TERMO DE REFERÊNCIA

1. **DESCRIÇÃO DO OBJETO:**

1.1. Contratação de empresa para fornecimento de licenças de antivírus com tecnologia EDR para desktops, contemplando a configuração da solução em nuvem, treinamento da equipe interna e suporte pelo período do contrato.

2. **TABELA DE REFERÊNCIA:**

ITEM	QTDE	DESCRIÇÃO	MARCA MODELO FABRICANTE	VALOR TOTAL MÁXIMO ACEITÁVEL
1	150	LICENÇAS PARA 150 DESKTOPS PARA USO DE SOLUÇÃO CORPORATIVA DE ANTIVÍRUS COM GERÊNCIA EM NUVEM E TECNOLOGIA EDR – 36 meses	_____	R$ 47.985,00
2	1	TREINAMENTO PARA SISTEMA DE ANTIVÍRUS		R$ 12.000,00
3	1	SUPORTE TÉCNICO PARA A SOLUÇÃO DE ANTIVÍRUS		R$ 21.000,00
VALOR TOTAL DO GRUPO (ITENS 1 AO 3)				**R$ 80.985,00**

3. **QUALIFICAÇÃO TÉCNICA:**

3.1. Apresentar atestado de capacidade técnica, emitido por entidade pública ou privada, demostrando que a licitante já instalou e prestou suporte de solução semelhante, em quantidade mínima de 75 dispositivos.

3.2. Os técnicos que farão a instalação e customização da solução antivírus e o instrutor do treinamento deverão, todos, ser certificados pelo fabricante do produto, este deverá ser comprovado mediante apresentação de certificado expedido pela fabricante da solução de antivírus, como condição para assinatura do contrato.

4. **CARACTERÍSTICAS GERAIS DA SOLUÇÃO DE SEGURANÇA ENDPOINT:**

4.1. Todos os componentes que fazem parte da solução de segurança deverão ser fornecidos por um único fabricante;

4.2. A solução de antivírus ofertada deverá dar suporte, mantendo atualizações e vacinas, para os sistemas operacionais Windows 10 e versões superiores durante toda a vigência do contrato;

4.3. Em caso de descontinuidade da solução de antivírus ofertada, durante a vigência do contrato, a contratada deverá fornecer a versão mais nova ou superior ao produto ofertado, contemplando instalação e treinamento, sem custos ao CRM-PR;

4.4. Deverá possuir central de monitoramento e configuração, baseada em web, on premisse ou em nuvem, que deverá conter todas a ferramentas necessárias à verificação e controle da proteção dos dispositivos;
4.5. A instalação deverá ser feita via cliente específico, por download da gerência central ou também via e-mail de configuração. O instalador deverá permitir a distribuição do cliente via Active Directory (AD) para múltiplas máquinas;
4.6. A console deverá apresentar Dashboard com o resumo dos status de proteção dos computadores e usuários, bem como indicar todos os alertas de eventos de criticidades;
4.7. A console deverá permitir a segregação dos computadores, dentro da estrutura de gerenciamento em grupos;
4.8. A console deverá atualizar a políticas de segurança quando um computador for movido de um grupo para outro manualmente ou automaticamente;
4.9. A console deverá permitir a aplicação de regras diferenciadas baseado em grupos ou usuários;
4.10. A console deverá permitir a definição de grupos de usuários com diferentes níveis de acesso às configurações, políticas e logs;
4.11. Deverá permitir sincronização com o Active Directory (AD) para gestão de usuários e grupos integrados às políticas de proteção;
4.12. Deverá possibilitar a criação e edição de diferentes políticas para a aplicação das proteções exigidas e aplicadas a nível de usuários, não importando em que equipamentos eles estejam acessando;
4.13. Deverá fornecer atualizações do produto e das definições de vírus e proteção contra intrusos;
4.14. Deverá permitir exclusões de escaneamento para um determinado websites, pastas, arquivos ou aplicações, tanto a nível geral quanto específico em uma determinada política;
4.15. Deverá permitir o agendamento da varredura contra vírus com a possibilidade de selecionar uma máquina, grupo de máquinas ou domínio, com periodicidade definida pelo administrador;
4.16. Atualização automática das assinaturas de ameaças (malwares) e políticas de prevenção desenvolvidas pelo fabricante em tempo real ou com periodicidade definida pelo administrador;
4.17. Atualização incremental, remota e em tempo real, da vacina dos antivírus e do mecanismo de verificação (Engine) dos clientes;
4.18. Deverá utilizar protocolos seguros padrão HTTPS para comunicação entre a console de gerenciamento e clientes gerenciados;
4.19. Deverá permitir a exportação dos relatórios gerenciais para os formatos CSV e PDF;
4.20. Os Recursos do relatório e monitoramento deverão ser nativos da própria console central de gerenciamento;
4.21. Deve possibilitar a exibição de informações, tais como o nome da máquina, a versão do antivírus, sistema operacional, versão da engine, data da vacina, data da última verificação, eventos recentes e status;
4.22. Deverá possuir um elemento de comunicação para mensagens e notificações entre estações e a console de gerenciamento utilizando comunicação criptografada;
4.23. Deverá fornecer solução de gerenciamento de arquivos armazenados em nuvem, garantindo que um arquivo que foi feito um upload (exemplo Dropbox), tenha o processo monitorado e gerenciado, bem como realizar automaticamente o escaneamento do arquivo contra malwares, procuradas palavras chaves ou informações confidenciais;
4.24. Deverá permitir a configuração das portas de comunicação;

4.25. Deverá permitir a seleção da versão do software de preferência para um grupo de controle, permitindo assim o teste da atualização antes da implantação em toda a rede;
4.26. O agente antivírus deverá proteger laptops e desktops em tempo real, sob demanda ou agendado para detectar, bloquear e limpar todos os vírus, trojans, worms e spyware;
4.27. No Windows o agente também deverá detectar PUA, adware, comportamento suspeito, controle de aplicações e dados sensíveis. O agente ainda deverá fornecer controle de dispositivos terceiros e, controle de acesso à web;
4.28. Deverá possuir mecanismo contra a desinstalação do endpoint pelo usuário, podendo ser definidas senhas distintas para grupos de usuários;
4.29. Deverá prover, no endpoint, o módulo de HIPS (Host Instrusion Prevention System) para a detecção automática e proteção contra comportamentos maliciosos (análise de comportamento) e deverá ser atualizado diariamente;
4.30. Deverá prover proteção automática contra web sites infectados e maliciosos, assim como prevenir o ataque de vulnerabilidades de browser via web exploits;
4.31. Deverá permitir o monitoramento e o controle de dispositivos removíveis nos equipamentos dos usuários, tais como dispositivos USB, periféricos da própria estação de trabalho e redes sem fio, estando sempre atrelado ao usuário o controle e não ao dispositivo;
4.32. O controle de dispositivos deverá ser ao nível de permissão, somente leitura ou bloqueio;
4.33. Os seguintes dispositivos deverão ser, no mínimo, gerenciados: HD (hard disks) externos, pendrives USB, storages removíveis, CD, DVD, interfaces de rede sem fio, modems, bluetooth, infravermelho, além de MTP (Media Transfer Protocol), tais como iPhone e o Android smartphone;
4.34. A ferramenta de administração centralizada deverá gerenciar todos os componentes da proteção para endpoints e deverá ser projetada para a fácil administração, supervisão e elaboração de relatórios dos endpoint e servidores;
4.35. Deverá possuir interface gráfica web, preferencialmente, com suporte a língua portuguesa (padrão brasileiro);
4.36. A Console de administração deverá incluir um painel com um resumo visual em tempo real para verificação do status de segurança;
4.37. Deverá exibir os endpoints gerenciados de acordo com critérios da categoria (detalhes do estado do computador, detalhes sobre a atualização, detalhes de avisos e erros, detalhes do antivírus, etc), e classificar os computadores em conformidade;
4.38. Deverá permitir, após a identificação de um incidente, a correção dos problemas remotamente, com no mínimo as opções abaixo:
4.38.1. Proteger o dispositivo com a opção de início de uma varredura;
4.38.2. Forçar uma atualização naquele momento;
4.38.3. Ver os detalhes dos eventos ocorridos;
4.38.4. Executar verificação completa do sistema;
4.38.5. Forçar o cumprimento de uma nova política de segurança;
4.38.6. Mover o computador para outro grupo;
4.38.7. Apagar o computador da lista.
4.39. Deverá gravar um log de auditoria seguro, que monitore a atividade no console de gerenciamento para o cumprimento de regulamentações, auditorias de segurança, análise e solução de problemas forenses;
4.40. Deverá gerar relatórios, estatísticos ou gráficos, com as seguintes informações mínimas:

4.40.1. Usuários estão ativos, inativos ou desprotegidos, bem como seus respectivos detalhes;
4.40.2. Detalhamento dos computadores que estão ativos, inativos ou desprotegidos, incluindo detalhes de alertas e das varreduras;
4.40.3. Detalhamento dos periféricos permitidos ou bloqueados, bem como detalhes de onde e quando cada periférico foi usado;
4.40.4. Detalhamento das principais aplicações bloqueadas e os servidores/usuários que tentaram acessá-las;
4.40.5. Detalhamento das aplicações permitidas que foram acessadas com maior frequência e os servidores/usuários que as acessam;
4.40.6. Detalhamento dos servidores/usuários que tentaram acessar aplicações bloqueadas com maior frequência e as aplicações que eles tentaram acessar;
4.40.7. Detalhamento de todas as atividades disparadas por regras de prevenção de perda de dados.
4.41. Deverá permitir a exportação de relatório de logs de auditoria nos formatos CSV e PDF;
4.42. Deverá conter vários relatórios para análise e controle dos usuários e computadores. Os relatórios deverão ser divididos, no mínimo, em relatórios de: eventos, usuários, controle de aplicativos, periféricos e web, indicando todas as funções solicitadas para os endpoints;
4.43. Deverá fornecer relatórios utilizando listas ou gráficos, utilizando informações presentes na console, com no mínimo os seguintes tipos:
4.43.1. Grupo a qual o dispositivo faz parte;
4.43.2. Status de proteção do dispositivo;
4.43.3. Último escaneamento realizado;
4.43.4. Último update;
4.43.5. Último usuário logado no dispositivo;
4.43.6. Início da proteção;
4.43.7. Nome do dispositivo.

5. CARACTERÍSTICAS GERAIS DA SOLUÇÃO DE PROTEÇÃO PARA DESKTOPS:

5.1. Características básicas do agente de proteção contra malwares:

5.1.1. Realizar a pré-execução do agente para verificar o comportamento malicioso e detectar malwares desconhecidos;
5.1.2. Buscar algum sinal de malware ativo e detectar malwares desconhecidos;
5.1.3. Ter a capacidade de submeter o arquivo desconhecido à nuvem de inteligência do fabricante para verificação de reputação, identificando possíveis arquivos maliciosos;
5.1.4. Realizar a atualização várias vezes por dia para manter a detecção atualizada contra as ameaças mais recentes;
5.1.5. A solução deverá manter conexão direta com banco de dados de ameaças do fabricante para uso da rede de inteligência;
5.1.6. Realizar a verificação de todos os arquivos no disco rígido em intervalos programados;
5.1.7. Realizar a limpeza do sistema automaticamente, removendo itens maliciosos detectados e aplicações potencialmente indesejáveis (PUA);
5.1.8. Proteger os navegadores Internet Explorer (Edge), Firefox e Chrome, bloqueando o acesso a sites infectados conhecidos e pela verificação dos dados baixados antes de serem executados;

5.1.9. Permitir a autorização de detecções maliciosas e excluir da varredura diretórios e arquivos específicos;
5.1.10. É requerida a proteção integrada, ou seja, em um único agente, contra ameaças de segurança, incluindo vírus, spyware, trojans, worms, adware e aplicativos potencialmente indesejados (PUAs);
5.1.11. Suportar máquinas com arquitetura 32 e 64 bits;
5.1.12. Ser compatível com os sistemas operacionais Microsoft 10 ou superior;
5.1.13. Possuir a funcionalidade de proteção contra a alteração das configurações do agente, impedindo aos usuários, incluindo o administrador local, reconfigurar, desativar ou desinstalar componentes da solução de proteção;
5.1.14. Permitir a utilização de senha de proteção para possibilitar a reconfiguração local no cliente ou desinstalação dos componentes de proteção.
5.1.15. As soluções ofertadas devem ser contribuintes no MITRE ATT&CK de informações e técnicas de detecção. https://attack.mitre.org/resources/contribute/.

5.2. **O recurso de firewall e ids\ips da solução deverá:**
5.2.1. Possuir atualização periódica de novas assinaturas de ataque;
5.2.2. Reconhecer e bloquear automaticamente as aplicações em clientes, baseando-se no hash do arquivo;
5.2.3. Possuir capacidade de bloqueio de ataques baseado na exploração de vulnerabilidade conhecidas;
5.2.4. Possuir um sistema de prevenção de intrusão no host (HIPS), que monitore o código e blocos de código que podem se comportar de forma maliciosa antes de serem executados;
5.2.5. Deverá ser capaz de aplicar uma análise adicional, inspecionando finamente o comportamento de códigos durante a execução, para detectar comportamento suspeito de aplicações, tais como buffer overflow;
5.2.6. Possuir técnicas de proteção, incluindo:
5.2.6.1. Análise dinâmica de código - técnica para detectar malware criptografado mais complexo;
5.2.6.2. Algoritmo correspondente padrão - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificados como um vírus;
5.2.6.3. Emulação - uma técnica para a detecção de vírus polimórficos, ou seja, vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham;
5.2.6.4. Tecnologia de redução de ameaças - detecção de prováveis ameaças por uma variedade de critérios, como extensões duplas (por exemplo. jpg.txt) ou a extensão não coincida com o tipo de arquivo verdadeiro (por exemplo, um arquivo executável ou arquivo .exe com a extensão .txt);
5.2.6.5. Verificação de ameaças web avançadas – bloqueia ameaças verificando o conteúdo em tempo real e remontando com emulação de JavaScript e análise comportamental para identificar e parar o código malicioso de malware avançados.

5.3. **O recurso de antivírus e antispyware deverá:**
5.3.1. Possuir proteção em tempo real contra vírus, trojans, worms, rootkits, botnets, spyware, adwares e outros tipos de códigos maliciosos;
5.3.2. Possuir proteção anti-malware nativa da solução ou incorporada automaticamente por meio de plug-ins sem a utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante;

5.3.3. As configurações do anti-spyware deverão ser realizadas através da mesma console do antivírus;
5.3.4. Permitir a configuração de ações diferenciadas para programas potencialmente indesejados ou malware, com possibilidade de inclusão de arquivos em listas de exclusão (whitelists) para que não sejam verificados pelo produto;
5.3.5. Permitir a varredura das ameaças da maneira manual, agendada e em tempo real na máquina do usuário;
5.3.6. Possuir capacidade de detecção e reparo em tempo real de vírus de macro conhecidos e novos através do antivírus;
5.3.7. Possuir capacidade de remoção automática total dos danos causados por spyware, adwares e worms, como limpeza do registro e pontos de carregamento, com opção de finalizar o processo e terminar o serviço da ameaça no momento de detecção;
5.3.8. A remoção automática dos danos causados deverá ser nativa do próprio antivírus; ou adicionada por plugin, desde que desenvolvido ou distribuído pelo fabricante;
5.3.9. Possuir capacidade de bloquear origem de infecção através de compartilhamento de rede com opção de bloqueio da comunicação via rede;
5.3.10. Permitir o bloqueio da verificação de vírus em recursos mapeados da rede;
5.3.11. Antivírus de Web (verificação de sites e downloads contra vírus);
5.3.12. Permitir o controle de acesso a sites por categoria;
5.3.13. Proteger a navegação na web, mesmo aos usuários fora da rede, para todos os principais navegadores (IE, Firefox e Chrome), fornecendo controle da Internet independentemente do browser utilizado, como parte da solução de proteção a estações de trabalho, incluindo a análise do conteúdo baixado pelo navegador web, de forma independente do navegador usado, onde não é possível ser ignorada pelos usuários, protegendo os usuários de websites infectados e categorias específicas de websites;
5.3.14. O Controle da Web deverá controlar o acesso a sites impróprios, com categorias predeterminadas de segurança e com a possibilidade de criação de listas personalizadas;
5.3.15. Todas as atividades de navegação na Internet bloqueadas deverão ser enviadas à console de gerenciamento, informando detalhes do evento e a razão para o bloqueio;
5.3.16. Possuir capacidade de verificar somente arquivos novos e alterados;
5.3.17. Possuir funcionalidades específicas para prevenção contra a ação de ransomwares, tais como a capacidade de impedir a criptografia quando feita por aplicativos desconhecidos ou a capacidade de fazer backup de arquivos antes de serem criptografados para posteriormente permitir sua restauração.

5.4. **A funcionalidade de detecção proativa de reconhecimento de novas ameaças deverá:**
5.4.1. Possuir a funcionalidade de detecção de ameaças via técnicas de deep machine learning;
5.4.2. Possuir a funcionalidade de detecção de ameaças desconhecidas que estão em memória;
5.4.3. Possuir a capacidade de detecção, e bloqueio proativo de keyloggers e outros malwares não conhecidos (ataques de dia zero) através da análise de comportamento de processos em memória (heurística);
5.4.4. Possuir a capacidade de detecção e bloqueio de Trojans e Worms, entre outros malwares, por comportamento dos processos em memória;
5.4.5. Possuir a capacidade de analisar o comportamento de novos processos ao serem executados, em complemento à varredura agendada.

5.5. **A funcionalidade de proteção contra ransomwares deverá:**
5.5.1. Dispor de capacidade de proteção contra ransomware não baseada exclusivamente na detecção por assinaturas;
5.5.2. Dispor de capacidade de prevenção contra a ação de criptografia maliciosa executada por ransomwares, possibilitando ainda o bloqueio dos computadores de onde partirem tal ação;
5.5.3. Prevenir ameaças e interromper que elas sejam executadas em dispositivos da rede, detectando e limpando os malwares, além da realização de uma análise detalhada das alterações realizadas;

5.6. **Realizar a detecção e o bloqueio de, no mínimo, as seguintes técnicas de exploit:**
5.6.1. A solução deverá trabalhar silenciosamente na máquina do usuário e deverá detectar a criptografia maliciosa de dados (ransomware), realizando a sua interrupção. No caso de arquivos serem criptografados a solução deverá realizar o retorno destes arquivos ao seu estado normal realizando a limpeza e remoção completa do ransomware na máquina do usuário;
5.6.2. Fornecer uma análise detalhada das modificações realizadas pelo ransomware, realizando a correlação dos dados em tempo real, indicando todas as modificações feitas em registros, chaves, arquivos alvos, conexões de redes e demais componentes contaminados;
5.6.3. A console de monitoramento e configuração deverão ser feitas através de uma central única, baseada em web e em nuvem, que deverá conter todas as ferramentas para a monitoramento e controle da proteção dos dispositivos para a solução de anti-exploit e anti-ransomware;
5.6.4. A console deverá apresentar Dashboard com o resumo dos status de proteção dos computadores e usuários, bem como indicar os alertas de eventos de criticidades alta, média e informacional, bem como todas as identificações para o mapeamento instantâneo dos efeitos causados pelo ransomware nos endpoints;

5.7. **O recurso de endpoint detection and response (edr) deverá:**
5.7.1. Possuir a capacidade de implementar técnicas de EDR (*Endpoint Detection and response*), possibilitando detecção e investigação nos endpoints com atividades suspeitas;
5.7.2. Possuir a capacidade de submeter arquivos identificados em incidentes a uma segunda consulta a nuvem de inteligência do fabricante;
5.7.3. Em caso de incidente a solução deverá permitir visualizar toda a cadeia de ataque, permitindo assim análise de causa raiz;
5.7.4. A solução de EDR deverá ser integrada ao agente de antivírus a ser instalado com um agente único, em estação de trabalho, servidores físicos e virtuais a fim de diminuir o impacto ao usuário final;
5.7.5. O gerenciamento da solução de EDR deverá ser feito, preferencialmente, a partir da mesma console de gerenciamento da solução antivírus;
5.7.6. Possuir resposta imediata para remediar as detecções, permitindo encerrar processos, isolar endpoints, atualizar a segurança e fazer mais varreduras;
5.7.7. Ser capaz realizar buscas de ameaças em todo o ambiente, sendo capaz de buscar por hash, nome, endereços IP, domínio ou linha de comando;
5.7.8. Ser capaz de exibir todos os processos, acessos, arquivos e chaves de registros gerados pela ameaça;
5.7.9. Ser capaz de exibir linha de comando gerada pelo processo suspeito.

5.7.10. Após a análise da nuvem de inteligência do fabricante a solução deverá apresentar um relatório sobre a ameaça contendo, no mínimo:
5.7.10.1. Detalhes do Processo, como nome, hash, hora e data da detecção e remediação;
5.7.10.2. Reputação do arquivo e correlação da detecção do arquivo em outras soluções de antivírus através de bases de conhecimento ou API do Fabricante;
5.7.10.3. Resultado da análise do arquivo suspeito pela funcionalidade de Machinne Learning;
5.7.10.4. Propriedades gerais do arquivo, como nome, versão, tamanho, idioma, etc.;

5.8. **A funcionalidade de controle de aplicações e dispositivos deverá:**
5.8.1. Deverá possuir controle de aplicativos para monitorar e impedir que os usuários executem ou instalem aplicações que podem afetar a produtividade ou o desempenho da rede;
5.8.2. Deverá atualizar automaticamente a lista de aplicativos que podem ser controlados, permitindo que aplicativos específicos ou categorias específicas de aplicações possam ser liberadas ou bloqueadas;
5.8.3. Deverá verificar a identidade de um aplicativo de maneira genérica para detectar todas as suas versões. Permitir a solicitação de adição de novas aplicações nas listas de controle de aplicativos através de interface web;
5.8.4. Deverá oferecer proteção para chaves de registro e controle de processos;
5.8.5. Deverá proibir, através de política a inicialização de um processo ou aplicativo, baseado em nome e no Hash do arquivo;
5.8.6. Deverá detectar aplicativo controlado quando os usuários o acessarem, com as opções de permitir e alertar ou bloquear e alertar;
5.8.7. Deverá possuir a opção de customizar uma mensagem a ser mostrada ao usuário em caso de bloqueio de execução do aplicativo;
5.8.8. Deverá gerenciar o uso de dispositivos de armazenamento USB (ex: pen-drives e HDs USB);
5.8.9. Deverá permitir, através de regras, o bloqueio ou liberação da leitura/escrita/execução do conteúdo desses dispositivos;
5.8.10. Controlar o uso de outros dispositivos periféricos, como comunicação infravermelha e modem externo;
5.8.11. As funcionalidades do Controle de Aplicações e Dispositivos deverão ser nativas do produto ou incorporadas automaticamente por meio de plug-ins sem utilização de agentes adicionais, desde que desenvolvidos e distribuídos pelo fabricante;
5.8.12. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
5.8.13. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
5.8.14. A gestão desses dispositivos deverá ser feita diretamente console de gerenciamento com a possibilidade de definir políticas diferentes por grupos de endpoints;
5.8.15. Deverá permitir a autorização de um dispositivo com no mínimo as seguintes opções: Todos os dispositivos do mesmo modelo; um único dispositivo, com base em seu número de identificação único; Acesso total; Acesso somente leitura; Bloqueio de pontes entre duas redes, por exemplo, um laptop conectado ao mesmo tempo na LAN e se tornar um hotspot Wi-Fi, ou através de um modem.

6. **CARACTERÍSTICAS GERAIS DO SUPORTE TÉCNICO E MONITORAMENTO DA SOLUÇÃO IMPLANTADA:**

6.1. A CONTRATADA deverá disponibilizar ao CRM-PR, durante toda a vigência do Contrato, uma Central de Atendimento (sítio na Internet e telefone) para aberturas e acompanhamento de chamados técnicos, das 8:00 às 18:00 horas, de segunda a sexta;

6.2. Todos chamados de assistência remota para auxilio devem ser catalogados na ferramenta de tickets/helpdesk da contratada, sendo necessário sempre o envio de e-mails com as ações realizadas;

6.3. A contratada deverá iniciar o atendimento de suporte remoto em no máximo 2 horas úteis após a abertura do chamado e solução do problema em até 4 horas;

6.4. Atendimentos que necessitem deslocamento técnico deverão ser atendidos em no máximo oito (6) horas após abertura do chamado por profissional legalmente empregado da empresa vencedora do edital;

6.5. O serviço de suporte técnico deverá ser prestado nas modalidades on-line e on-site, pela CONTRATADA, em função do nível de complexidade do chamado;

6.6. As atividades de suporte técnico incluem, mas não se restringem a prover informação, assistência e orientação para:

6.6.1. Instalação, desinstalação, configuração, substituição e atualização de programas (software);

6.6.2. Aplicação de correções (patches) e atualizações de software;

6.6.3. Diagnósticos, avaliações e resolução de problemas;

6.6.4. Ajustes finos e customização da solução.

6.7. **As atividades de suporte e monitoramento incluem:**

6.7.1. Auxiliar o setor técnico no monitoramento de estações de trabalho com agente de antivírus desativado ou software desatualizado e aplicar procedimento para sua correção;

6.7.2. Auxiliar o setor técnico a monitorar e garantir que o software de antivírus de 90% das estações de trabalho esteja atualizado com, no máximo, 10 (dez) dias de defasagem para a definição mais atual do fabricante da ferramenta de antivírus;

6.7.3. Auxiliar o setor técnico no monitoramento dos resultados de escaneamento dos agentes de antivírus dos servidores e realizar os procedimentos necessários para sanar os problemas eventualmente detectados.

7. **PRAZO DO CONTRATO:**

7.1. O contrato terá o prazo de vigência de 36 (trinta e seis) meses**, a contar de 27/01/2022**, com instalação completa até o dia 03/02/2022, podendo ser prorrogado até o limite estabelecido no Inciso IV do art. 57 da Lei nº 8.666/93.

8. **TREINAMENTO PARA SOLUÇÃO DE ANTIVÍRUS:**

8.1. O prazo para a execução do treinamento é de até 30 (trinta) dias, a contar de 27/01/2022;

8.2. Deverá ser fornecido treinamento da solução de antivírus adquirida para uma equipe de até 05 (cinco) pessoas designadas pela contratante por um período mínimo de 6 horas;

8.3. A contratada deverá fornecer todo material para o treinamento sem custos a CONTRATATA;

8.4. O treinamento deverá conter em seu conteúdo questões práticas e teóricas sobre o funcionamento e os recursos da solução proposta;

8.5. Deve ser incluído, caso exista, módulos básicos e avançados de modo a cobrir todas as funcionalidades da solução ofertada;
8.6. Este treinamento poderá ser realizado de forma presencial ou por videoconferência sem custos a CONTRATADA;
8.7. Os cursos deverão ser realizados em horários e datas a serem acordados pela CONTRATADA e CONTRATANTE.

9. DAS OBRIGAÇÃO DA CONTRATADA

9.1. Fornecer informação e solucionar dúvidas a respeito do serviço.

9.2. Fornecer orientação operacional.

9.3. Identificar eventuais problemas nas funcionalidades.

9.4. Cumprir fielmente as obrigações assumidas neste termo, conforme as especificações no Edital e seus Anexos.

9.5 Comunicar o CONTRATANTE, por escrito, quando verificar quaisquer condições inadequadas para a execução dos serviços ou a iminência de fatos que possam prejudicar a perfeita execução do Contrato, propondo as ações corretivas necessárias.

9.6 Não se obrigar perante terceiros, dando o presente contrato como garantia ou compensar direitos de créditos decorrentes da execução dos serviços ora pactuados em operações bancárias e/ou financeiras, sem prévia autorização expressa do CONTRATANTE.

9.7 Submeter-se à fiscalização por parte do CONTRATANTE, acatando as determinações e especificações contidas no Termo de Referência.

9.8 Manter todas as condições de habilitação do processo licitatório até o final do contrato.

10. DAS OBRIGAÇÕES DO CONTRATANTE

10.1 Prestar as informações e os esclarecimentos pertinentes que venham a ser solicitados pelo representante da Contratada.
10.2 Exercer a fiscalização dos serviços por pessoas especialmente designadas.
10.3 Efetuar os pagamentos à Contratada, de acordo com as condições estabelecidas no Contrato.
10.4 Exigir o cumprimento de todas as obrigações assumidas pela Contratada de acordo com as cláusulas deste Instrumento.

11. DA SUBCONTRATAÇÃO
11.1 Não será permitida a subcontratação em nenhum serviço elencado neste Termo de Referência.

12 DA ALTERAÇÃO SUBJETIVA
12.1 É admissível a fusão, cisão ou incorporação da CONTRATADA com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições

do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

13 DAS SANÇÕES ADMINISTRATIVAS

13.1 Comete infração administrativa nos termos da Lei nº 8.666, de 1993 e da Lei nº 10.520, de 2002, A CONTRATADA que:

13.1.1 Inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

13.1.2 Ensejar o retardamento da execução do objeto;

13.1.3 Fraudar na execução do contrato;

13.1.4 Comportar-se de modo inidôneo;

13.1.5 Cometer fraude fiscal;

13.1.6 Não mantiver a proposta.

13.2 A CONTRATADA que cometer qualquer das infrações discriminadas no subitem acima ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

13.2.1 Advertência por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para o CONTRATANTE;

13.2.2 Dos valores das multas:

Infração	Valor da multa
Inexecução total.	10% do valor total do contrato
Atraso no cumprimento do prazo dos serviços	R$ 100,00 por dia de atraso.
Permitir situação que crie a possibilidade de causar dano físico, lesão corporal ou consequências letais.	R$ 500,00 por ocorrência.
Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços contratuais.	R$ 500,00 por ocorrência.
Manter funcionário sem qualificação para executar os serviços contratados.	R$ 500,00 por funcionário e por dia.
Deixar de substituir empregado que se conduza de modo inconveniente ou não atenda às necessidades do serviço.	R$ 500,00 por funcionário e por dia.
Deixar de cumprir quaisquer dos itens do Edital e seus Anexos não previstos nesta tabela de multas, após reincidência formalmente notificada pelo órgão fiscalizador.	R$ 200,00 por item e por ocorrência.

13.2.3 Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

13.2.4 Impedimento de licitar e contratar com a União com o consequente descredenciamento no SICAF pelo prazo de até cinco anos;

13.2.5 Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a CONTRATADA ressarcir ao CONTRATANTE pelos prejuízos causados;

13.3 Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:
13.3.2 Tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;
13.3.3 Tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;
13.3.4 Demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.
13.4 A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à CONTRATADA, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.
13.5 A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.
13.6 As penalidades serão obrigatoriamente registradas no SICAF.

Curitiba, 13 de dezembro de 2021.

Departamento de Tecnologia da Informação do CRM-PR