maliciosos (ransomware);
1.2.4.2. A solução deve ser capaz de avaliar aplicações desconhecidas e potencialmente maliciosas executando-as em ambiente controlado;
1.2.4.3. Deve permitir a indicação de aplicações confiáveis para que não caiam no filtro de análise;
1.2.4.4. Não deve requerer conexão com centro de inteligência do fabricante para que a proteção seja ativada ou executada
1.2.4.5. Solução deve manter um cache de reputação local com informações de aplicações - conhecidas, desconhecidas e maliciosas.

CETESB

COMPANHIA AMBIENTAL DO ESTADO DE SÃO PAULO

DIVISÃO DE SUPRIMENTOS
SETOR DE APOIO AOS GESTORES DE CONTRATOS E DE CADASTRO DE PRODUTOS E FORNECEDORES

COTAÇÃO DE PREÇOS Nº 13/2026/326

1.2.4.6. Dentre os comportamentos maliciosos, deve ser capaz de detectar:
- 1.2.4.6.1. Criação de arquivos em qualquer local de rede;
- 1.2.4.6.2. Leitura/exclusão/gravação de arquivos visados por ransomwares;
- 1.2.4.6.3. Bloqueio de modificação de arquivos críticos do Windows e locais do registro;
- 1.2.4.6.4. Bloqueio de modificação de pastas de dados de usuários;
- 1.2.4.6.5. Bloqueio de suspensão de um processo;
- 1.2.4.6.6. Bloqueio de término de outro processo.

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

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

1.2.4.9. O modo de ativação da análise de comportamento de aplicações deve ser aplicado para quaisquer arquivos desconhecidos acessados pelo sistema operacional e nunca vistos pela solução;

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

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

1.2.4.12. Deve possuir capacidade de inspecionar arquivos suspeitos e detectar comportamentos maliciosos utilizando técnicas de "machine learning";

1.2.4.13. A solução deve ter a capacidade de remediação de ações efetuadas por artefatos maliciosos, como criação de arquivos e alteração de chaves de registro;
- 1.2.4.13.1. A remediação deve ser efetuada de maneira automática, a partir do momento em que o artefato é identificado como malicioso.

1.2.5. Módulo de Controle de Dispositivos

1.2.5.1. Deve controlar o uso de dispositivos por parte dos usuários, como por exemplo Mídias Removíveis, Unidades USB, Dispositivos Bluetooth, DVDs, e CDs regraváveis;

1.2.5.2. Deve permitir a configuração dos dispositivos nos modos:
- 1.2.5.2.1. Bloqueio, ou;
- 1.2.5.2.2. Somente leitura;

1.2.5.3. Deve classificar os dispositivos em 2 categorias:
- 1.2.5.3.1. Gerenciado;
- 1.2.5.3.2. Não gerenciado;

1.2.5.4. Deve ser capaz de identificar o dispositivo (plug and play) através de pelo menos duas das seguintes informações:
- 1.2.5.4.1. Tipo de BUS;
- 1.2.5.4.2. Classe do dispositivo (Device Class);
- 1.2.5.4.3. ID do fabricante (Vendor ID);
- 1.2.5.4.4. ID do produto (Product ID);

1.2.5.5. Deve ser capaz de identificar Dispositivos Removíveis através das seguintes informações:
- 1.2.5.5.1. Tipo de BUS;
- 1.2.5.5.2. Tipo de sistema de arquivo;

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

1.3. Características de proteção para clientes Linux

1.3.1. Módulo Antimalware

1.3.1.1. Características da prevenção de ameaças

CETESB

COMPANHIA AMBIENTAL DO ESTADO DE SÃO PAULO

DIVISÃO DE SUPRIMENTOS
SETOR DE APOIO AOS GESTORES DE CONTRATOS E DE CADASTRO DE PRODUTOS E FORNECEDORES

COTAÇÃO DE PREÇOS Nº 13/2026/326

1.3.1.1.1. Deve permitir a atualização automática das vacinas de detecção;
1.3.1.1.2. Deve detectar ameaças usando métodos de acesso e de varredura sob demanda;
1.3.1.1.3. Deve permitir a execução de varreduras por meio da console centralizada por meio de tarefas;
1.3.1.1.4. Ao detectar uma ameaça, deverá responder com, no mínimo, as seguintes ações:
1.3.1.1.4.1. Limpar o arquivo;
1.3.1.1.4.2. Excluir o arquivo;
1.3.1.1.4.3. Negar acesso ao arquivo;
1.3.1.1.5. Deve possibilitar ao administrador, criar exceções de análise, ou seja, não permitir que a ferramenta execute uma análise em determinadas pastas ou arquivos;
1.3.1.1.6. Deve permitir a opção de manter a configuração de exclusão realizada no agente, não sendo sobrescrita pela política principal;
1.3.1.1.7. Deve permitir a gestão do agente local por meio de linha de comando;
1.3.1.1.8. Ao configurar a análise ao acessar, deve permitir:
1.3.1.1.8.1. Quando analisar (exemplo: ao ler o arquivo);
1.3.1.1.8.2. O que analisar (exemplo: todos os arquivos);
1.3.1.1.8.3. Análise de arquivos compressos;
1.3.1.1.8.4. Análise de volumes de rede;
1.3.1.1.9. Ao configurar a análise sob demanda, deve permitir:
1.3.1.1.9.1. Análise de arquivos compressos;
1.3.1.1.9.2. Análise de programas desconhecidos;
1.3.1.1.9.3. Análise de pastas e subpastas;
1.3.1.1.9.4. Análise de macros;
1.3.1.1.9.5. Exclusão de paths, pastas e tipos de arquivos;
1.3.1.1.10. Deve possuir quarentena local para armazenar ameaças desconhecidas;
1.3.1.1.11. Deve possuir ação para mover artefatos maliciosos para a área de quarentena;
1.3.1.1.12. Deve usar heurística para detectar arquivos potencialmente maliciosos;
1.3.1.1.13. Caso aconteça um timeout durante uma análise, deve permitir ao administrador a configuração de permitir ou negar o acesso ao arquivo;

1.3.2. Módulo de Firewall de Host
1.3.2.1. Deve permitir a ativação/desativação do módulo de Firewall através da console;
1.3.2.2. Deve possuir um firewall de estação stateful bloqueando tráfego de entrada e controlando o tráfego de saída;
1.3.2.3. O módulo deve permitir a criação de regras de maneira adaptativa, ou seja, em uma estação modelo definida pelo administrador deve ser capaz de criar as regras de maneira automática;
1.3.2.4. Deve permitir inspeção do protocolo FTP;
1.3.2.5. O módulo de Firewall deve vir com regras pré-indicadas pelo próprio fabricante.
1.3.2.6. O módulo de Firewall deve permitir a criação de regras customizadas, com no mínimo os seguintes parâmetros:
1.3.2.6.1. Ação:
1.3.2.6.1.1. Bloquear;
1.3.2.6.1.2. Permitir;
1.3.2.6.2. Direção:
1.3.2.6.2.1. Ambas;
1.3.2.6.2.2. Entrada;
1.3.2.6.2.3. Saída;

CETESB

COMPANHIA AMBIENTAL DO ESTADO DE SÃO PAULO

DIVISÃO DE SUPRIMENTOS
SETOR DE APOIO AOS GESTORES DE CONTRATOS E DE CADASTRO DE PRODUTOS E FORNECEDORES

COTAÇÃO DE PREÇOS Nº 13/2026/326

1.3.2.6.3. Protocolo:
1.3.2.6.3.1. Protocolo IP;
1.3.2.6.3.2. IPv4;
1.3.2.6.4. Especificação da Rede:
1.3.2.6.4.1. Endereço IP;
1.3.2.6.4.2. Subnet;
1.3.2.6.4.3. Range;
1.3.2.6.4.4. FQDN;
1.3.2.6.5. Protocolo de Transporte:
1.3.2.6.5.1. Todos;
1.3.2.6.5.2. ICMP;
1.3.2.6.5.3. TCP;
1.3.2.6.5.4. UDP;
1.3.2.6.6. Agendamento:
1.3.2.6.6.1. Dias da semana;
1.3.2.6.6.2. Hora de início e fim;

1.4. Características de proteção para clientes Mac

1.4.1. Módulo Antimalware
1.4.1.1. Características da varredura ao acessar
1.4.1.1.1. A Varredura deve ser passível de habilitação/desativação por opção do administrador;
1.4.1.1.2. O administrador da solução deve especificar o tempo máximo de análise para um único arquivo;
1.4.1.1.3. A solução deve possuir conexão com Centro de Inteligência do fabricante, passível de ativação ou desativação por parte do administrador;
1.4.1.1.4. Deve permitir a configuração do nível de agressividade da análise;
1.4.1.1.5. Deve possibilitar aplicar as configurações a todos os processos do sistema operacional ou a uma lista específica criada pelo administrador;
1.4.1.1.6. Deve realizar varredura quando o processo:
1.4.1.1.6.1. Ler o disco;
1.4.1.1.6.2. Gravar no disco;
1.4.1.1.7. Deve possibilitar análise em:
1.4.1.1.7.1. Unidades de rede;
1.4.1.1.7.2. Arquivos compactados;
1.4.1.1.8. Deve detectar programas indesejados, ameaças em programas desconhecidos e ameaças em macro desconhecidas;
1.4.1.1.9. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar uma ameaça:
1.4.1.1.9.1. Limpar o arquivo;
1.4.1.1.9.2. Excluir o arquivo;
1.4.1.1.9.3. Negar acesso ao arquivo;
1.4.1.1.10. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar um programa indesejado:
1.4.1.1.10.1. Limpar o arquivo;
1.4.1.1.10.2. Excluir o arquivo;
1.4.1.1.10.3. Permitir acesso ao arquivo;
1.4.1.1.10.4. Negar acesso ao arquivo;
1.4.1.1.11. Deve possibilitar ao administrador a gestão de uma lista de exclusões;
1.4.1.2. Características da Varredura sob demanda

CETESB

COMPANHIA AMBIENTAL DO ESTADO DE SÃO PAULO

DIVISÃO DE SUPRIMENTOS
SETOR DE APOIO AOS GESTORES DE CONTRATOS E DE CADASTRO DE PRODUTOS E FORNECEDORES

COTAÇÃO DE PREÇOS Nº 13/2026/326

1.4.1.2.1. Deve ser possível realizar varreduras agendadas com periodicidade diária ou semanal.
1.4.1.2.2. Deve permitir a criação de repetição da tarefa.
1.4.1.2.3. Deve permitir definir a hora da execução da tarefa de análise;
1.4.1.2.4. Deve permitir a criação da tarefa de varredura de maneira aleatória;
1.4.1.2.5. Deve permitir a realização de varreduras agendadas após logon do usuário ou durante inicialização do sistema operacional.
1.4.1.2.6. Deve permitir escolher (um ou mais) os alvos da varredura, dentre eles:
1.4.1.2.6.1. Os locais da varredura:
1.4.1.2.6.1.1. Todas as unidades fixas;
1.4.1.2.6.1.2. Todas as unidades removíveis;
1.4.1.2.6.1.3. Todas as unidades mapeadas;
1.4.1.2.6.1.4. Pasta de perfil do usuário;
1.4.1.2.6.1.5. Arquivo ou pasta especificada pelo administrador;
1.4.1.2.6.2. Os tipos de arquivos que serão analisados;
1.4.1.2.6.3. Opções adicionais, como por exemplo detecção de programas indesejados, ameaças em programas desconhecidos e ameaças em macro desconhecidas.
1.4.1.2.6.4. Áreas de exclusão que não deverão ser varridas;
1.4.1.2.7. Deve permitir a integração com o Centro de Inteligência do fabricante durante a varredura agendada.
1.4.1.2.8. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar uma ameaça:
1.4.1.2.8.1. Limpar o arquivo;
1.4.1.2.8.2. Excluir o arquivo;
1.4.1.2.8.3. Continuar varredura;
1.4.1.2.9. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar um programa indesejado:
1.4.1.2.9.1. Limpar o arquivo;
1.4.1.2.9.2. Excluir o arquivo;
1.4.1.2.9.3. Continuar varredura;
1.4.1.2.10. Para minimizar o impacto ao usuário, a solução deve permitir:
1.4.1.2.10.1. Utilização de cache, ou seja, arquivos que já foram analisados e não tiveram seu conteúdo alterado não serão novamente analisados;
1.4.1.2.10.2. Iniciar a varredura apenas quando o sistema estiver ocioso ou diminuir a agressividade conforme o uso de memória;

1.4.2. Firewall de Host
1.4.2.1. Deve permitir a ativação/desativação do módulo de Firewall através da console;
1.4.2.2. Deve possuir um firewall de estação stateful bloqueando tráfego de entrada e controlando o tráfego de saída;
1.4.2.3. O módulo deve permitir a criação de regras de maneira adaptativa, ou seja, em uma estação modelo definida pelo administrador deve ser capaz de criar as regras de maneira automática;
1.4.2.4. Deve permitir inspeção do protocolo FTP;
1.4.2.5. O módulo de Firewall deve vir com regras pré-indicadas pelo próprio fabricante.
1.4.2.6. O módulo de Firewall deve permitir a criação de regras customizadas, com no mínimo os seguintes parâmetros:
1.4.2.6.1. Ação:
1.4.2.6.1.1. Bloquear;
1.4.2.6.1.2. Permitir;
1.4.2.6.2. Direção:

CETESB

COMPANHIA AMBIENTAL DO ESTADO DE SÃO PAULO

DIVISÃO DE SUPRIMENTOS
SETOR DE APOIO AOS GESTORES DE CONTRATOS E DE CADASTRO DE PRODUTOS E FORNECEDORES

COTAÇÃO DE PREÇOS Nº 13/2026/326

1.4.2.6.2.1. Ambas;
1.4.2.6.2.2. Entrada;
1.4.2.6.2.3. Saída;
1.4.2.6.3. Protocolo:
1.4.2.6.3.1. Protocolo IP;
1.4.2.6.3.2. IPv4;
1.4.2.6.4. Especificação da rede:
1.4.2.6.4.1. Endereço IP;
1.4.2.6.4.2. Subnet;
1.4.2.6.4.3. Range;
1.4.2.6.4.4. FQDN;
1.4.2.6.5. Protocolo de transporte:
1.4.2.6.5.1. ICMP;
1.4.2.6.5.2. TCP;
1.4.2.6.5.3. UDP;
1.4.2.6.6. Aplicações;

1.4.3. Módulo de Filtragem Web
1.4.3.1. Deve permitir o controle de browsers suportados, dentre eles:
1.4.3.1.1. Chrome;
1.4.3.1.2. Firefox;
1.4.3.1.3. Edge;
1.4.3.2. Deve ser capaz de utilizar lista de categorias para bloqueio de sites relacionados ao conteúdo não autorizado;
1.4.3.3. Deve possuir, no mínimo, duas das seguintes categorias:
1.4.3.3.1. Browser exploits;
1.4.3.3.2. Download maliciosos;
1.4.3.3.3. Sites maliciosos;
1.4.3.3.4. Phishing;
1.4.3.3.5. Pornografia;
1.4.3.3.6. Hacking/Computer Crime;
1.4.3.3.7. Spyware/Adware/Keyloggers;
1.4.3.3.8. Anonymizer;
1.4.3.4. Deve ser possível bloquear um site conforme a sua classificação de risco;
1.4.3.5. Deve ser possível bloquear um site quando este nunca foi visto pelo Centro de Inteligência do Fabricante;
1.4.3.6. Deve ser possível excluir endereços IP da análise;
1.4.3.7. Deve bloquear links que direcionem para sites com alto risco.
1.4.3.8. Deve permitir a customização das mensagens apresentadas para o usuário;

1.4.4. Módulo de Ameaças Avançadas
1.4.4.1. Não deve requerer conexão com centro de inteligência do fabricante para que a proteção seja ativada ou executada;
1.4.4.2. Solução deve manter um cache de reputação local com informações de aplicações - conhecidas, desconhecidas e maliciosas;
1.4.4.3. Deve ser capaz de informar ao usuário as ameaças encontradas através de mensagem customizada;
1.4.4.4. Deve ser possível atribuir a regra conforme política equilibrada, visando maior segurança ou produtividade do usuário;

1.4.5. Módulo de Controle de Dispositivos

CETESB

COMPANHIA AMBIENTAL DO ESTADO DE SÃO PAULO

DIVISÃO DE SUPRIMENTOS
SETOR DE APOIO AOS GESTORES DE CONTRATOS E DE CADASTRO DE PRODUTOS E FORNECEDORES

COTAÇÃO DE PREÇOS Nº 13/2026/326

1.4.5.1. Deve controlar o uso de dispositivos por parte dos usuários, como por exemplo Mídias Removíveis, Unidades USB, DVDs, e CDs regraváveis;
1.4.5.2. Deve permitir a configuração dos dispositivos nos modos:
1.4.5.2.1. Bloqueio, ou;
1.4.5.2.2. Somente leitura;
1.4.5.3. Deve classificar os dispositivos em duas categorias:
1.4.5.3.1. Gerenciado;
1.4.5.3.2. Não gerenciado;
1.4.5.4. Deve ser capaz de identificar o dispositivo (plug and play) através das seguintes informações:
1.4.5.4.1. Tipo de BUS;
1.4.5.4.2. ID do fabricante (Vendor ID);
1.4.5.4.3. ID do produto (Product ID);
1.4.5.5. Deve ser capaz de identificar Dispositivos Removíveis através das seguintes informações:
1.4.5.5.1. Tipo de BUS;
1.4.5.5.2. Tipo de sistema de arquivo;
1.4.5.6. Deve ser possível habilitar ou desabilitar uma determinada regra de proteção uma vez que esteja dentro da rede (Exemplo: Quando conectado à rede do órgão libera o uso de pen-drive);

1.5. Características do módulo de reputação de arquivos e compartilhamento de informações de segurança

1.5.1. A solução deve possuir capacidade de criar uma reputação local, além de utilizar uma já existente em nuvem através da catalogação de todos os executáveis existentes no ambiente;
1.5.2. O servidor de reputação deverá habilitar a troca de informação de ameaças entre os endpoints e servidores protegidos.
1.5.3. Este módulo deverá habilitar um protocolo de troca de informações de ameaças que permita o intercâmbio de informações entre soluções do mesmo fabricante e de fabricantes terceiros;
1.5.4. A solução deverá apresentar a reputação dos arquivos definida para cada um dos ativos conectados, dentre eles:
1.5.4.1. Reputação local;
1.5.4.2. Reputação do centro de inteligência;
1.5.5. Ao catalogar um arquivo, a solução deve apresentar, no mínimo as seguintes informações:
1.5.5.1. Nome do arquivo;
1.5.5.2. Caminho do arquivo;
1.5.5.3. Hash;
1.5.5.4. Primeira visualização do arquivo na rede;
1.5.5.5. Tamanho do arquivo;
1.5.6. Caso o arquivo tenha como origem a Internet, a solução deverá ser capaz de informar a partir de qual URL o arquivo foi obtido e a reputação desta última;
1.5.7. Deve ser possível realizar uma pesquisa do arquivo em base de conhecimento de terceiros (exemplo: Virus Total);
1.5.8. Após análise pela solução o administrador deve ter a possibilidade de:
1.5.8.1. Rastrear em quais estações o arquivo foi executado;
1.5.8.2. Identificar o arquivo como confiável;
1.5.8.3. Identificar o arquivo como desconhecido;
1.5.8.4. Identificar o arquivo como malicioso
1.5.9. Para minimizar o impacto a solução deve ter a capacidade de ser ativada no modo de observação nos endpoints e servidores protegidos;

CETESB

COMPANHIA AMBIENTAL DO ESTADO DE SÃO PAULO

DIVISÃO DE SUPRIMENTOS
SETOR DE APOIO AOS GESTORES DE CONTRATOS E DE CADASTRO DE PRODUTOS E FORNECEDORES

COTAÇÃO DE PREÇOS Nº 13/2026/326

1.5.10. Deve ser possível bloquear a execução de arquivos nunca vistos ou suspeitos no ambiente e informar o usuário por meio de mensagem;
1.5.11. Deve ser capaz de identificar manualmente um arquivo como malicioso impedindo sua execução no ambiente;
1.5.12. Deve ser gerenciado pela mesma console de gerenciamento da solução de proteção de endpoints e servidores;

1.6. Características da solução de detecção e resposta a incidentes

1.6.1. Capacidade de detectar e responder a incidentes relacionadas a ameaças avançadas, com capacidade avançada de investigação e que permita ao gestor da solução rápida resposta;
1.6.2. Deve permitir por meio de severidade dos alertas que o operador da solução facilmente entenda a ameaça e priorize o tratamento;
1.6.3. Deve facilitar a operação por meio de guias de investigação que automaticamente coleta, sumariza e visualmente evidencie, por meio de fontes diversas, a interação conforme a investigação avance;
1.6.4. A ferramenta deve possuir capacidade de monitoramento contínuo em tempo real;
1.6.5. Deve possuir base de dados analítica na nuvem, permitindo uma adoção mais rápida e otimizada das novas técnicas e motores analíticos para auxiliar na detecção de ameaça;
1.6.6. A ferramenta deve possuir mapeamento do framework do MITRE ATT&CK para determinar a fase de uma determinada ameaça, risco associado e que com base nestas informações auxilie na priorização de uma resposta;
1.6.7. Os guias de investigação devem utilizar inteligência artificial para auxiliar na identificação dos principais problemas detectados que identifiquem a causa raiz do ataque;
1.6.8. A solução poderá ser composta por mais de um endpoint do mesmo fabricante, a fim de atender a todos os requisitos previstos neste Edital;
1.6.8.1. No caso da solução ser composta por mais de um endpoint, a console de gerenciamento deverá ser única e integrada
1.6.9. A solução deverá prover buscas diversas, abrangendo:
1.6.9.1. Busca histórica, permitindo a visibilidade, em detalhes, dos indicadores de comprometimento e indicadores de ataque. A informação deverá estar disponível mesmo que o dispositivo investigado esteja desligado;
1.6.9.2. Busca tempo real, permite o acesso em tempo real ao dispositivo investigado em busca de uma determinada informação;
1.6.9.3. Busca sob demanda, para suplementar uma investigação, deve permitir a captura de uma imagem (snapshot) do dispositivo investigado, permitindo que esta imagem seja capturada de máquinas gerenciadas e não gerenciadas;
1.6.10. A gestão dos dispositivos, pode ser feita por meio de console:
1.6.10.1. On-Premise: Toda camada de comunicação e gestão dos agentes é instalada no ambiente, entretanto a console de investigação está na nuvem do fabricante (SaaS);
1.6.10.2. SaaS: Toda camada de comunicação e gestão dos agentes é gerenciada na nuvem do fabricante, em conjunto com a console de investigação;
1.6.11. Deve suportar sistemas operacionais nas arquiteturas 32-bits e 64-bits para os agentes, dentre os sistemas, deverão suportar, no mínimo:
1.6.11.1. Windows 8 ou superior;
1.6.11.2. Windows Server 2012 (64-bits) ou superior;
1.6.12. MacOS
1.6.12.1. Catalina 10.15.6 e superiores;
1.6.13. Linux
1.6.13.1. Oracle Linux 7x (64-bits) e superiores;
1.6.13.2. Red Hat 7.x (64-bits) e superiores;
1.6.13.3. CentOS 7.x (64-bits) e superiores;

CETESB

COMPANHIA AMBIENTAL DO ESTADO DE SÃO PAULO

DIVISÃO DE SUPRIMENTOS
SETOR DE APOIO AOS GESTORES DE CONTRATOS E DE CADASTRO DE PRODUTOS E FORNECEDORES

COTAÇÃO DE PREÇOS Nº 13/2026/326

1.6.14. A solução deve possuir capacidade investigativa, informando:
- 1.6.14.1. Total de investigações abertas;
- 1.6.14.2. Novas Investigações por dia;
- 1.6.14.3. Principais detecções;
- 1.6.14.4. Quantidade de investigações com prioridade alta;
- 1.6.14.5. Quantidade de investigações fechadas;
- 1.6.14.6. Quantidade de investigações em aberto;

1.6.15. A solução deverá possuir um painel de alertas, contendo os principais “achados” (findings) detectados pela solução;
- 1.6.15.1. Deverá dividir os alertas por prioridade;

1.6.16. O painel de alerta, deverá possuir integração com o Framework do MITRE ATT&CK, apresentando:
- 1.6.16.1. Data, hora e ano da ocorrência;
- 1.6.16.2. Linha de comando envolvida;
- 1.6.16.3. Táticas e técnicas;
- 1.6.16.4. Ativo envolvido;
- 1.6.16.5. Nome do Processo;
- 1.6.16.6. Indicadores Suspeitos, com detalhes;

1.6.17. O Painel de Alertas deverá permitir ao analista, que este possa visualizar, em mais detalhes o alerta, apresentando:
- 1.6.17.1. Versão do sistema operacional;
- 1.6.17.2. Endereço IP;
- 1.6.17.3. Usuário logado;

1.6.18. Na busca em modo histórico, ao selecionar um dos dispositivos gerenciados, deverá apresentar:
- 1.6.18.1. Detecções e alertas, contendo:
  - 1.6.18.1.1. Data, hora e ano;
  - 1.6.18.1.2. ID do processo envolvido;
  - 1.6.18.1.3. Nome do processo;
  - 1.6.18.1.4. Linha de comando;
  - 1.6.18.1.5. Usuário;
  - 1.6.18.1.6. Táticas e técnicas;
- 1.6.18.2. Histórico de execução de processos;
- 1.6.18.3. Manipulação de arquivos;
- 1.6.18.4. Detecção de scripts;
- 1.6.18.5. Ferramentas administrativas ou hacking;
- 1.6.18.6. Alteração dos serviços do sistema operacional;
- 1.6.18.7. Conexão de rede;
- 1.6.18.8. Tarefas agendadas;
- 1.6.18.9. Requisições de DNS;
- 1.6.18.10. Atividade de logon;

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

1.6.20. O fabricante deverá disponibilizar coletores para, no mínimo, a coleta das seguintes informações nos dispositivos gerenciados:
- 1.6.20.1. Registro do Windows;
- 1.6.20.2. Perfil dos usuários;
- 1.6.20.3. Softwares instalados;
- 1.6.20.4. Serviços do sistema operacional;
- 1.6.20.5. Tarefas agendadas;
- 1.6.20.6. Processos em execução;
- 1.6.20.7. Flows de rede;

CETESB

COMPANHIA AMBIENTAL DO ESTADO DE SÃO PAULO

DIVISÃO DE SUPRIMENTOS
SETOR DE APOIO AOS GESTORES DE CONTRATOS E DE CADASTRO DE PRODUTOS E FORNECEDORES

COTAÇÃO DE PREÇOS Nº 13/2026/326

1.6.20.8. Usuários logados;
1.6.20.9. Updates do Windows instalados;
1.6.21. Ferramenta deve permitir que coletores customizados sejam criados para as plataformas suportadas;
1.6.22. A criação de coletores customizados deve utilizar linguagem comum aos sistemas, como por exemplo:
1.6.22.1. Powershell;
1.6.22.2. Python;
1.6.22.3. Visual Basic;
1.6.22.4. Bash;
1.6.22.5. Comandos do sistema operacional;
1.6.23. A busca em tempo real, ao se obter o resultado desejado, deve permitir que se aplique reações, frente a busca realizada;
1.6.24. As reações devem conter:
1.6.24.1. Isolamento de um endpoint;
1.6.24.2. Encerrar um processo;
1.6.24.3. Remover um arquivo;
1.6.24.4. Logoff do usuário logado;
1.6.25. Deve permitir a criação de reações customizadas para atuar em conjunto com a busca realizada e seu respectivo resultado;
1.6.26. A busca em tempo real deve possuir capacidade de sugerir os parâmetros de busca para facilitar a obtenção do resultado desejado;
1.6.27. Caso a busca tenha um erro em sua sintaxe, a console deverá emitir um alerta de erro. Caso contrário, apresentar que a busca é válida;
1.6.28. Deve apresentar a quantidade de hosts que receberam o comando de busca em tempo real;
1.6.29. Deve prover registro do histórico de ações executados com as seguintes informações em tela:
1.6.29.1. Dispositivo;
1.6.29.2. Ação;
1.6.29.3. Sistema operacional;
1.6.29.4. Endereço IP;
1.6.30. Deve ser capaz de apresentar, no mínimo, as seguintes informações após a busca:
1.6.30.1. Endereço IP;
1.6.30.2. Hash do processo em execução;
1.6.30.3. ID do processo;
1.6.30.4. Status da transação TCP;
1.6.30.5. Número da porta que originou o pacote de rede;
1.6.30.6. Nome do arquivo;
1.6.30.7. Última data de gravação do arquivo;
1.6.30.8. Data de criação e exclusão do arquivo;
1.6.30.9. Comando que iniciou o processo;
1.6.30.10. Caminho e valor da chave de registro;
1.6.31. Cada porção de dado coletado pela solução para apresentação no painel de investigação, deve ficar disponível por até 30 dias;
1.6.32. Ao acessar um caso de investigação, a solução deverá apresentar, de maneira sumarizada, a quantidade de artefatos descoberta, a quantidade de artefatos chave e a quantidade de pontos chave no qual o operador da solução deve focar;
1.6.33. Por meio de painéis interativos (widgets) a solução deve prover informações relacionadas a:
1.6.33.1. Itens investigados: Sumário contendo a quantidade de dispositivos envolvidos, contas de usuário, endereços IPs, DNS, FQDN, processos, serviços, arquivos e conexões de rede;
1.6.33.2. Investigações correlacionadas;
1.6.33.3. Guias de investigações: Os guias de investigação deverão ser baseados em:

CETESB

COMPANHIA AMBIENTAL DO ESTADO DE SÃO PAULO

DIVISÃO DE SUPRIMENTOS
SETOR DE APOIO AOS GESTORES DE CONTRATOS E DE CADASTRO DE PRODUTOS E FORNECEDORES

COTAÇÃO DE PREÇOS Nº 13/2026/326

1.6.33.3.1. Perguntas respondidas: Contendo as principais perguntas que devem ser respondidas pelos analistas, como por exemplo: Quais processos desconhecidos em execução foram encontrados? Existe algum processo abrindo alguma comunicação de rede que não é comum? Existe processo em execução com nome randomizado? Existe alguma evidência de uso de ferramentas de hacking ou admin?;
1.6.33.3.2. Questões Mitre: deve relacionar as principais respostas do MITRE framework relacionadas a evidências encontradas;
1.6.33.3.3. Hipótese: indicativo de comportamento anômalo baseado em hipótese com base em perguntas chave (Inteligência Artificial);
1.6.33.4. Visualização geral da investigação:
1.6.33.4.1. Gráfica: Apresentação em formato gráfico com os links de relacionamento entre todos os artefatos encontrados. A visualização gráfica deve se moldar, permitindo o drill-down desde o montante total de artefatos descobertos até os achados principais;
1.6.33.4.2. Deve ser possível identificar os relacionamentos entre entidades externas e entidades internas;
1.6.33.4.3. Deve ser possível agrupar os artefatos descobertos e os principais indícios por grupo, para facilitar a visualização;
1.6.33.4.4. Deve ser possível filtrar o gráfico dentre as opções:
1.6.33.4.4.1. Dispositivo;
1.6.33.4.4.2. Arquivo;
1.6.33.4.4.3. Conexão de rede;
1.6.33.4.4.4. Processo;
1.6.33.4.4.5. Serviço;
1.6.33.4.5. Ao interagir com algum dos indícios encontrados, a solução de investigação deverá apresentar um widget na qual deverá apresentar mais detalhes sobre os indicativos, inclusive permitindo a interação por meio de ações, como por exemplo:
1.6.33.4.5.1. Capturar uma imagem da máquina;
1.6.33.4.5.2. Isolar a máquina da rede;
1.6.33.4.5.3. Buscar um processo executado em outras máquinas monitoradas;
1.6.33.4.6. Dispositivos: Dispositivos afetados, incluindo nome, versão do sistema operacional, identificador e o status;
1.6.33.5. Deverá possuir um painel de monitoramento onde a incidência de atividade maliciosa deve ser apresentada;
1.6.33.6. Para cada artefato malicioso monitorado, deve apresentar:
1.6.33.6.1. Painel de ação;
1.6.33.6.2. Painel com detalhes do processo;
1.6.33.6.3. Parar um processo;
1.6.33.6.4. Parar e remover;
1.6.33.6.5. Colocar em quarentena a estação de trabalho;
1.6.33.7. Painel de comportamento:
1.6.33.7.1. Apresentar as técnicas observadas e compará-las a matriz do Mitre;
1.6.33.7.2. Apresentar os indicadores suspeitos identificados;
1.6.33.8. Deve apresentar a interação dos processos de maneira sequencial, temporal e detalhado.
1.6.33.9. Deve possuir auxílio de Inteligência Artificial generativa para análise dos incidentes gerados;
1.6.33.9.1. A análise por IA deve permitir a sumarização completa do incidente, além da interação com o administrador para obtenção das seguintes respostas:
1.6.33.9.1.1. Detalhamento do incidente;
1.6.33.9.1.1.1. Resumo do incidente, de forma textual;

CETESB

COMPANHIA AMBIENTAL DO ESTADO DE SÃO PAULO

DIVISÃO DE SUPRIMENTOS
SETOR DE APOIO AOS GESTORES DE CONTRATOS E DE CADASTRO DE PRODUTOS E FORNECEDORES

COTAÇÃO DE PREÇOS Nº 13/2026/326

1.6.33.9.1.1.2. Processos envolvidos;
1.6.33.9.1.1.3. Relação entre os eventos;
1.6.33.9.1.1.4. Conexões de rede observadas;
1.6.33.9.1.2. Relação dos TTPs (Mitre Attack) associados, incluindo:
1.6.33.9.1.2.1. Descrição
1.6.33.9.1.2.2. Ações observadas no incidente
1.6.33.9.1.2.3. Táticas relacionadas
1.6.33.9.1.3. Sugestão de ações recomendadas para tratativa do incidente, incluindo:
1.6.33.9.1.3.1. Investigação de processos
1.6.33.9.1.3.2. Análise de conexões de rede
1.6.33.9.1.3.3. Preservação de evidências
1.6.33.9.1.4. Detalhamento de informações do dispositivo envolvido
1.6.33.9.1.4.1. Nome do dispositivo
1.6.33.9.1.4.2. Usuário
1.6.33.9.1.4.3. Nome e versão do Sistema Operacional
1.6.33.9.1.4.4. Interfaces de rede
1.6.33.9.1.5. Criação e formatação de um e-mail descritivo do incidente para envio ao usuário ofensor, contendo no mínimo:
1.6.33.9.1.5.1. Detalhes sobre o dispositivo: nome, Sistema Operacional e data do último boot.
1.6.33.9.1.5.2. Detalhes sobre o processo e/ou arquivo malicioso detectado
1.6.33.9.1.5.2.1. Data da primeira detecção
1.6.33.9.1.5.2.2. Linha de comando de execução
1.6.33.9.1.5.2.3. ID do processo
1.6.33.9.1.5.2.4. Conexões de rede efetuadas
1.6.33.9.1.5.2.5. Hash
1.6.33.9.1.5.2.6. Caminho do arquivo no sistema
1.6.33.9.1.5.2.7. Usuário
1.6.33.9.1.5.3. Sugestão de perguntas e questionamentos que devem ser enviados ao usuário para descrição do contexto da máquina no momento do incidente.
1.6.33.10. Deve ser possível a definição na IA para que as respostas dadas estejam em português-BR.

1.7. Módulo de análise avançada de artefatos (Sandbox)

1.7.1. Características gerais

1.7.1.1. O serviço deve fornecer um módulo de análise avançada de hashes, arquivos e URLs hospedada em nuvem.
1.7.1.1.1. A manutenção da solução é de responsabilidade do fabricante, no modelo conhecido como Software as a Service (SaaS);
1.7.1.2. Deve ser possível executar e examinar ataques com segurança usando malware avançado, ameaças de dia zero e ameaças persistentes avançadas (APTs) incorporadas em páginas da Web, anexos de e-mail e arquivos;
1.7.1.3. Deve ser possível realizar submissão manual e automatizada de hashes;
1.7.1.4. Deve ser possível realizar submissão manual e automatizada de arquivos;
1.7.1.5. Deve ser possível realizar submissão manual e automatizada de URLs;
1.7.1.6. Deve ser possível a integração com a solução de proteção de endpoints e EDR, especificada neste Termo de Referência, para receber arquivos para análise.
1.7.1.7. A solução deve ser dimensionada para 2300 usuários.
1.7.1.8. A solução deve oferecer capacidades pré-execução, que visem evitar uma submissão para arquivos já conhecidos;

CETESB

COMPANHIA AMBIENTAL DO ESTADO DE SÃO PAULO

DIVISÃO DE SUPRIMENTOS
SETOR DE APOIO AOS GESTORES DE CONTRATOS E DE CADASTRO DE PRODUTOS E FORNECEDORES

COTAÇÃO DE PREÇOS Nº 13/2026/326

1.7.1.9. A solução deve ser capaz de rastrear e evidenciar ações desencadeadas pela detonação de URLs, sejam essas uma abertura de página ou um download de arquivos;
1.7.1.10. Deve fornecer uma visão completa de um ataque, desde a exploração inicial até a destinos de retorno de chamada e siga em tentativas de download binário;
1.7.1.11. O código suspeito deve ser totalmente executado em um ambiente de análise virtual Microsoft Windows e Apple Mac OS X e Linux;
1.7.1.12. Deve permitir a importação de regras YARA personalizadas para definir regras no nível de byte e analisar rapidamente objetos suspeitos relacionados a ameaças;
1.7.1.13. Deve incluir perfis de ataque de malware gerados pela análise de malware, como identificadores de código de malware, URLs de exploração e outras fontes de infecção e ataque;
1.7.1.14. Deve possuir vários perfis de Sistemas Operacionais para realizar a análise, contendo no mínimo:
1.7.1.14.1. CentOS;
1.7.1.14.2. Windows XP;
1.7.1.14.3. Windows 7;
1.7.1.14.4. Windows 10;
1.7.1.14.5. Mac OSX.
1.7.1.15. Deve possuir o detalhamento das seguintes informações dos artefatos analisados:
1.7.1.15.1. Artefatos maliciosos;
1.7.1.15.2. Gráficos e tabelas de eventos;
1.7.1.15.3. Detalhes de macro;
1.7.1.15.4. Parâmetros de execução;
1.7.1.15.5. Associação com o framework MITRE ATT&CK;
1.7.1.15.6. Visualizações de arquivos hexadecimais;
1.7.1.15.7. Capturas de tela;
1.7.1.15.8. Pacotes de rede.
1.7.1.16. Deve permitir a customização do host em parâmetros como:
1.7.1.16.1. Conta de Outlook e Skype;
1.7.1.16.2. FTP;
1.7.1.16.3. Linguagem do SO;
1.7.1.16.4. Timezone do SO;
1.7.1.16.5. Entradas DNS cache;
1.7.1.16.6. Host File;
1.7.1.16.7. Definição de variáveis Honeypot (Credenciais, arquivos, diretórios);
1.7.1.16.8. Definições de ambiente (Domínio, Hostname, Username);
1.7.1.16.9. Arquivos temporários (Windows Recent, Office Recent).
1.7.1.17. Deve permitir a integração nativa com componentes de cloud via API, possuindo no mínimo as seguintes integrações:
1.7.1.17.1. Via RestfulAPI;
1.7.1.17.2. Via Scripts (Python);
1.7.1.17.3. Via PostMan;
1.7.1.17.4. Microsoft Power Automate;
1.7.1.17.5. Slack e Slack Enterprise;
1.7.1.17.6. BOX (Cloud Storage);
1.7.1.17.7. Microsoft Teams, Sharepoint e Onedrive;
1.7.1.17.8. Dropbox;
1.7.1.17.9. Webex,
1.7.1.17.10. Google Chrome Extension;
1.7.1.17.11. Amazon AWS S3;
1.7.1.17.12. Azure Blob Storage;

CETESB

COMPANHIA AMBIENTAL DO ESTADO DE SÃO PAULO

DIVISÃO DE SUPRIMENTOS
SETOR DE APOIO AOS GESTORES DE CONTRATOS E DE CADASTRO DE PRODUTOS E FORNECEDORES

COTAÇÃO DE PREÇOS Nº 13/2026/326

1.7.1.17.13. GCP Storage.
1.7.1.18. Deve oferecer documentação online de referência sobre os comandos de utilização da API;
1.7.1.19. Deve oferecer experiência de detonação com emulação de comportamentos similares ao comportamento humano, como abertura de documentos e outras técnicas capazes de revelar malwares com características anti-evasão;
1.7.1.20. Deve permitir notificações via SMTP e HTTP;
1.7.1.21. Deve oferecer relatórios no mínimo no formato PDF;
1.7.1.22. Deve oferecer relatórios dinâmicos na console e permitir a exportação (estática) do relatório em PDF
1.7.1.23. Os relatórios dinâmicos ou em PDF devem fornecer minimamente:
1.7.1.23.1. Visão Geral: Detalhes sobre a detecção, Screenshots, Análise gráfica da arvore de processos, injeção de comandos e parâmetros com as devidas assinaturas ou comportamentos suspeitos/maliciosos encontrados
1.7.1.23.2. Lista de Detecções: Comportamentos suspeitos/maliciosos detectados
1.7.1.23.3. Objetos Extraídos: Objetos e ações desencadeadas pela detonação
1.7.1.23.4. Associação com Mitre Framework Att&ck
1.7.1.23.5. Arquivos descarregados: Detalhes sobre os arquivos obtidos de fontes externas
1.7.1.23.6. Processos Observados: Detalhes sobre os processos listados no SO mediante detonação
1.7.1.23.7. Alterações e ações em nível de registro
1.7.1.23.8. Chamadas de API para fontes externas
1.7.1.23.9. Chamadas e conexões de Rede para fontes externas
1.7.1.23.10. Busca por string: pesquisa objetiva (live Search) por todas as informações contidas no relatório;
1.7.1.23.11. Levantamento dos Indicadores de Comprometimento IoCs
1.7.1.23.12. Coleta de Artefatos e obtenção material de:
1.7.1.23.12.1. Vídeo da captura VNC;
1.7.1.23.12.2. PCAP da comunicação;
1.7.1.23.12.3. Arquivos (IoCs, descarregados, etc).
1.7.1.23.12.4. Sumário de atividades maliciosas: status da detecção (malicioso ou não), número de regras, arquivos, registros, chamadas (API, Rede), Hashes (MD5, SHA1, SHA256)
1.7.1.24. Deve permitir gerar um PCAP como parte do processo de detalhamento da análise;
1.7.1.25. Deve ter a capacidade de reproduzir um vídeo no formato MP4 como parte do processo de análise de detalhes;
1.7.1.26. Deve ser capaz de prover acesso interativo ao host, durante a detonação, via visualização remota em sistemas Windows;

1.8. Características do módulo de gerenciamento

1.8.1. Deve ser disponibilizado em solução local (on-premise) ou em nuvem;
1.8.2. Solução de gerenciamento on-premise:
1.8.2.1. Deve suportar a instalação nos seguintes sistemas operacionais:
1.8.2.1.1. Windows Server 2012 ou superiores;
1.8.2.2. A arquitetura dos sistemas operacionais deve ser 64-bits;
1.8.2.3. Deve suportar a instalação em Cluster Microsoft;
1.8.2.4. Deve suportar a virtualização do sistema operacional com base nos seguintes hypervisors:
1.8.2.4.1. Microsoft Hyper-V;
1.8.2.4.2. VMware ESX;
1.8.2.5. Deve possuir suporte a uma das seguintes bases de dados:
1.8.2.5.1. SQL Server 2014 ou superior;

CETESB

COMPANHIA AMBIENTAL DO ESTADO DE SÃO PAULO

DIVISÃO DE SUPRIMENTOS
SETOR DE APOIO AOS GESTORES DE CONTRATOS E DE CADASTRO DE PRODUTOS E FORNECEDORES

COTAÇÃO DE PREÇOS Nº 13/2026/326

1.8.2.5.2. SQL Express;
1.8.2.5.3. Oracle 12c ou superior;
1.8.2.5.4. Oracle Express;
1.8.2.5.5. Base de dados próprias;
1.8.2.6. Deve ser possível segregar a instalação da solução em:
1.8.2.6.1. Servidor console central;
1.8.2.6.2. Servidor base de dados;
1.8.2.6.3. Servidor de interação com os agentes;
1.8.2.6.4. Agentes distribuidores de vacina;
1.8.2.7. Permitir a instalação dos módulos da solução a partir de um único servidor;
1.8.2.8. Suportar o uso de múltiplos repositórios para atualização de produtos e arquivo de vacina com replicação seletiva;
1.8.3. A console de gerência deve ser acessada via WEB;
1.8.4. Deve possuir compatibilidade com os seguintes browsers:
1.8.4.1. Chrome;
1.8.4.2. Firefox;
1.8.4.3. Edge;
1.8.5. Permitir a alteração das configurações dos módulos da solução nos clientes de maneira remota;
1.8.6. Permitir a atualização incremental da lista de definições de vírus nos clientes, a partir de um único ponto da rede local;
1.8.7. Deve permitir a visualização das características básicas de hardware das máquinas;
1.8.8. Integração e importação automática da estrutura de domínios do Active Directory já existentes na rede local;
1.8.9. Permitir a criação de tarefas de atualização, verificação de vírus e upgrades em períodos pré-determinados, na inicialização do sistema operacional ou no logon na rede;
1.8.10. Permitir o armazenamento das informações coletadas nos clientes em um banco de dados centralizado;
1.8.11. Permitir diferentes níveis de administração do servidor, de maneira independente do login da rede;
1.8.12. Suporte a múltiplos usuários, com diferentes níveis de acesso e permissões aos produtos gerenciados;
1.8.13. Criação de grupos de máquinas baseadas em regras definidas em função do número IP do cliente;
1.8.14. Permitir a criação de grupos virtuais através de marcadores;
1.8.15. Permitir aplicar as marcações nos sistemas por vários critérios incluindo: produtos instalados, versão de sistema operacional, quantidade de memória, dentre outros;
1.8.16. Forçar a configuração determinada no servidor para os clientes. Caso o cliente altere a configuração, ela deverá retornar ao padrão estabelecido no servidor, quando ela for verificada pelo agente;
1.8.17. A comunicação entre as máquinas clientes e o servidor de gerenciamento deve ser segura usando protocolo de autenticação HTTPS ou outro que garanta a confidencialidade da comunicação;
1.8.18. Forçar a instalação dos módulos da solução nos clientes;
1.8.19. A desinstalação dos módulos da solução deve ser bloqueada, mas em caso de desinstalação, os mesmos deverão ser reinstalados, quando o agente verificar o ocorrido;
1.8.20. O módulo de gestão deverá apresentar relatórios e dashboards consolidados para as soluções propostas neste termo de referência:
1.8.21. Deve ser possível realizar a customização dos relatórios gráficos gerados;
1.8.22. Exportação dos relatórios para os em um dos seguintes formatos: HTML, CSV, PDF, XML;
1.8.23. Geração de relatórios que contenham as seguintes informações:
1.8.23.1. Máquinas com a lista de definições de vírus desatualizada;
1.8.23.2. Qual a versão do software (inclusive versão gerenciada pela nuvem) instalado em cada máquina;
1.8.23.3. Os vírus que mais foram detectados;

CETESB

COMPANHIA AMBIENTAL DO ESTADO DE SÃO PAULO

DIVISÃO DE SUPRIMENTOS
SETOR DE APOIO AOS GESTORES DE CONTRATOS E DE CADASTRO DE PRODUTOS E FORNECEDORES

COTAÇÃO DE PREÇOS Nº 13/2026/326

1.8.23.4. As máquinas que mais sofreram infecções em um determinado período;
1.8.23.5. Os usuários que mais sofreram infecções em um determinado período;
1.8.24. A solução de gestão deve possuir dashboards no gerenciamento da solução;
1.8.25. Estes dashboards devem conter no mínimo todos os seguintes relatórios de fácil visualização:
1.8.25.1. Relatório dos últimos 30 (trinta) dias da detecção de códigos maliciosos;
1.8.25.2. Top 10 Computadores com infecções;
1.8.25.3. Top 10 Computadores com sites bloqueados pela política;
1.8.26. Gerenciar a atualização do antivírus em computadores portáteis (notebooks), automaticamente, mediante conexão em rede local ou remota (VPN);
1.8.27. Deve possuir uma base de inteligência global, do próprio fabricante, sobre campanhas de ameaças existentes;
1.8.28. Deve ser capaz de dar visibilidade sobre campanhas de ameaças globais com segregação por vertical de negócio;
1.8.29. Deve ser capaz de dar visibilidade sobre campanhas de ameaças globais com segregação por pais, incluindo o Brasil;
1.8.30. A solução deve ser capaz de proporcionar a busca em campanhas globais por ameaças baseadas em nome e/ou indicadores de compromisso IOC (Indicator Of Compromise);
1.8.31. Deve ser capaz de indicar quantos e quais dispositivos dentro da empresa estão vulneráveis a uma determinada campanha;
1.8.32. Deve ser capaz de mostrar o nível de postura de segurança da organização, em relação as campanhas de ameaças globais identificadas na base de inteligência do fabricante;
1.8.33. Deve ser capaz de propor procedimentos de mitigação dos riscos de segurança (playbooks) nos endpoints referentes a campanhas de ameaças específicas;
1.8.33.1. Estes procedimentos devem ser indicados para cada campanha, incluindo inclusive configurações em ferramentas terceiras, como o Active Directory.
1.8.34. Cada campanha identificada pela solução deverá possuir as seguintes informações:
1.8.34.1. Descrição;
1.8.34.2. IOCs;
1.8.34.3. Detalhes do impacto no ambiente;
1.8.34.4. Prevalência global;
1.8.34.5. Endpoints afetados.
1.8.34.6. Comportamento da ameaça.
1.8.35. Deve ser capaz de identificar em cada campanha de ameaça as técnicas utilizadas, relacionadas e mapeadas ao MITRE Framework;
1.8.36. Ter a capacidade de gerar registros/logs para auditoria;
1.8.37. A solução de gerenciamento deve ter a capacidade de atribuir etiquetas as máquinas, facilitando assim a distribuição automática dentro dos grupos hierárquicos na estrutura de gerenciamento.
1.8.38. A solução deve disponibilizar APIs para que sejam consumidas por terceiros, tanto de forma a coletar eventos ou logs, como realização de ações nos endpoints gerenciados.

2. Serviço de implantação e migração da solução para proteção de endpoints e servidores

2.1. Características Gerais

2.1.1. A PARTICIPANTE vencedora será inteiramente responsável pela instalação, atualização ou migração da solução antivírus atualmente em uso pela CONTRATANTE, bem como às despesas diretas ou indiretas para execução das atividades pela sua equipe técnica;
2.1.2. A instalação, atualização ou migração dos softwares em estações de trabalho poderá ser realizada remotamente, sem causar indisponibilidade do ambiente, devendo ser realizada em horários a serem definidos pela CONTRATANTE;

CETESB

COMPANHIA AMBIENTAL DO ESTADO DE SÃO PAULO

DIVISÃO DE SUPRIMENTOS
SETOR DE APOIO AOS GESTORES DE CONTRATOS E DE CADASTRO DE PRODUTOS E FORNECEDORES

COTAÇÃO DE PREÇOS Nº 13/2026/326

2.1.3. A instalação, atualização ou migração dos softwares em servidores de rede poderá ser realizada remotamente, devendo ser realizada em horários a serem definidos pela CONTRATANTE;
2.1.4. A CONTRATANTE poderá autorizar a instalação, atualização ou migração durante o horário de expediente se, ao seu exclusivo critério, entender que não oferece risco ao funcionamento de sua rede de computadores e serviços em produção;
2.1.5. O processo de instalação, atualização ou migração da solução deverá ser acompanhado por analistas da CONTRATANTE;
2.1.6. Para garantir que a instalação, atualização ou migração não afetará o ambiente da CONTRATANTE, os procedimentos e atividades deverão ser realizados por técnicos certificados pelo fabricante.

3. Serviço Gerenciado e Suporte Técnico

3.1. Serviço Gerenciado

3.1.1. As soluções ofertadas deverão ser gerenciadas, em termos de sustentação, pela CONTRATADA. Esta ficará responsável por manter os componentes necessários ao funcionamento da solução em perfeito estado, por meio de monitoramento e adoção de melhores práticas recomendadas pelo fabricante;
3.1.2. Deverá ocorrer a monitoração 24x7 do correto funcionamento dos produtos e componentes contidos no serviço e soluções contratados de acordo com os critérios a serem definidos entre a CONTRATADA e a CONTRATANTE;
  3.1.2.1. Os critérios a serem definidos devem garantir os serviços de confidencialidade, integridade e disponibilidade dos componentes das soluções que serão monitorados e os serviços sustentados por eles;
3.1.3. A CONTRATADA deverá prover alertas e comunicação de incidentes de segurança da informação diante dos eventos registrados no monitoramento;
  3.1.3.1. Os incidentes de disponibilidade são relacionados aos eventos de disponibilidade ou desempenho das soluções monitoradas, como por exemplo: solução indisponível, placa de rede desativada ou desconectada, disco rígido cheio, consumo médio de memória superior a 95%, média de utilização de CPU superior a 80%, dentre outros;
  3.1.3.2. A CONTRATANTE deverá ser informada sobre os incidentes detectados através do Portal de Atendimento, e-mail e/ou por telefone, conforme previamente acordado com o CONTRATANTE;
  3.1.3.3. Os serviços de monitoramento deverão permitir o estabelecimento de indicadores de DISPONIBILIDADE e DESEMPENHO dos ativos a serem monitorados;
  3.1.3.4. A CONTRATADA deverá coordenar o processo de alerta e escalonamento de incidentes, notificando à CONTRATANTE as ocorrências que possam afetar os níveis de serviço contratados;
  3.1.3.5. A CONTRATADA deverá prover suporte especializado e administração de sistemas e serviços de infraestrutura de TI necessários para o pleno funcionamento da Solução de Segurança;
3.1.4. Realizar a administração da infraestrutura da solução, incluindo, mas não se limitando a:
  3.1.4.1. Administrar e monitorar a disponibilidade e desempenho dos componentes envolvidos das soluções;
  3.1.4.2. Identificar necessidade de upgrade/downgrade dos equipamentos e ajustes/melhorias que possam impactar o funcionamento e performance da aplicação;
  3.1.4.3. Implementar melhorias no ambiente sob demanda e sugerir melhorias baseadas em melhores práticas de mercado, recomendações do fabricante ou no resultado do monitoramento contínuo da solução;
  3.1.4.4. Realizar rotinas de verificação dos sistemas e aplicações suportados, inclusive a implantação e manutenção de rotinas automáticas;

CETESB

COMPANHIA AMBIENTAL DO ESTADO DE SÃO PAULO

DIVISÃO DE SUPRIMENTOS
SETOR DE APOIO AOS GESTORES DE CONTRATOS E DE CADASTRO DE PRODUTOS E FORNECEDORES

COTAÇÃO DE PREÇOS Nº 13/2026/326

3.1.4.5. Esclarecimento de dúvidas, fornecimento de informações e/ou orientações técnicas, necessárias para a solução de problemas detectados na utilização dos produtos referenciados;
3.1.4.6. Gestão de níveis de serviço do serviço de gerenciamento da solução
3.1.4.7. Possuir sistema de chamados para controle, gerência, históricos e relatórios das atividades desenvolvidas;

3.1.5. Gerar relatórios personalizados conforme alinhamento com a CONTRATANTE no momento da ativação do serviço. O relatório deverá ser apresentado mensalmente em datas a serem definidas em comum acordo com a CONTRATANTE. Deverá conter, no mínimo:
3.1.5.1. Número de incidentes, solicitações e consultas efetuadas;
3.1.5.2. Disponibilidade dos componentes monitorados;
3.1.5.3. Disponibilidade das VPNs/links monitorados;
3.1.5.4. Lista dos principais tipos de ataques detectados;

3.1.6. A CONTRATADA deverá ter acesso a Rede Corporativa da CONTRATANTE através de VPN Site to Site e/ou Client to Site;

3.1.7. Garantir e manter durante a vigência do contrato o nível de parceria junto aos fabricantes da solução;
3.1.7.1. A CONTRATADA deverá possuir comprovante de parceria com os fabricantes das soluções, a serem comprovadas por meio de documento emitido pelo fabricante ou através do sítio eletrônico do mesmo;

3.2. Suporte Técnico

3.2.1. O serviço de suporte técnico objetiva a manutenção de todas as soluções em perfeitas condições de operação, incluindo assistência técnica, atualizações de versão e manutenção durante o período de vigência contratual.

3.2.2. A CONTRATADA deverá disponibilizar suporte técnico nas soluções ofertadas na modalidade 24x7, pelo período de garantia dos produtos;

3.2.3. O serviço de suporte deve ser prestado preferencialmente de maneira remota, sendo necessária a presença on-site nos casos em que o suporte remoto não seja suficiente para solução do problema.

3.2.4. Todos os técnicos de suporte da CONTRATADA devem ser capacitados pelo fabricante dos produtos a prestar atendimento de suporte técnico;

3.2.5. A CONTRATADA deverá disponibilizar acesso total ao conteúdo presente em área restrita de suporte no endereço eletrônico (web site) para todos os produtos que compõem a solução, contemplando toda a documentação técnica (guias de instalação/configuração atualizados, FAQs, com pesquisa efetuada por meio de ferramentas de busca), e atualizações (drivers, firmware e demais releases ofertados pelo fabricante);

3.2.6. Prestar suporte consultivo quando solicitado, serviço categorizado como não crítico, para criação, alteração ou exclusão de:
3.2.6.1. Configurações dos equipamentos/produtos;
3.2.6.2. Elaboração de relatórios;
3.2.6.3. Desenvolvimento de regras e automação de tarefas;
3.2.6.4. Integração de dispositivos;
3.2.6.5. Dúvidas e orientações quanto à administração da solução.

3.2.7. A abertura de chamados para Suporte Técnico será efetuada por correio eletrônico, via web ou por telefone. No caso de abertura por meio de telefone, o contato será efetuado por meio de número nacional isento de tarifação telefônica (por exemplo, prefixo 0800), ou número local da cidade ou município de disposição dos produtos, sendo que em qualquer um dos casos o atendimento deve ser efetuado em língua portuguesa;

3.2.8. É de competência do Suporte Técnico da CONTRATADA:

CETESB

COMPANHIA AMBIENTAL DO ESTADO DE SÃO PAULO

DIVISÃO DE SUPRIMENTOS
SETOR DE APOIO AOS GESTORES DE CONTRATOS E DE CADASTRO DE PRODUTOS E FORNECEDORES

COTAÇÃO DE PREÇOS Nº 13/2026/326

3.2.8.1. Cumprir as obrigações de manutenção e atualização de drivers, firmware e demais releases que venham a ser disponibilizadas, além de contemplar a correção de bugs, fixing e patches;
3.2.8.2. Cumprir obrigações de suporte técnico que incluem serviços de atendimento a dúvidas técnicas direto do fabricante;
3.2.8.3. Prestar suporte consultivo quando solicitado, serviço categorizado como não crítico, para criação, alteração ou exclusão de:
3.2.8.3.1. Configurações dos equipamentos/produtos;
3.2.8.3.2. Elaboração de relatórios;
3.2.8.3.3. Desenvolvimento de regras e automação de tarefas;
3.2.8.3.4. Integração de dispositivos;
3.2.8.3.5. Dúvidas e orientações quanto à administração da solução.
3.2.9. O suporte técnico deverá oferecer, no mínimo, as seguintes características:
3.2.9.1. Garantia de atendimento de número ilimitado de chamados;
3.2.9.2. Tempo máximo de espera para abertura do chamado após a comunicação do problema a Central de Atendimento: 30 (trinta) minutos;
3.2.10. Para a execução de atendimento, é necessária a autorização da CONTRATANTE para instalação ou desinstalação de quaisquer softwares, equipamentos ou componentes.

Assinaturas do documento

"Cotação de preços nº 13_2026_326"

Código para verificação: **Q6543BCJ**

Este documento foi assinado digitalmente pelos seguintes signatários nas datas indicadas:

GABRIELA BLEKER DE OLIVEIRA (CPF: ***.917.388-**) em 10/04/2026 às 09:06:08 (GMT-03:00)
Emitido por: "SolarBPM", emitido em 27/10/2025 - 08:28:01 e válido até 27/10/2028 - 08:28:01.
(Assinatura do Sistema)

Para verificar a autenticidade desta cópia, acesse o link https://e.ambiente.sp.gov.br/atendimento/conferenciaDocumentos e informe o processo **CETESB.021113/2025-87** e o código **Q6543BCJ** ou aponte a câmera para o QR Code presente nesta página para realizar a conferência.