



Serviço Público Federal  
Conselho Regional de Medicina Veterinária do Estado de São Paulo

ANEXO II

PREGÃO ELETRÔNICO Nº 90005/2026  
Processo Administrativo nº 00.00030/2026

ESPECIFICAÇÃO TÉCNICA DO SISTEMA GED

1. DAS DIRETRIZES E CLASSIFICAÇÃO DOS REQUISITOS

1.1. Para fins de avaliação, homologação e cumprimento contratual, todos os requisitos técnicos descritos neste Anexo são considerados essenciais e de cumprimento obrigatório, com exceção aos requisitos que representam melhorias tecnológicas desejáveis que não impedem o funcionamento central da solução. Estes estarão expressamente identificados ao final de sua descrição com a tag **[COMPLEMENTAR]**.

2. DA VISÃO GERAL E MODOS DE OPERAÇÃO

2.1. O sistema deverá permitir seu acesso por meio da internet, não havendo a necessidade de instalação de programas específicos para sua execução além de um navegador web (Chrome, Firefox, Edge, Safari, etc.), em sua última versão estável.

2.2. O sistema deve ser responsivo para adaptar-se a diferentes tipos de dispositivos mobile, independente do sistema operacional (Apple, Android) **[COMPLEMENTAR]**.

2.3. O sistema deve possuir funcionalidades de expiração de senha, bloqueio de acesso por número limite de 3 (três) tentativas de autenticação, além de oferecer suporte a Múltiplo Fator de Autenticação (MFA) na etapa de login.

2.4. Deve-se controlar o tempo de inatividade da sessão dos usuários conectados à solução ("logados") através de parametrização.

2.5. Deve suportar o acesso de 120 usuários simultâneos, além de consulta de 3.676.800 páginas de documentos sem a degradação do ambiente, com tempo de resposta inferior a 5 (cinco) segundos.

2.6. A interface do sistema deverá permitir, em seu próprio ambiente, que o usuário abra várias telas simultaneamente.

2.7. Permitir a integração a outros sistemas através de Interface de Programação de Aplicações (API) documentadas com as seguintes características mínimas **[COMPLEMENTAR]**:

2.7.1. Utilização do protocolo de segurança mTLS na comunicação entre sistemas.

2.7.2. Autenticação baseada em padrões atuais de segurança de acesso, utilizando tokens de acesso de vida curta, entre 6 e 12 horas e mecanismos de renovação segura, garantindo a revalidação periódica de credenciais.

2.7.3. Aplicação do princípio do menor privilégio, tendo a permissão apenas para o que é estritamente necessário.

2.7.4. Definição do número máximo de chamadas à API por minuto/hora.

2.7.5. Lista de permissão de IPs (IP Whitelisting), restringindo o acesso à API para requisições vindas de endereços IPs específicos e conhecidos.

2.7.6. Logging detalhado e monitoramento em tempo real: Registro de todas as tentativas de acesso (sucesso e falhas), com data, horário, IP, no mínimo, além de alertas anômalos, com picos súbitos de erros de autenticação.

2.8. A interface do sistema deverá ser amigável, intuitiva e eficiente, desenvolvida conforme boas práticas de UX Design, permitindo que o usuário execute tarefas comuns com o mínimo de navegação.

3. DAS FUNCIONALIDADES DE GESTÃO

3.1. O sistema deve permitir a captura, indexação, armazenamento e gerenciamento de documentos digitais e digitalizados.

3.2. Deve possuir motor de OCR nativo para reconhecimento de caracteres em arquivos PDF/A, permitindo busca textual completa (Full-Text).

3.3. Os filtros de buscas documentais devem permitir, no mínimo, o seguinte:

3.3.1. Pesquisa de documentos:

3.3.1.1. Segmentar a pesquisa por tipo de documento: PF/PJ, financeiro, administrativo, etc., conforme definido na tabela do Subitem nº "4.7" do Estudo Técnico Preliminar (APENSO I).

3.3.1.2. Pesquisa por combinação de campos de indexação.

3.3.1.3. Pesquisa por período de datas.



Serviço Público Federal  
Conselho Regional de Medicina Veterinária do Estado de São Paulo

3.3.1.4. Pesquisa por palavra contida no corpo do documento.

3.3.1.5. Pesquisa pelo nome do documento.

3.3.1.6. Pesquisa pelo número de CRMV-SP.

3.3.1.7. Pesquisa pelo nome profissional/empresa.

3.3.1.8. Pesquisa pelo CPF/CNPJ.

3.3.1.9. Pesquisa pelo número da caixa.

3.3.2. **Pesquisa de caixas:**

3.3.2.1. Pesquisa pelo Centro de Custo.

3.3.2.2. Pesquisa pelo número da caixa.

3.3.2.3. Pesquisa pelo conteúdo da caixa.

3.3.2.4. Pesquisa pelo lacre da caixa.

3.3.2.5. Pesquisa pelo tipo da caixa.

3.3.2.6. Pesquisa pelo status caixa.

3.4. Deve permitir pesquisas de Ordem de Serviço contendo, no mínimo, os seguintes filtros:

3.4.1. Número da OS.

3.4.2. Solicitante.

3.4.3. Data de início e fim.

3.4.4. Número da caixa.

3.4.5. Número do documento.

3.4.6. Páginas.

3.4.7. Cada registro retornado deve conter a rastreabilidade, além do status de atendimento da OS.

3.5. Gestão automatizada do ciclo de vida documental conforme Tabela de Temporalidade (TTD) definida pelo CRMV-SP, além de manter o Código de Classificação de Documentos (CCD) em sistema, com alertas configuráveis sobre prazos de guarda e notificações automáticas antes do expurgo definitivo **[COMPLEMENTAR]**.

3.6. Deve permitir o mapeamento de caixas e documentos digitais à sua localização física.

3.7. Integração nativa para assinatura de documentos utilizando certificados digitais padrão ICP-Brasil (PADES), garantindo validade jurídica sem a necessidade de softwares externos de assinatura, de acordo com o Decreto 10.278/2020 e as Leis 13.874/2019 e 12.682/2012.

3.8. O sistema deve permitir visualizar documentos diretamente na interface do navegador sem a necessidade de download prévio dos arquivos.

3.9. O sistema deve permitir o download e o upload de documentos.

3.10. O sistema deve permitir o controle de acesso às funcionalidades do sistema baseados no perfil de acesso ao usuário.

3.11. O sistema deve permitir a criação de grupos de usuários, onde compartilham as mesmas permissões

3.12. O sistema deve restringir o acesso a tipos específicos de documentos, impedindo que usuários não autorizados os acessem.

3.13. Permitir a geração de relatórios, no mínimo, em formato PDF, com as seguintes características:

3.13.1. Relatório de espaço utilizado em sistemas de arquivos distribuídos **[COMPLEMENTAR]**.

3.13.2. Relatório de quantidade de documentos indexados por pessoa por intervalo de tempo **[COMPLEMENTAR]**.

3.13.3. Relatório de quantidade de documentos enviados por pessoa por intervalo de tempo **[COMPLEMENTAR]**.

3.13.4. Relatório de quantidade de documentos indexados e não indexados por tipo de documento **[COMPLEMENTAR]**.

3.13.5. Relatório dos serviços prestados, para fins de contabilidade e faturamento do serviço.

3.14. O sistema deve apresentar em tela, na sessão do usuário, todo e qualquer erro ou homologação de uma ação.

3.15. O sistema deve possuir funcionalidade para gerenciar o processo de eliminação de documentos cujo prazo de guarda (TTD) tenha expirado. A solução deve **[COMPLEMENTAR]**:

3.15.1. Gerar automaticamente a listagem de eliminação de documentos para aprovação da Comissão Permanente de Avaliação de Documentos (CPAD) do CRMV-SP.



**Serviço Público Federal**  
**Conselho Regional de Medicina Veterinária do Estado de São Paulo**

**3.15.2.** Bloquear a exclusão sistêmica de qualquer arquivo até que um usuário com perfil de administrador insira o número do Edital de Eliminação publicado no Diário Oficial da União (DOU), além do portal de transparência do CRMV-SP.

**3.15.3.** Permitir o upload e o vínculo do Termo de Fragmentação/Destruição ao registro dos documentos eliminados, mantendo os metadados (índices) na base histórica para comprovação futura de que o documento existiu e foi descartado legalmente.

**4. DOS REQUISITOS DE INFRAESTRUTURA EM NUVEM**

**4.1.** O(s) Datacenter(s) que hospedará(ão) a solução deve(m) possuir classificação equivalente a Tier II ou superior, localizado em território brasileiro.

**4.2.** Disponibilidade mínima (SLA) de 99,5% ao ano.

**4.3.** Os procedimentos de armazenamentos de dados, arquivos e documentos deverão seguir protocolos de segurança por acesso restrito por autenticação, consumo de APIs por criptografias, camadas SSL, restrições de redes por firewalls, load-balances e proxys, havendo acessos a base de dados e repositórios restrito por vários níveis em camadas de segurança física e lógica.

**4.4.** A aplicação deverá ser protegida por firewall de aplicação web (WAF) e bloqueio de BOTs e SPAMs.

**4.4.1.** A solução deverá permitir a configuração de bloqueio de acessos baseado em Geolocalização (GeoIP) **[COMPLEMENTAR]**.

**4.5.** A CONTRATADA deverá configurar o firewall de aplicação, de forma a trabalhar com inspeção bidirecional de ataques.

**4.6.** Todo o tráfego de informações do sistema deverá ser transitado com criptografia HTTPS. A CONTRATADA também aplicará melhoras práticas, como uso do protocolo TLS 1.3, com cifras fortes e desativação de protocolos vulneráveis.

**4.7.** Ter mecanismos de proteção contra-ataque de força bruta para roubo de credenciais e negação de serviço (DoS/DDoS).

**5. DA POLÍTICA DE BACKUP E SEGURANÇA DOS DADOS**

**5.1.** A CONTRATADA deve assegurar a custódia e integridade do acervo digital legado (documentos e metadados), bem como de todos os novos documentos inseridos no sistema de GED.

**5.2.** Deve manter uma rotina rigorosa de cópias de segurança (backup) automatizadas, garantindo redundância e proteção contra perda de dados, com as seguintes características mínimas:

**5.2.1.** Backup completo (full): Realização de cópias completas realizadas, preferencialmente em horários de baixa utilização do sistema, para não impactar a performance de consulta dos usuários.

**5.2.2.** Backup incremental: Realização de cópias diárias, capturando apenas alterações e novos documentos inseridos no período de 24 horas.

**5.2.3.** Recovery Point Objective (RPO): O ponto máximo de perda de dados aceitável é de 24 (vinte e quatro) horas corridas. Em caso de falha crítica, o sistema deve ser restaurado com os dados do dia anterior.

**5.2.4.** Recovery Time Objective (RTO): O tempo total para restauração completa do ambiente e retorno da operação não deve ultrapassar 24 (vinte e quatro) horas corridas. Para restaurações pontuais de arquivos ou pastas, o prazo não deve ultrapassar de 4 (quatro) horas úteis.

**5.2.5.** A CONTRATADA manterá o histórico de versões dos backups pelo prazo mínimo de 90 (noventa) dias, permitindo a recuperação de documentos que possam ter sido corrompidos ou deletados indevidamente.

**5.2.6.** Os backups devem ser armazenados em locais com redundância geográfica (armazenamento geodistribuído), para garantir a recuperação em caso de desastres no datacenter principal.

**5.2.7.** Os dados em repouso e em trânsito deve estar obrigatoriamente criptografado, utilizando padrões de mercado (AES-256 e TLS 1.3).

**5.3.** A CONTRATADA deve realizar teste de restauração (restore) periodicamente, no mínimo a cada 6 (seis) meses, enviando à CONTRATANTE relatório circunstanciado comprovando a integridade das cópias e o tempo de recuperação.

**5.4.** A solução deverá permitir a criptografia automática de dados e objetos armazenados usando AES (Advanced Encryption Standard) de, no mínimo, 256 bits ou outro algoritmo com força de chave equivalente ou superior.

**5.5.** A solução deverá possibilitar comunicação criptografada e protegida para transferência de dados.

**5.6.** A CONTRATADA deve implementar controles para isolamento e segurança dos dados armazenados na nuvem.



Serviço Público Federal  
Conselho Regional de Medicina Veterinária do Estado de São Paulo

**6. DA SEGURANÇA DA INFORMAÇÃO E GOVERNANÇA**

**6.1.** A CONTRATADA, sempre que solicitado pela CONTRATANTE, deverá evidenciar de forma transparente os controles e práticas de segurança projetados para proteger a confidencialidade, integridade e disponibilidade do conteúdo, proteção dos dados de qualquer processamento não autorizado e atividades que possibilitam perda ou destruição ilegal de dados.

**6.2.** Deverá adotar o conceito de “assinaturas de ataques” com intuito de detectar eventos de segurança específicos e o conceito de “anomalia de comportamento” com intuito de detectar incidentes através de tráfego anormal.

**6.3.** Todos os eventos de segurança detectados deverão ser registrados em log. Esses logs serão analisados pela equipe de especialistas em cibersegurança da CONTRATADA, para que possam ser tomadas as melhores medidas de prevenção. Tais medidas deverão ser reportadas ao CONTRATANTE.

**6.4.** A CONTRATADA deverá fornecer relatórios com as seguintes informações: IP de origem, tipo de incidente por período, horário do incidente, função ou módulo afetado pelo incidente, quantidade de eventos correlacionados, entre outros que possibilitem a rastreabilidade das ocorrências.

**6.5.** Deve possuir registro inalterável (logs) de todas as visualizações, *download*, impressões e alterações realizadas nos dados, contendo no mínimo as seguintes informações: data, IP de origem, usuário, dado alterado e descrição da ação. Tais informações devem estar disponíveis em tela específica para perfis de administradores do sistema, para fins de auditoria e rastreabilidade da informação.

**6.6.** Os logs supracitados não devem ser confundidos com os logs de sistema, que também devem registrar de forma imutável de toda e qualquer alteração sistêmica, que envolva banco de dados, alterações de funções por desenvolvedores, acesso por ssh, etc., que afetem auditorias forenses. Tais informações devem ser alocadas em ambiente próprio e servir de monitoramento interno para a equipe técnica da CONTRATADA, além de disponibilização de informações específicas para o CONTRATANTE, sempre que solicitado, para fins de comprovação e levantamento de evidências.

**6.7.** Todos os registros de eventos (logs) mencionados nos itens anteriores devem utilizar uma fonte de tempo comum e confiável, devendo os sistemas estarem obrigatoriamente sincronizados via protocolo NTP (Network Time Protocol), preferencialmente utilizando o estrato do Projeto NTP.br, para garantir a precisão cronológica e a integridade da linha do tempo em auditorias e perícias.

**6.8.** A CONTRATADA obriga-se a manter o armazenamento principal e todas as cópias de segurança (redundância) em datacenters localizados em território brasileiro, submetendo-se exclusivamente à legislação da brasileira.

**6.8.1.** Fica Vedado a transferência, hospedagem ou trânsito de qualquer parte do acervo digital e seus respectivos metadados para servidores localizados fora do Brasil, salvo autorização prévia, expressa e fundamentada do CONTRATANTE.

**6.8.2.** Os serviços de “Gestão de Vulnerabilidades” devem ser capazes de detectar e avaliar vulnerabilidades encontradas nos sistemas e recursos do ambiente de armazenamento contratado, especialmente quanto ao impacto no ambiente computacional e ao risco inerente à segurança das informações custodiadas por meio de análises periódicas de conformidade.

**6.9.** Manter o sistema atualizado com todas as correções necessárias de vulnerabilidades, sem custos adicionais para o CRMV-SP, seguindo as boas práticas de gestão de mudanças (GMUD).

**6.10.** Qualquer alteração do sistema no que tange novas funcionalidades, deverão seguir as mesmas práticas de gestão de mudanças, além de informar e agendar previamente com o CRMV-SP a data da aplicação, propondo ao Conselho um treinamento específico daquela nova funcionalidade.

**6.10.1.** A CONTRATADA deve verificar vulnerabilidades para, no mínimo: detecção de hot fixes, service packs, registros, backdoors, ransomware, trojan, worms e malwares.

**6.10.2.** A CONTRATADA deverá sugerir melhorias de segurança de forma a minimizar a exploração de vulnerabilidades no ambiente do armazenamento do CONTRATANTE.

**6.10.3.** A CONTRATADA deverá administrar os sistemas de detecção, monitorando de forma proativa o tráfego de entrada e saída, além das tentativas de intrusão, buscando e interrompendo ataques e atividades suspeitas em tempo real, continuamente.

**6.10.4.** A CONTRATADA deverá seguir as melhores práticas para que quaisquer incidentes de cibersegurança sofridos pelo ambiente de nuvem, sejam identificados, controlados, interrompidos ou cessados, em caráter provisório ou definitivo, mantendo o CONTRATANTE sempre ciente de tais ocorrências.

**6.10.5.** É vedado o tratamento de informações não autorizadas pelo CONTRATANTE.



Serviço Público Federal  
Conselho Regional de Medicina Veterinária do Estado de São Paulo

**6.10.6.** A CONTRATADA deverá assegurar que as informações sob sua custódia serão tratadas como informações sigilosas, não podendo ser usadas por ele ou fornecidas a terceiros, sob nenhuma hipótese, sem autorização formal do CONTRATANTE.

**6.10.7.** A solução ofertada deve dispor de plano de comunicação de incidentes, devendo a CONTRATADA informar imediatamente ao CONTRATANTE todos os incidentes de segurança da informação ou existência de vulnerabilidades do objeto da contratação, assim considerados os eventos não previstos ou não desejados, bem como qualquer violação das regras de sigilo estabelecidas que tenham ocorrido por sua ação ou omissão, independentemente de dolo, que acarretem dano à confidencialidade, disponibilidade, integridade ou autenticidade dos dados do CONTRATANTE.

**6.10.8.** O provedor que integra a solução deve possuir plano de continuidade, recuperação de desastres e contingência de negócio, que possa ser testado regularmente, objetivando a disponibilidade dos dados e serviços em caso de interrupção, bem como desenvolver e colocar em prática procedimentos de respostas a incidentes relacionados com os serviços.

São Paulo, data e hora conforme assinatura digital<sup>1</sup>

Elaborado por:

INTEGRANTE I	INTEGRANTE II
Assinado digitalmente <b>Artur dos Santos Ribeiro</b> Matrícula nº 3058 Chefe do Setor de Multas	Assinado digitalmente <b>Geni da Silva</b> Matrícula nº 3067 Coordenadora de Atendimento e Registros
INTEGRANTE III	INTEGRANTE IV
Assinado digitalmente <b>Silvana Basaglia Beringer</b> Matrícula nº 3060 Coordenadora de Ética Profissional	Assinado digitalmente <b>Richard Roberto de Almeida Silva</b> Matrícula nº 4171 Líder Técnico de TI

Aprovado por:

AUTORIDADE MÁXIMA DO CRMV-SP
Assinado digitalmente <b>Daniela Pontes Chiebao</b> Presidente do CRMV-SP CRMV-SP nº 15.782/V

<sup>1</sup> Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020, e na Resolução CRMV-SP nº 2.993, de 30 de novembro de 2022.



## Página de assinaturas eletrônicas

**Doc:** 07 - ANEXO II - Especificação Técnica do Sistema GED.pdf

### Assinaturas:



Documento assinado eletronicamente por **Artur dos Santos Ribeiro, CHEFE DE MULTAS, SEDE - FISCALIZAÇÃO, IP de acesso 170.0.135.226**, em 08/06/2026, às 12:53:11, conforme horário oficial de Brasília. Com fundamento na Lei nº 14.063, de 23 de setembro de 2020.



Documento assinado eletronicamente por **Richard Roberto de Almeida Silva, Líder Técnico de Tecn. da Informação, SEDE - INFORMÁTICA, IP de acesso 170.0.135.226**, em 08/06/2026, às 13:17:32, conforme horário oficial de Brasília. Com fundamento na Lei nº 14.063, de 23 de setembro de 2020.



Documento assinado eletronicamente por **Geni da Silva, COORDENADORA DE ATENDIMENTO E REGISTRO, SEDE - REGISTRO, IP de acesso 200.155.132.218**, em 08/06/2026, às 14:11:04, conforme horário oficial de Brasília. Com fundamento na Lei nº 14.063, de 23 de setembro de 2020.



Documento assinado eletronicamente por **Silvana Basaglia Beringer, COORDENADORA DE ÉTICA PROFISSIONAL, SEDE - ÉTICA PROFISSIONAL, IP de acesso 200.155.132.218**, em 08/06/2026, às 14:16:50, conforme horário oficial de Brasília. Com fundamento na Lei nº 14.063, de 23 de setembro de 2020.



Documento assinado eletronicamente por **Daniela Pontes Chiebao, PRESIDENTE, SEDE - DIRETORIA EXECUTIVA, IP de acesso 200.155.132.218**, em 08/06/2026, às 15:39:06, conforme horário oficial de Brasília. Com fundamento na Lei nº 14.063, de 23 de setembro de 2020.