

Anexo I - requisitos técnicos e da prestação do serviço

Processo administrativo número 23343.005287.2025-45

Pregão Eletrônico SRP nº 90022/2025 - Registro de preços para a aquisição licença de antivírus

VALOR GLOBAL ESTIMADO: R\$ 510.782,40

Dos locais de entrega:

- 1 Reitoria: Av. Vicente Simões, 1111 – Nova Pouso Alegre – Pouso Alegre – MG – CEP 37.553-465;
- 2 Campus Pouso Alegre: Estrada do Aeroporto, 1.730 - Jardim Aeroporto – Pouso Alegre – MG – CEP 37.550-000;
- 3 Campus Três Corações: R. Coronel Edgar Cavalcanti de Albuquerque, 61 - Chácara das Rosas – Três Corações – MG - CEP 37410-000;
- 4 Campus de Carmo de Minas: Alameda Murilo Eugênio Rubião, S/N – Chacrinha – Carmo de Minas – MG – CEP 37.472-000;
- 5 Poços de Caldas: Avenida Dirce Pereira Rosa, 300, Jardim Esperança - Poços de Caldas - MG - CEP 37713-100;
- 6 Campus Passos: R. da Penha, 290 - Penha II, Passos - MG, 37903-070;
- 7 Campus Inconfidentes: Praça Tiradentes, 416 - Centro - Inconfidentes / MG, CEP 37576-000;
- 8 Campus Machado: Rod. Machado - Paraguaçu, s/n - Santo Antonio, Machado - MG, CEP 37750-000;
- 9 Campus Muzambinho: Estrada de Muzambinho, Bairro - Morro Preto, Muzambinho - MG, CEP 37890-000;

Requisitos técnicos

Requisitos gerais

10.1 Fundamentalmente a solução deve ser do tipo endpoint, além disso, deverá ser capaz de gerir políticas de segurança distintas, visto que existem demandas personalizadas de acordo com as necessidades de usuários específicos, deve conter funcionalidades essenciais à segurança, como firewall, políticas de acesso a websites, bloqueio de transmissão de informações sensíveis e acesso a informações avançadas sobre as ações executadas, para que assim possam-se realizar auditorias referentes a possíveis danos ao ambiente institucional.

10.2 Deve possuir plataforma para gerência de configurações e ajustes relacionados ao Endpoint. A plataforma deverá possuir características essenciais como envio de relatórios, por e-mail, referentes ao uso das funcionalidades da solução, como websites e aplicações

bloqueadas e atividades referentes ao firewall, deverá possuir também dashboard personalizável com as informações que exigem maior atenção, como níveis de ameaça e quantidade de riscos.

10.3 Deverá fornecer atualizações de políticas via rede, fornecer capacidade de agregar múltiplos dispositivos em diferentes unidades organizacionais, garantindo assim maior eficácia ao adotar as medidas personalizáveis de segurança.

10.4 O endpoint deverá ser capaz de analisar as ações tomadas pelo usuário e identificar possíveis incidentes que afetem a rede de computadores. A solução deverá ser capaz de remover outras soluções que ajam de maneira concomitante com a mesma.

10.5 O endpoint também deverá possuir controles relacionados a permissibilidade, para que apenas usuários administradores possam realizar configurações e ajustes manuais, como reiniciar módulos. Deverá realizar varreduras em unidades externas (exemplo: USB) que venham a se conectar com o dispositivo, e, caso possuam arquivos ou possam vir a causar malefícios, tomar medidas para o bloqueio da atividade suspeita.

10.6 A solução de software antivírus deverá possuir as seguintes funcionalidades:

10.6.1 **Antimalware:** a solução deverá realizar análises heurísticas acerca dos tipos de vírus que podem vir a causar malefícios ao dispositivo, tais quais vírus, worms, trojans, spywares, adwares, keyloggers, rootkits, entre outros. Deverá também conter formas personalizáveis de escaneamento envolvendo processamento em nuvem;

10.6.2 **Análise de riscos dos Endpoints:** identifica, realiza o acesso e remedia vulnerabilidades através de análises de vulnerabilidade, que por sua vez podem ser agendadas ou requisitadas. Após realizar a análise, a solução deverá fornecer um resumo dos riscos encontrados em uma dashboard, ou um relatório, e instruir dicas de como mitigar as vulnerabilidades;

10.6.3 **Controle avançado de ameaças:** destinado a aplicações maliciosas que por ventura venham a evadir a análises heurísticas. Neste módulo, a solução deverá monitorar, de maneira contínua, o comportamento dos processos e bloquear possíveis formas de manipulação;

10.6.4 **Controle avançado contra exploração de vulnerabilidades:** a solução deverá atuar contra ataques zero-day. Neste módulo, a solução se atualizará sobre os exploits mais recentes para que possa mitigar vulnerabilidades que possam ter se evadido de outras varreduras. Deverá acompanhar processos e proteger o dispositivo contra brechas de segurança;

10.6.5 **Controle de conteúdo:** a solução deverá executar ações como controle de tráfego, controle de acesso a web, proteção de dados e controle de aplicações;

Controle de dispositivos: prevenir que dados sensíveis ou vírus sejam atrelados ao computador via dispositivos removíveis, como CD/DVDs, pendrives, dispositivos de armazenamento, entre outros;

10.6.6 **Defesa em ataques relacionados a rede:** a solução deverá realizar uma análise do tráfego de rede a fim de identificar vulnerabilidades;

10.6.7 **Firewall:** este módulo deverá controlar a atividade de rede nas aplicações do computador.

10.6.8 **Deteção e Resposta em Endpoints (EDR):** a solução deverá realizar monitoramento contínuo dos endpoints, detectar ameaças avançadas por análise comportamental, permitir investigação forense dos incidentes e possibilitar resposta remota, como isolamento do endpoint, bloqueio de processos e remediação.

10.6.9 **As licenças deverão ser multiplataforma,** permitindo a instalação em diferentes sistemas operacionais e dispositivos, sem restrições prévias.

Dos serviços correlacionados

10.7 A contratada deverá prestar serviços de manutenção e suporte técnico da solução de software, durante toda a vigência contratual;

10.8 Devido às características da solução, há necessidade de realização de manutenções (corretivas/preventivas/adaptativa/evolutiva) pela Contratada, visando à manutenção da disponibilidade da solução e ao aperfeiçoamento de suas funcionalidades;

10.8.1 Manutenção corretiva: correção de defeitos / erros identificados na solução contratada, abrangendo comportamentos inadequados que causem problemas de uso ou funcionamento e quaisquer desvios em relação a requisitos estabelecidos;

10.8.2 Manutenção Adaptativa: adequação na solução de software contratada, em decorrência de mudanças que não impliquem inserção, alteração ou exclusão de requisitos funcionais;

10.8.3 Manutenção de Interface: adequação na solução de software contratada para promover mudanças de interface e layout, sem alteração de funcionalidades sob o ponto de vista do usuário;

10.8.4 Manutenção Evolutiva: mudanças em requisitos funcionais da solução de software já concluído que implicam inclusão, alteração e/ou exclusão de funcionalidades;

10.8.5 Os serviços de manutenção compreendem não apenas a modificação do código da aplicação, mas também todas as atividades necessárias para o atendimento de quaisquer das manutenções acima;

10.8.6 Não será admitida cobrança retroativa de valores referentes a serviços correlacionados e de atualização de versões;

10.8.7 Não será admitida a cobrança de valores para eventual reativação de serviços agregados;

10.8.8 Não será admitida a cobrança de valores relativos ao serviço de correção de erros, inclusive retroativos, que devem ser corrigidos sem ônus à contratante, durante o prazo de validade técnica da subscrição dos softwares, nos termos do Capítulo III da Lei nº 9.609, de 19 de fevereiro de 1998.

10.8.9 A contratada obriga-se a manter a solução de software atualizada.

10.8.10 A contratada obriga-se a disponibilizar todas as atualizações da solução de software, bem como novas funcionalidades incorporadas da solução sem incidência de custos para a contratante.

Do Suporte Técnico

10.9 A contratada deverá disponibilizar plataforma, email e/ou WhatsApp para abertura de chamados de suporte técnico;

10.10 A abertura de chamados deverá permitir aos usuários da contratante registro de qualquer tópico, incluindo tanto dúvidas de uso do sistema quanto a ajustes/solicitações de funcionalidades;

10.11 Os níveis de serviço para atendimento de chamados de suporte técnico deverão observar o que segue:

10.12 Solicitação Crítica: relativo a incidentes que impeçam totalmente as atividades da instituição, ou que impeça parcialmente qualquer atividade para os operadores da solução, sendo que tais processos precisam ser executados imediatamente, sem exceder o prazo limite de 48 (quarenta e oito) horas para solução;

10.13 Solicitação Urgente: Relativos a incidentes que impeça totalmente as atividades de um operador, sendo que tais processos precisam ser executados em um prazo curto, limitado a 7 (sete) dias para solução;

10.14 Solicitação Necessária: Relativos a incidentes que impeçam parcialmente as atividades de um operador ou que reduza a produtividade de um setor, esta solicitação tem um prazo para atendimento mais flexível, limitado a no máximo 15 (quinze) dias para solução;

10.15 Solicitação Desejável: Solicitação de melhoria ou nova funcionalidades, devendo ser respondida em até 14 (quatorze) dias, indicando a viabilidade ou não da implementação pela contratada, e se for o caso, apresentar estimativa de prazo para atendimento.

10.16 A contratada deverá prestar suporte técnico online para a instalação da solução;

10.17 Para efeitos de instalação a contratada deverá:

10.17.1 Fornecer template / manual de instalação;

10.17.2 Realizar migração das regras / configurações pré existentes.

Dos Direitos Autorais

10.18 Esta contratação não inclui a cessão de direitos de propriedades intelectuais e autorais da solução a ser contratada;

10.19 Deverão ser observadas eventual política de privacidade de software;

10.20 É vedado o acesso não autorizado aos códigos-fonte do Software, sob pena de indenização e multa por parte do infrator;

10.21 A contratada é detentora dos direitos autorais sobre o Software, protegidos e regulados pela Lei 9.609/98, ou deter direitos de comercialização;

Da Proteção de Dados

10.22 A base de dados do software decorrente do uso da solução será de propriedade da contratante. Em caso de encerramento contratual, a contratada deverá disponibilizar para a contratante aquela base de dados gerada na execução dos serviços, incluindo documentos e elementos de informação (como dados pessoais dos servidores), em um formato que

permita a migração, para que ela tenha condições de migrar as informações para sua base de dados.

10.23 A contratada deverá informar o seu Encarregado pela proteção de Dados, nos termos do art. 41 da Lei Federal nº 13.709/18;

10.24 As partes deverão assinar o Termo de Compromisso de Manutenção de Sigilo conforme modelo que constará do termo de Referência.

10.25 O software deverá seguir as regulamentações de coleta, uso, tratamento e descarte de dados pessoais previstas na Política de Privacidade e Proteção de dados do IFSULDEMINAS (Resolução nº 131/2021/CONSUP/IFSULDEMINAS), assim como a Política de Segurança da Informação do IFSULDEMINAS (Resolução nº 355/2023/CONSUP/IFSULDEMINAS).