O Consórcio Instituição de Cooperação Intermunicipal do Médio Paraopeba – ICISMEP torna público a quem possa interessar que estará recebendo cotações para contratação direta do objeto mencionado a seguir.

OBJETO	Contratação de empresa especializada para a prestação de serviços gerenciados de hospedagem de servidores destinados ao Website Institucional, desenvolvido em plataforma WordPress e demais soluções Open Source, abrangendo o fornecimento de infraestrutura de alta disponibilidade e desempenho, suporte técnico especializado, manutenção preventiva e corretiva, implementação de rotinas automatizadas de backup, acesso a painel de painel DNS, atualização e inclusão de páginas, instalação e configuração de recursos adicionais e a migração de dados e arquivos oriundos de plataformas legadas.

Deverão ser observados os seguintes quesitos para o fornecimento de cotação:

A proposta deverá conter:

1) Marca dos itens a serem fornecidos, no caso de aquisições;
2) Razão Social;
3) CNPJ;
4) Endereço;
5) Nome do representante legal ou procurador;
6) Contatos (e-mail e telefone);
7) **Ser emitida, preferencialmente, em papel timbrado.**

Informações

1) O prazo para pagamento será de até **30 (trinta) dias** após o aceite da Nota Fiscal.
2) Será de inteira responsabilidade da empresa a entrega dos materiais no local de destino em perfeitas condições de uso, entregues em suas embalagens originais lacradas, já inclusos todas as despesas com transportes, fretes, impostos e serviços (caso seja necessário), ferramentas para a devida prestação que incidam sobre a mercadoria/serviço.

Setor requisitante: Tecnologia da Informação

Responsável Técnico: João Gabriel Miranda de Souza

Endereço de E-mail: ti@icismep.mg.gov.br

Telefone: (31) 2571-3026 / (31) 97364-0171.

ESPECIFICAÇÕES DA CONTRATAÇÃO
DISPENSA DE LICITAÇÃO

1 DO OBJETO

Contratação de empresa especializada para a prestação de serviços gerenciados de hospedagem de servidores destinados ao Website Institucional, desenvolvido em plataforma WordPress e demais soluções Open Source, abrangendo o fornecimento de infraestrutura de alta disponibilidade e desempenho, suporte técnico especializado, manutenção preventiva e corretiva, implementação de rotinas automatizadas de backup, acesso a painel de painel DNS, atualização e inclusão de páginas, instalação e configuração de recursos adicionais e a migração de dados e arquivos oriundos de plataformas legadas.

2 DA ESPECIFICAÇÃO DO OBJETO:

2.1 A especificação detalhada do objeto encontra-se delimitada a seguir:

Lote único				
Item	Descrição	Unidade	Quantitativo	Valor Total
1	Hospedagem de servidores de alta disponibilidade e desempenho destinados para Website Institucional, WordPress e demais soluções com suporte backup e restauração.	UND	12	R$
2	Hospedagem de servidores de alta disponibilidade e desempenho destinados para sistema HESK/GLPI, com suporte backup e restauração.	UND	12	R$
3	Suporte e manutenção de sites e aplicativos, adotando as melhores práticas do ITIL v3, com gerenciamento de suporte, manutenção, criação de novas páginas e aplicações sob demanda utilizando tecnologias como HTML, CSS, JavaScript, React.js, Vue.js, Python, PHP (Laravel), MySQL, PostgreSQL e MongoDB.	UND	12	R$
4	Serviço de migração de dados, compreendendo a transferência de arquivos, documentos, e demais informações do site legado em plataforma WordPress para o novo ambiente de produção, incluindo a validação da integridade dos dados	UND	1	R$

	migrados, a verificação de inconsistências ou corrompimentos de arquivos, bem como a elaboração da documentação técnica correspondente.			

2.2 ITEM 1: Especificação do Servidor dedicado para acesso Ilimitado para site institucional em WordPress:

2.2.1 ***Servidor de Aplicação***

2.2.1.1 Disponibilidade e SLA: Garantia de Uptime mensal mínimo de 99,95% (excluindo janelas de manutenção programada). O provedor deverá fornecer Acordo de Nível de Serviço (SLA) documentado.

2.2.1.2 Tipo: Servidor Virtual Privado (VPS), Servidor Dedicado ou Instância de Cloud IaaS com recursos dedicados.

2.2.1.3 Processador: Mínimo de 4 (quatro) vCPUs dedicadas, arquitetura x86_64 com frequência mínima de 2,6 GHz. Garantia de não superalocação (oversubscription) excessiva.

2.2.1.4 Memória RAM: Mínimo de 16 (dezesseis) GB de RAM.

2.2.1.5 Armazenamento: Mínimo de 500 (quinhentos) GB SSD NVMe, garantindo altíssima performance de I/O para carregamento rápido de arquivos e banco de dados.

2.2.1.6 Sistema Operacional: Ubuntu Server 22.04 LTS, Debian 12 (64 bits) ou AlmaLinux/Rocky Linux

2.2.1.7 Conectividade: Link mínimo de 1 Gbps, com endereço IP fixo público dedicado.

2.2.1.8 Acesso Remoto e Gerenciamento: SSH seguro e/ou painel administrativo web de alta performance (cPanel, Plesk, ou painel gerenciado do provedor) com Autenticação de Dois Fatores (2FA).

2.2.1.9 CDN (Rede de Entrega de Conteúdo): Opcional ou nativo da plataforma (ex: Cloudflare), para distribuição global de conteúdo estático e aceleração.

2.2.2 ***Servidor Web e Ambiente de Aplicação (Foco em Velocidade)***

2.2.2.1 Servidor Web: Nginx (como servidor web principal ou proxy reverso) ou LiteSpeed Server (ideal para performance e cache nativo). Deve suportar HTTP/2 ou HTTP/3 (QUIC).

2.2.2.2 Linguagem de Programação: PHP 8.1 ou superior, operando com PHP-FPM (FastCGI Process Manager) com configuração otimizada para concorrência e pool de processos.

2.2.2.3 Mecanismo de Aceleração: OPcache ativo e ajustado para o ambiente WordPress, garantindo o cache do código PHP.

2.2.2.4 Extensões obrigatórias do PHP: curl, dom, exif, fileinfo, filter, gd, iconv, intl, mbstring, mysqli, pcre, pdo_mysql, imagick, zip, e xml.

2.2.2.5 Cache de Objeto Persistente: Redis ou Memcached dedicado para o cache de objetos do WordPress, reduzindo a carga no banco de dados.

2.2.2.6 Controle de Versão: Git instalado no servidor para facilitar o *deployment* e o controle de versão da aplicação.

2.2.2.7 Serviço de E-mail: Postfix, Sendmail ou equivalente, configurado com SPF e DKIM para evitar que notificações e e-mails transacionais caiam em spam.

*2.2.3 **Banco de Dados***

2.2.3.1 Sistema Gerenciador: MariaDB 10.6+ ou MySQL 8.0+, configurado com o motor InnoDB.

2.2.3.2 Configuração Otimizada: O arquivo de configuração (my.cnf ou equivalente) deve ser ajustado para o WordPress, especialmente o innodb_buffer_pool_size para alocar pelo menos 50% da RAM dedicada à memória do pool de buffer do InnoDB.

2.2.3.3 Banco de dados dedicado exclusivamente ao site WordPress.

2.2.3.4 Conexões restritas ao servidor de aplicação (IP privado ou localhost).

2.2.3.5 Realização de otimização periódica de tabelas e limpeza de transientes/revisões excessivas para manter a performance do banco.

*2.2.4 **Segurança da Informação (Reforçada para WordPress)***

2.2.4.1 Certificado SSL/TLS: Certificado Let's Encrypt ou ICP-Brasil válido, com renovação automática e redirecionamento obrigatório HSTS (HTTP Strict Transport Security).

2.2.4.2 Firewall de Aplicação (WAF): Ativo e configurado (como ModSecurity ou WAF nativo do provedor) para mitigar ataques comuns ao WordPress (brute force, injeção de SQL, XSS).

2.2.4.3 IDS/IPS: Sistema de Detecção e Prevenção de Intrusão (Fail2ban configurado para bloquear tentativas de login SSH/FTP e ataques ao wp-login).

2.2.4.4 Hardening do SO: Desativação de serviços desnecessários e Autenticação via chave pública SSH (senha desativada para root).

2.2.4.5 Isolamento de Contas: Permissões de arquivos restritas (chown e chmod adequados) para garantir que apenas o usuário do web server tenha acesso de escrita necessário.

2.2.4.6 Monitoramento de Integridade: Ferramenta ou política para monitorar a integridade dos arquivos do core do WordPress e alertar sobre alterações não autorizadas.

2.2.4.7 Logs: Logs de acesso e erro do Servidor Web e Banco de Dados mantidos e monitorados por, no mínimo, 90 dias.

*2.2.5 **Política de Backup e Recuperação***

2.2.5.1 Frequência de Backup: Backup automático e incremental do banco de dados e diretórios da aplicação (incluindo wp-content) a cada 12 (doze) horas (ou mais frequentemente, dependendo da criticidade e volume de alterações).

2.2.5.2 Armazenamento: Backups armazenados em local seguro, distinto do servidor principal (off-site) e em cópia imutável (Storage Object).

2.2.5.3 Retenção: Retenção mínima de 30 (trinta) dias, com pelo menos 1 (um) backup mensal retido por 1 (um) ano.

2.2.5.4 Restaurabilidade: Garantia de restauração total do ambiente (incluindo arquivos e banco de dados) em até 4 horas (RTO - Recovery Time Objective) após a solicitação.

2.2.5.5 Procedimento: Procedimento documentado de restauração e teste de integridade dos backups realizado e documentado a cada 6 meses.

*2.2.6 **Outros Requisitos para o Site:***

2.2.6.1 4.1. Advanced Custom Fields: Será obrigatória a instalação e ativação da versão Advanced Custom Fields PRO para a customização e gerenciamento de campos personalizados. Este plugin é fundamental para garantir a flexibilidade, o poder e a interface intuitiva na criação e manipulação de metadados, Post Types e blocos personalizados do site. O uso do ACF PRO permite a estruturação avançada do conteúdo, dissociando a apresentação (front-end) da gestão de dados (back-end), resultando em um código

mais limpo e uma experiência de edição de conteúdo otimizada para os administradores.

2.2.6.2 Akismet Anti-spam: Spam Protection: É mandatório o uso do plugin Akismet Anti-spam: Spam Protection para assegurar a defesa do website contra comentários e submissões de formulários de spam. O Contratado deverá realizar a configuração completa do plugin, incluindo a obtenção e ativação da chave API apropriada (Akismet é freemium, mas o contratado deve garantir que a chave esteja ativa e funcionando, usando o plano gratuito ou adquirindo um, se necessário) para manter o site protegido em tempo integral, garantindo a integridade da seção de comentários e a qualidade dos dados submetidos.

2.2.6.3 CookieYes | GDPR Cookie Consent: O plugin CookieYes | GDPR Cookie Consent deverá ser implementado e configurado para garantir a conformidade do website com as regulamentações de privacidade de dados, como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o GDPR na União Europeia. A solução deve exibir de forma clara e funcional um banner de consentimento de cookies, permitindo que o usuário aceite, rejeite ou personalize as preferências, conforme as exigências legais vigentes.

2.2.6.4 Dante Testa - Search posts by Title: Será exigida a instalação do plugin Dante Testa - Search posts by Title. Este plugin deve ser integrado de forma correta com o JetSmartFilters (conforme item 4.10) para estender a funcionalidade de busca, permitindo que os usuários realizem pesquisas eficazes especificamente pelo título dos posts ou tipos de conteúdo personalizados configurados.

2.2.6.5 Editor clássico: A instalação do plugin Editor clássico é obrigatória para garantir a compatibilidade e a funcionalidade da interface de edição de conteúdo tradicional do WordPress. Este requisito visa manter a familiaridade do ambiente de edição para o corpo editorial e garantir o funcionamento de meta boxes e outras funcionalidades que dependem do antigo estilo da tela de edição, mesmo que a construção de páginas seja primariamente feita via Elementor.

2.2.6.6 Elementor: O desenvolvimento de todas as páginas e templates do site deverá utilizar o construtor de páginas Elementor. Este plugin é o alicerce principal para a construção da arquitetura visual e funcional do website, sendo essencial para o desenvolvimento pixel-perfect, a edição responsiva e a capacidade de arrastar e soltar. Sua instalação é pré-requisito para diversos outros plugins listados, e a estrutura de desenvolvimento deve seguir as melhores práticas do Elementor.

2.2.6.7 JetElements For Elementor: A utilização do plugin JetElements For Elementor é requerida para expandir a biblioteca de módulos e

widgets disponíveis no Elementor. Este aditivo deve ser empregado para criar diversos tipos de conteúdo e aplicar estilos atrativos de forma eficiente, complementando as funcionalidades nativas do Elementor e auxiliando na agilidade e riqueza do design de página.

2.2.6.8 JetEngine, JetEngine - Custom visibility conditions e JetEngine - Get attachment file link by ID: Será obrigatório o uso do conjunto de plugins JetEngine (incluindo JetEngine - Custom visibility conditions e JetEngine - Get attachment file link by ID) para a gestão avançada de dados dinâmicos. O JetEngine deve ser utilizado para a criação e gerenciamento de Custom Post Types, Taxonomias Personalizadas, Meta Boxes complexas e Lists Dinâmicas, sendo a solução central para a estruturação do conteúdo não-estático do site. Os plugins auxiliares devem ser configurados para implementar lógica de visibilidade avançada e facilitar a recuperação de links de arquivos anexados dinamicamente.

2.2.6.9 JetSmartFilters: O plugin JetSmartFilters deverá ser implementado para adicionar funcionalidades de filtragem baseadas em AJAX às listagens dinâmicas de conteúdo (construídas com JetEngine e Elementor/CrocoBlock). O Contratado deve configurar os filtros de maneira intuitiva e de alta performance, permitindo que os usuários naveguem e refinem o conteúdo de forma eficiente e sem recarregamento da página.

2.2.6.10 LiteSpeed Cache: Para garantir a alta performance e otimização da velocidade de carregamento, o plugin LiteSpeed Cache deverá ser instalado e configurado de maneira minuciosa. O Contratado é responsável por aplicar as configurações ideais de cache de página, otimização de imagens, CSS e JavaScript (incluindo minificação, combinação e carregamento assíncrono), de forma a atingir os melhores resultados de page speed e core web vitals possíveis para a infraestrutura de hospedagem fornecida.

2.2.6.11 ManageWP – Worker: A instalação e conexão do plugin ManageWP - Worker é exigida para fins de gerenciamento e manutenção centralizada do site. Este plugin deve ser ativado e conectado à plataforma de gestão (ManageWP ou GoDaddy Pro), possibilitando que a equipe de manutenção realize backups, atualizações, monitoramento de segurança e outras tarefas de forma eficiente a partir de um único painel.

2.2.6.12 PRO Elements: O plugin PRO Elements deve ser utilizado em conjunto com o Elementor (conforme item 4.6) para habilitar as funcionalidades GPL (General Public License) que mimetizam os recursos avançados do Elementor Pro, como widgets adicionais, o Theme Builder e o construtor de Popups. Esta exigência visa prover

ferramentas de desenvolvimento robustas e flexíveis sem a necessidade da licença comercial do Elementor Pro.

2.2.6.13 PWA: A funcionalidade de Progressive Web App (PWA) será implementada através do plugin PWA. O Contratado deve garantir que o plugin esteja ativo e configurado para trazer os recursos de PWA para o website (como a possibilidade de instalação do site na tela inicial do dispositivo, funcionamento offline básico, etc.), melhorando a experiência do usuário em dispositivos móveis.

2.2.6.14 Simple History: O plugin Simple History deverá ser instalado e mantido ativo para registrar detalhadamente todas as ações significativas ocorridas no back-end do WordPress. Esta ferramenta é essencial para a auditoria e rastreamento de atividades de usuários, facilitando a identificação de alterações de conteúdo, configurações e atividades de manutenção.

2.2.6.15 Social Chat: O plugin Social Chat deve ser configurado para integrar um canal de comunicação via WhatsApp, permitindo que os visitantes entrem em contato com a equipe com apenas um clique. A funcionalidade deve ser responsiva e personalizável conforme a identidade visual e as necessidades de atendimento especificadas neste Termo.

2.2.6.16 String Locator: A instalação do plugin String Locator é um requisito técnico para o desenvolvimento. Ele será usado para auxiliar na localização de strings de texto (textos) dentro dos arquivos de temas e plugins. Embora possa ser desativado após o desenvolvimento e a tradução final, sua presença é exigida para fins de otimização e garantia da qualidade na fase de construção.

2.2.6.17 Wordfence Security: Para a proteção do site, o plugin Wordfence Security deverá ser instalado, ativado e configurado em sua versão gratuita. O Contratado é responsável por configurar o firewall, o antivírus e o scanner de malware, aplicando as melhores práticas para garantir uma camada robusta de segurança, monitoramento e defesa contra ataques cibernéticos.

2.2.6.18 WP Mail SMTP Pro: O plugin WP Mail SMTP Pro deve ser utilizado e configurado para reconfigurar a função de envio de e-mails (wp_mail()), garantindo a alta entregabilidade e confiabilidade das comunicações transacionais (formulários de contato, senhas, etc.). O Contratado deverá integrar o plugin com um provedor de SMTP profissional (ex: Gmail, Mailgun, SendGrid ou SMTP de terceiros) a ser fornecido/contratado pela Contratante. A licença PRO (se necessária) deve ser providenciada pela Contratante, mas a instalação e configuração são responsabilidade do Contratado.

2.2.6.19 WPS Hide Login: O plugin WPS Hide Login é mandatório para aumentar a segurança da área administrativa do site. O Contratado deve utilizá-lo para alterar a URL padrão de login (wp-login.php), dificultando ataques de força bruta e varreduras automáticas que visam acessar a administração do WordPress.

2.2.6.20 Yoast SEO: A otimização para mecanismos de busca (SEO) deve ser gerenciada pelo plugin Yoast SEO. O Contratado é responsável pela correta instalação, ativação e configuração inicial (incluindo a configuração do sitema XML, títulos e meta descrições para a página inicial e tipos de conteúdo) de acordo com as diretrizes de SEO fornecidas pela Contratante.

2.2.6.21 PDF Embedder (Versão Comercial / Premium): Será obrigatória a instalação e a ativação do plugin PDF Embedder na sua versão comercial ou premium. Este recurso é essencial para permitir a incorporação (embedding) de documentos PDF diretamente nas páginas e posts do WordPress, garantindo que o conteúdo seja visualizado de forma responsiva, amigável ao usuário e sem a necessidade de pop-ups ou downloads forçados. A versão comercial deve ser utilizada para explorar funcionalidades avançadas, como segurança de download (proteção de PDFs) e personalização da barra de ferramentas de navegação e zoom do leitor.

2.2.6.22 Plugins de Flipbook / Visualização 3D: É exigida a instalação de um plugin de mercado de reconhecida qualidade, apto a criar a funcionalidade de Flipbook ou Visualização 3D para documentos estáticos (como catálogos, revistas ou relatórios anuais). O recurso deve proporcionar uma experiência de leitura interativa e engajadora, simulando o folhear de páginas. O Contratado deve garantir que o plugin escolhido seja compatível com a arquitetura Elementor/Crocoblock e otimizado para mobile, com carregamento rápido e navegação intuitiva.

2.2.6.23 PDF Generator for WP Pro: O plugin PDF Generator for WP Pro deve ser instalado e configurado para possibilitar a geração dinâmica e on-demand de documentos em formato PDF a partir do conteúdo do website. Este requisito visa permitir que os usuários gerem cópias formatadas de páginas, artigos ou relatórios de maneira eficiente. O Contratado é responsável por adquirir a licença PRO e configurar o design do PDF gerado para aderir ao branding e à identidade visual do site, além de garantir a correta gestão dos modelos de documentos.

2.2.6.24 Integrações com Sistemas .NET Legados: A solução final de WordPress deve prever e implementar, no escopo do desenvolvimento, a capacidade de integração e comunicação com sistemas legados baseados na plataforma .NET da administração. O

Contratado deverá desenvolver ou configurar endpoints (via APIs, Web Services REST/SOAP ou bibliotecas específicas) que permitam a troca de dados em tempo real ou assíncrona com os sistemas .NET da Contratante, como, por exemplo, para consultas de dados cadastrais, validação de informações ou submissão de formulários complexos. A arquitetura de integração deverá ser segura, escalável e devidamente documentada no As-Built.

2.2.6.25 Busca em PDF Adobe ou equivalente: É imperativo que a funcionalidade de busca nativa do WordPress seja estendida e configurada para permitir a indexação e a busca de conteúdo textual presente dentro de documentos PDF hospedados no site. O Contratado deverá utilizar e configurar plugins ou soluções de terceiros (como plugins de busca avançada com suporte a indexação de documentos) que sejam capazes de realizar a análise e a identificação de palavras-chave no corpo dos arquivos PDF, integrando esses resultados de forma coesa aos resultados de busca padrão do WordPress, garantindo que o usuário possa localizar informações relevantes mesmo quando estiverem contidas em documentos anexados e não apenas no corpo dos posts ou páginas.

2.3 **ITEM 2 - Especificação do Servidor dedicado para acesso Ilimitado para sistema GLPI:**

2.3.1.1 Servidor de Aplicação: Servidor Virtual Privado (VPS) ou servidor dedicado em ambiente de nuvem;

2.3.1.2 Disponibilidade e SLA: Garantia de Uptime mensal mínimo de 99,9% (excluindo janelas de manutenção programada). O provedor deverá fornecer Acordo de Nível de Serviço (SLA) documentado.

2.3.1.3 Tipo: Servidor Virtual Privado (VPS) ou servidor dedicado em ambiente de nuvem (IaaS).

2.3.1.4 Processador: mínimo de 4 (quatro) vCPUs dedicadas, arquitetura x86_64 com frequência mínima de 2,6 GHz. Deve ser garantida a não superalocação (oversubscription) excessiva de recursos para evitar degradação de desempenho.

2.3.1.5 Memória RAM: mínimo de 8 (oito) GB.

2.3.1.6 Armazenamento: mínimo de 120 (cento e vinte) GB SSD, preferencialmente em tecnologia NVMe, com garantia de alta performance de I/O (Input/Output).

2.3.1.7 Sistema Operacional: Ubuntu Server 22.04 LTS ou Debian 12 (64 bits). O provedor deve oferecer suporte a estas distribuições.

2.3.1.8 Conectividade: link mínimo de 1 Gbps, com endereço IP fixo público dedicado.

2.3.1.9 Acesso remoto: SSH seguro e/ou painel administrativo web (com autenticação forte, como 2FA).

2.3.1.10 Monitoramento: Ferramenta de monitoramento de recursos (CPU, RAM, Disco, Rede) e status do serviço (HTTP/HTTPS) com alertas configuráveis.

*2.3.2 **Servidor Web e Ambiente de Aplicação***

2.3.2.1 Servidor Web: Apache HTTP Server 2.4 ou superior, compatível com as dependências do GLPI. Alternativamente, Nginx pode ser utilizado como proxy reverso para otimizar o desempenho de requisições estáticas.

2.3.2.2 Linguagem de Programação: PHP 8.1 ou superior, com mecanismo de aceleração de bytecode ativo (OPcache configurado).

2.3.2.3 Extensões obrigatórias do PHP: pdo, pdo_mysql, mysqli, gd, zip, mbstring, curl, intl, xml, json, openssl e ldap. Todas as extensões devem estar na versão estável e compatível com a versão do PHP utilizada.

2.3.2.4 Gerenciador de dependências: Composer 2.x.

2.3.2.5 Serviço de e-mail: Postfix ou equivalente, para envio de notificações automáticas do sistema. Deve ser configurado com Sender Policy Framework (SPF) e DomainKeys Identified Mail (DKIM) para evitar que e-mails sejam marcados como spam.

2.3.2.6 Mecanismo de cache: Redis ou Memcached. O mecanismo de cache deve ser dedicado e ter recursos de memória adequados (mínimo de 512MB dedicado, se não estiver incluso na RAM do VPS/dedicado).

2.3.2.7 Job Scheduler: Configuração de cron jobs para tarefas automáticas do GLPI (e.g., mail collector, actions), com monitoramento de execução.

*2.3.3 **Banco de Dados***

2.3.3.1 Sistema Gerenciador: MariaDB 10.6, MySQL 8.0 ou superiores.

2.3.3.2 Banco de dados dedicado exclusivamente ao sistema GLPI.

2.3.3.3 Conexões restritas ao servidor de aplicação (localhost ou endereço IP privado específico).

2.3.3.4 Política de backup diário automatizado, com retenção mínima de 30 (trinta) dias.

2.3.3.5 Realização de otimização periódica de índices e limpeza de registros temporários.

2.3.3.6 Configuração Otimizada: O arquivo de configuração (my.cnf ou equivalente) deve ser otimizado para a carga de trabalho do GLPI (e.g., ajustes em innodb_buffer_pool_size, max_connections, query_cache).

2.3.3.7 Replicação: Disponibilidade de replicação de banco de dados (Master/Slave ou Cluster) como opcional de escalabilidade e alta disponibilidade.

*2.3.4 **Segurança da Informação***

2.3.4.1 Certificado digital SSL/TLS válido (Let's Encrypt ou ICP-Brasil). Deve ser configurada a renovação automática e o redirecionamento obrigatório de HTTP para HTTPS (HSTS).

2.3.4.2 Firewall de aplicação ativo (WAF - Web Application Firewall, como ModSecurity ou equivalente) e Firewall de Rede (UFW, CSF ou equivalente).

2.3.4.3 Bloqueio de portas não utilizadas e restrição de acesso administrativo (apenas via VPN ou IPs de origem definidos).

2.3.4.4 Autenticação via chave pública SSH para administradores. Desativação do login de root via SSH com senha.

2.3.4.5 Sistema de detecção e prevenção contra tentativas de acesso indevido (Intrusion Detection/Prevention System - IDS/IPS), como Fail2ban configurado.

2.3.4.6 Políticas automáticas de atualização de segurança do sistema operacional e pacotes (patches de segurança com reinicialização em janela programada).

2.3.4.7 Registro e retenção de logs com rotação semanal (logrotate configurado). Os logs de acesso e erro do Servidor Web e Banco de Dados devem ser monitorados e mantidos por no mínimo 90 dias.

2.3.4.8 Hardening do Sistema Operacional: Aplicação de hardening no SO, seguindo as melhores práticas de segurança (ex: desativação de serviços desnecessários).

2.3.4.9 Varredura de Vulnerabilidades: Realização de varredura periódica de vulnerabilidades no ambiente, com relatório e plano de mitigação apresentado

*2.3.5 **Política de Backup e Recuperação***

2.3.5.1 Backup automático e incremental do banco de dados e diretórios da aplicação a cada 24 (vinte e quatro) horas.

2.3.5.2 Armazenamento dos backups em local seguro e distinto do servidor principal (off-site ou em Storage Object dedicado).

2.3.5.3 Retenção mínima de 30 (trinta) dias, com pelo menos 1 (um) backup mensal retido por 1 (um) ano.

2.3.5.4 Procedimento documentado de restauração e verificação de integridade dos backups (Teste de Restauração deve ser realizado e documentado a cada 6 meses).

2.3.5.5 Disponibilização de acesso aos arquivos de backup (via SFTP, Painel Web ou equivalente) para a equipe técnica da contratante.

2.4 ITEM 3: Suporte e Manutenção de Sites e Aplicativos:

2.4.1 Suporte contínuo para sites e aplicativos, de acordo com as melhores práticas do ITIL v3, utilizando as seguintes tecnologias:

2.4.1.1 Front-end: HTML, CSS, JavaScript, React.js, Vue.js,

2.4.1.2 Back-end: PHP (com ênfase no framework Laravel), Python

2.4.1.3 Banco de Dados: MySQL, PostgreSQL, MongoDB.

2.4.1.4 Infraestrutura**:** Servidores Web (Apache/Nginx/LiteSpeed), Sistemas Operacionais Linux (Ubuntu, Debian) e plataformas de Cloud Computing.

2.4.2 Serviços de Desenvolvimento Sob Demanda e evolução: A manutenção deverá incluir a capacidade de realizar melhorias contínuas, otimizações e a criação de novas páginas e funcionalidades sob demanda. Estes serviços serão executados mediante solicitação formal da CONTRATANTE e análise, envio e aprovação do Plano de Trabalho da CONTRATADA, garantindo a qualidade, segurança e eficiência no desenvolvimento de novas soluções.

2.4.3 Processos de Suporte e Qualidade: A prestação do serviço deve aderir rigorosamente às melhores práticas do ITIL v3/v4, organizadas nos seguintes processos:

2.4.3.1 Gestão de Incidentes:

2.4.3.1.1 Suporte Contínuo: Fornecimento de suporte técnico para corrigir falhas e erros operacionais nos sistemas.

2.4.3.1.2 Abertura de Chamados: Plataforma de ticketing robusta para permitir a abertura, acompanhamento e fechamento de chamados de suporte, disponível 24x7 para incidentes de alta prioridade.

2.4.3.1.3 Priorização e SLA: Classificação de incidentes baseada em Impacto vs. Urgência. A resolução será priorizada conforme o Acordo de Nível de Serviço (SLA) estabelecido no Anexo A.

2.4.3.2 Gestão de Problemas:

2.4.3.2.1 Análise de Causa Raiz (RCA): Identificação e análise proativa e reativa das causas fundamentais de incidentes repetidos ou de alto impacto.

2.4.3.2.2 Soluções Permanentes: Proposição de soluções definitivas e implementação de Workarounds (soluções de contorno) para evitar a recorrência dos problemas.

2.4.3.3 Gestão de Mudanças e Releases (DevOps):

2.4.3.3.1 Controle de Versão: Uso obrigatório de sistemas de controle de versão (Git) para todo o código-fonte, garantindo rastreabilidade e reversibilidade das alterações.

2.4.3.3.2 Deployment Controlado: Planejamento e execução de todas as mudanças no ambiente de produção de forma controlada e automatizada (CI/CD).

2.4.3.3.3 Avaliação de Risco: Realização de avaliação de impactos e riscos antes da implementação de mudanças críticas, podendo envolver uma reunião de aprovação (CAB - Change Advisory Board).

2.4.3.4 Gestão de Conhecimento e Configuração:

2.4.3.4.1 Base de Conhecimento: Criação e manutenção de uma Base de Conhecimento (KB) acessível, contendo artigos de solução de problemas frequentes e FAQs para o usuário final e a equipe de suporte.

2.4.3.4.2 Gerenciamento de Configuração (CMDB): Manutenção de um inventário detalhado de todos os ativos de TI, suas

configurações, dependências e versões de software e sistemas utilizados.

2.4.3.5 Análise de Performance e Otimização

2.4.3.5.1 Monitoramento Contínuo: Monitoramento contínuo da performance, disponibilidade (uptime) e tempo de resposta do site e dos aplicativos.

2.4.3.5.2 Otimização Baseada em Dados: Implementação de melhorias de performance (e.g., otimização de consultas SQL, cache, entrega de ativos) baseadas em dados de análise e auditorias de código.

2.4.3.5.3 Relatórios Mensais: Apresentação de relatórios de desempenho e disponibilidade, incluindo indicadores-chave de performance (KPIs).

2.4.3.6 Segurança da Informação:

2.4.3.6.1 Atualizações de Segurança: Aplicação de políticas automáticas e manuais de patch para o sistema operacional, linguagens e frameworks de desenvolvimento, corrigindo vulnerabilidades conhecidas.

2.4.3.6.2 Hardening e Mitigação: Adoção de práticas de hardening e implementação de soluções de segurança (WAF, IDS/IPS) para prevenção contra tentativas de acesso indevido e ataques comuns (injeção SQL, XSS).

2.4.3.6.3 Backup e Recuperação: Verificação da integridade dos backups (banco de dados e arquivos) e manutenção de um procedimento documentado de restauração para garantir a capacidade de recuperação de desastres dentro do RTO (Recovery Time Objective) estabelecido.

2.5 **ITEM 4: Migração de conteúdo do site antigo do ICISMEP:**

2.5.1 O serviço consiste na migração seletiva de arquivos, documentos e informações específicas de um site WordPress legado (*Site A*) para o novo site WordPress em produção (*Site B*), com foco na recuperação de conteúdo de um banco de dados potencialmente corrompido e na sua alocação em uma nova seção dedicada.

2.5.2 ***Escopo e Pré-requisitos do Projeto:***

2.5.2.1 Origem (Site A - Legado): Ambiente WordPress com risco de corrupção de banco de dados.

2.5.2.2 Destino (Site B - Produção): Ambiente WordPress já em pleno funcionamento.

2.5.2.3 Destino Final do Conteúdo: O conteúdo migrado deverá ser consolidado em uma nova página (ou seção) no Site B, nomeada "Arquivos e Documentos Antigos".

2.5.2.4 Natureza da Migração: Migração seletiva e de recuperação, focada exclusivamente em arquivos, documentos e posts específicos (a ser detalhado no Anexo A), e não em configurações ou temas.

*2.5.3 **Processo Metodológico de Migração e Recuperação***

2.5.3.1 O processo será dividido em quatro fases críticas, com foco especial na segurança do Site B.

2.5.3.2 *Fase 1: Análise, Clonagem e Isolamento*

2.5.3.2.1 Análise de Integridade: Realização de uma análise inicial do banco de dados e da estrutura de arquivos do Site A para identificar o nível e a natureza da corrupção.

2.5.3.2.2 Clonagem de Segurança: Criação de um clone completo do Site A para um ambiente de staging isolado e seguro, garantindo que as operações de recuperação não afetem o ambiente legado original ou o Site B em produção.

2.5.3.2.3 Backup Imediato: Execução de backup completo e verificado do Site B (destino) antes de iniciar qualquer importação, garantindo um ponto de restauração imediato.

2.5.3.3 *Fase 2: Recuperação e Extração Seletiva*

2.5.3.3.1 Recuperação do Banco de Dados: Aplicação de ferramentas e técnicas especializadas para tentar reparar a corrupção do banco de dados no ambiente de staging isolado.

2.5.3.3.2 Extração de Arquivos: Extração manual e seletiva de documentos (PDFs, DOCs, etc.) e mídias (imagens) do diretório wp-content/uploads do Site A.

2.5.3.3.3 Extração de Conteúdo (Posts/Páginas):

- *Se Banco Reparado:* Exportação seletiva de posts e páginas específicos via ferramenta nativa do WordPress ou SQL, focando apenas no conteúdo listado.

- *Se Banco Irreparável:* Extração manual do conteúdo (texto e links internos) diretamente do front-end do Site A ou de cópias em cache, garantindo a integridade textual.

2.5.3.4 *Fase 3: Sanitização, Importação e Alocação*

2.5.3.4.1 Sanitização de Dados: Todo o conteúdo extraído (especialmente dados do banco de dados) será filtrado e limpo para remover scripts maliciosos, códigos legados desnecessários ou referências de URL internas do Site A.

2.5.3.4.2 Criação da Estrutura de Destino: Criação da nova página/seção "Arquivos e Documentos Antigos" no Site B, com estrutura de posts ou custom post types dedicada para receber o conteúdo legado.

2.5.3.4.3 Importação de Mídia: Upload dos arquivos e documentos (Fase 2) para o Site B através da biblioteca de mídia ou FTP seguro, garantindo que o WordPress registre as novas URLs.

2.5.3.4.4 Inclusão de Conteúdo: Inclusão dos posts e documentos recuperados na estrutura recém-criada no Site B.

2.5.3.5 *Fase 4: Validação e Go-Live*

2.5.3.5.1 Teste de Links: Verificação dos links internos dos documentos migrados para garantir que apontem corretamente para os novos arquivos no Site B.

2.5.3.5.2 Teste de Visualização: Verificação da correta exibição e acesso de todos os arquivos e documentos listados na nova seção "Arquivos e Documentos Antigos" em diferentes navegadores e dispositivos.

2.5.3.5.3 Homologação do Cliente: O conteúdo migrado será submetido à aprovação do Contratante no ambiente de staging do Site B.

2.5.3.5.4 Deployment Final: Após aprovação, a seção "Arquivos e Documentos Antigos" será migrada do staging para o ambiente de produção do Site B.

2.5.4 **Requisitos de Segurança e Controle de Qualidade**

2.5.4.1 Segurança do Ambiente de Produção (Site B): Nenhuma injeção direta de banco de dados será permitida. Todos os dados migrados passarão por ferramentas de sanitização e serão importados via

APIs do WordPress ou ferramentas oficiais, minimizando o risco de comprometer a segurança do Site B.

2.5.4.2 Isolamento: Uso de um ambiente de staging completamente isolado para todas as operações de recuperação e manipulação do Site A.

2.5.4.3 Documentação de Falhas: Caso a corrupção do banco de dados impeça a recuperação de algum item listado, o item será documentado em um Relatório de Itens Não Recuperados, justificando a falha.

2.5.4.4 Relatório de Migração: Entrega de um relatório final detalhando os passos executados, a lista completa dos arquivos migrados com sucesso e as URLs de destino no Site B.

2.6 Qualificação dos profissionais

2.6.1 Profissional com Pós-Graduação em Desenvolvimento Fullstack: A Contratada deve disponibilizar pelo menos um (1) profissional registrado em seu quadro funcional ou com contrato ativo que possua Pós-Graduação em Desenvolvimento Fullstack ou área correlata. A comprovação desta exigência deverá ser feita mediante a apresentação de cópia do Certificado de Conclusão da Pós-Graduação e da comprovação do vínculo profissional (por meio de registro em carteira, contrato social ou contrato de prestação de serviços).

2.6.2 Profissional com Certificação ITIL v3: A Contratada deve disponibilizar pelo menos um (1) profissional registrado no quadro funcional ou prestando serviço que possua Certificação ITIL v3 (Information Technology Infrastructure Library) ou superior. A comprovação será realizada através da apresentação de cópia do Certificado de Conclusão da Certificação ITIL e da comprovação do vínculo profissional com a empresa.

2.6.3 Profissional Formado em Gestão de Projetos: A Contratada deve disponibilizar pelo menos um (1) profissional registrado em seu quadro funcional ou prestando serviço que seja formado (Graduado) em Gestão de Projetos ou área correlata. Para fins de comprovação, deverá ser apresentada cópia do Diploma de Conclusão da Graduação e a comprovação do vínculo profissional.

2.6.4 Profissional Formado em Marketing: A Contratada deve disponibilizar pelo menos um (1) profissional registrado no quadro funcional ou prestando serviço que seja formado (Graduado) em Marketing ou área correlata. A comprovação desta exigência dar-se-á pela apresentação de cópia do Diploma de Conclusão da Graduação e da comprovação do vínculo profissional com a empresa.

2.7 Painel DNS

2.7.1 A empresa de hospedagem deve fornecer um painel de controle (GUI) com credenciais de acesso exclusivas, que permita a gestão completa de todas as

Zonas DNS do domínio. Este acesso deve ser disponibilizado imediatamente após a ativação do serviço.

2.7.2 O acesso deve ser de nível Administrador (Full Access), permitindo todas as operações listadas no requisito 2. Não serão aceitas contas restritas ou de somente leitura (read-only).

3 DA FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

3.1 O critério de julgamento para a escolha da proposta mais vantajosa, será o menor preço.

3.2 As exigências de habilitação jurídica, fiscal, social e trabalhista são as usuais para a generalidade dos objetos.

3.3 Os critérios de habilitação técnica a serem atendidos pelo fornecedor serão:

3.3.1 Apresentação de no mínimo 1 (um) atestado de capacidade técnica em nome da empresa, fornecido por pessoa jurídica de direito público ou privado, em papel timbrado, comprovando que a empresa executa satisfatoriamente fornecimento ao objeto em complexidade, linguagens, requisitos e quantidades iguais ou similares.

4 DAS NORMAS DE EXECUÇÃO

4.1 SLA para o Serviço de Hospedagem de Servidores

4.1.1 Disponibilidade Mínima (Uptime): É necessário garantir um Uptime mensal mínimo de 99,95%.

4.1.2 Janelas de Manutenção: Manutenções programadas que resultem em indisponibilidade devem ser comunicadas com no mínimo 48 horas de antecedência e agendadas fora do horário comercial (preferencialmente entre 00:00 e 06:00, Horário de Brasília).

4.1.3 Penalidade por Quebra de SLA: Caso o Uptime mensal dos servidores caia abaixo de 99,95% ou hajam atrasos no SLA será aplicada uma penalidade cumulativa de até 25% no valor da mensalidade subsequente, dependendo da gravidade da queda de Uptime seguindo as seguintes regras:

4.1.3.1 **Penalidades de Uptime mensal (servidor):** Para um Uptime mensal abaixo de 99,95% de disponibilidade será descontado o percentual relativo à diferença entre o Uptime contratual e o Uptime real:

$$\boldsymbol{Penalidade\ P1 = 99,95\% - \ UptimeReal}$$

4.1.3.2 **Penalidades de atraso de SLA:** Para atrasos nos atendimentos de atendimentos de prioridade Baixa à Crítica (P4 à P1) segue-se o seguinte cálculo:

$$Atraso\ percentual\ SLA = \frac{Treal - SLA}{SLA}$$

$$Penalidade\ SLA = min(Atraso\ percentual, 1) \times 25\%$$

4.1.3.3 Embora as penalidades possam ser aplicadas de forma cumulativa dentro do mês, refletindo a reincidência ou a gravidade das falhas, o teto de 25% visa evitar que o total de descontos ou créditos supere o valor proporcional do risco assumido pela contratada, impedindo que o contrato se torne inviável economicamente.

3.1.1 A CONTRATADA deverá realizar o monitoramento ativo de CPU, RAM, I/O de disco e Uptime do serviço HTTP/HTTPS a cada 10 minutos, 24x7.

3.1.2 Notificação automática à equipe técnica responsável em até 5 minutos após a detecção de qualquer falha crítica ou queda de Uptime.

3.1.3 Em caso de falha crítica (queda total do servidor), o tempo máximo para início da ação de correção é de 15 minutos (24x7).

3.1.4 SLA para o Serviço de Suporte e Manutenção (ITIL): O SLA é baseado na prioridade do incidente, definida pela matriz Impacto vs. Urgência. O tempo de resposta e solução varia de acordo com essa prioridade.

3.1.5 Definição de Prioridades e Prazos:

Prioridade	Nível	Cenário de Exemplo	Tempo Máximo de Resposta (TMR)	Tempo Máximo de Solução (TMS)
Crítica	P1	Indisponibilidade Total do site principal ou perda crítica de dados.	15 minutos (24x7)	2 horas (24x7)
Alta	P2	Falha em Funcionalidade Principal.	30 minutos (Horário Comercial)	8 horas úteis
Média	P3	Falha Secundária ou Melhoria Pequena.	2 horas (Horário Comercial)	24 horas úteis
Baixa	P4	Dúvidas, solicitações de documentação ou ajustes cosméticos.	4 horas (Horário Comercial)	48 horas úteis

3.2 Gestão de Mudanças e Segurança

3.2.1 Processo de Release (DevOps): Qualquer alteração de código ou configuração no ambiente de produção deve seguir obrigatoriamente o ciclo Desenvolvimento → Staging (Homologação) → Produção.

3.2.2 Rollback: A equipe deve garantir a capacidade de realizar rollbacks (reversão) de qualquer mudança implementada (código ou patch) em no máximo 30 minutos, caso a mudança cause um incidente de Prioridade Crítica (P1).

3.2.3 Atualizações de Segurança Críticas: Correções (patches) para vulnerabilidades de segurança classificadas como Críticas (CVSS acima de 9.0) devem ser aplicadas em até 48 horas após a liberação do patch pelo fabricante ou comunidade.

3.3 Política de Backup e Recuperação (RPO/RTO)

3.3.1 Ponto de Recuperação Objetivo (RPO): O tempo máximo aceitável de perda de dados é de 24 horas. O backup deve ser realizado, no mínimo, a cada 24 horas.

3.3.2 Tempo de Recuperação Objetivo (RTO): O tempo máximo para restaurar completamente o site e o banco de dados a partir do último backup verificado, em caso de falha catastrófica, é de 4 horas.

3.3.3 Verificação de Integridade: O procedimento de restore do backup deve ser testado e documentado a cada 6 meses.

3.4 Normas de Execução para o Serviço de Migração

3.4.1 O serviço de migração é um projeto de escopo fechado e opera sob regras estritas para proteger o ambiente de produção.

3.4.2 Zero Impacto no Site em produção: Todas as manipulações e tentativas de recuperação de dados do site legado devem ocorrer em um ambiente de homologação isolado. O Site em produção não pode ter seu Uptime ou performance afetados durante a execução do projeto de migração.

3.4.3 Sanitização Obrigatória: É proibida a injeção ou importação direta de dados não sanitizados no Site em Produção. Todo o conteúdo deve passar por um processo de sanitização (limpeza de código malicioso e referências legadas) antes da importação final.

3.4.4 Validação de Conteúdo: A migração será considerada concluída somente após a validação e aceite formal (por e-mail ou sistema de ticketing) por parte do Contratante.

3.4.5 Relatório Final: Será entregue um Relatório de Migração detalhado, incluindo a lista completa dos arquivos migrados com sucesso e as URLs de destino na nova seção "Arquivos e Documentos Antigos", bem como a justificativa para qualquer item que não pôde ser recuperado.

3.4.6 Prazo de Projeto: O prazo total para o projeto de migração será definido em um Cronograma de Projeto específico, a ser acordado antes do início da Fase 1, e não segue os prazos de TMS dos incidentes (P1-P4).

4 DOS PRAZOS E LOCAL DE ENTREGA

4.1 Os recebimentos provisório e definitivo ficarão a cargo do Consórcio, em conformidade com o disposto no art. 140 da Lei Federal n° 14.133/2021.

4.2 O objeto será recebido provisoriamente, de forma sumária, pelo responsável por seu acompanhamento e fiscalização, com verificação posterior da conformidade do serviço com as exigências, e definitivamente por servidor ou comissão designada por autoridade competente.

4.3 Os serviços descritos nos itens 01 e 02 deverão ser executados em até 15 (quinze) dias úteis após emissão da Autorização de Fornecimento.

4.4 Os serviços descritos no item 04 deverão ser iniciados em no máximo 15 (quinze) dias corridos após emissão da Autorização de Fornecimento, com a apresentação de cronograma de execução para aprovação do Contratante

4.5 Os acessos, links e relatórios deverão ser entregues em até 15 (quinze) dias corridos após emissão da Autorização de Serviço/Fornecimento nos seguintes endereços eletrônicos:

4.5.1 **SETOR DE TECNOLOGIA DA INFORMAÇÃO ICISMEP:** ti@icismep.mg.gov.br.

5 DOS CRITÉRIOS DE ACEITABILIDADE DO OBJETO

5.1 O acompanhamento e a fiscalização serão realizados pelo responsável designado pelo Consórcio, para análise da qualidade e verificação de sua conformidade em relação às especificações exigidas no Termo de Referência.

5.2 O responsável designado atestará no documento fiscal correspondente a prestação do serviço/entrega dos produtos nas condições exigidas, constituindo tal atestação requisito para a liberação dos pagamentos ao fornecedor.

5.3 O recebimento definitivo do objeto somente se efetivará com a atestação referida anteriormente.

5.4 No caso de defeitos ou imperfeições nos serviços/produtos, os mesmos serão recusados, cabendo à fornecedora substituí-los por outros com as mesmas características exigidas neste termo, no prazo a ser determinado pelo órgão solicitante.

6 DA FORMA DE PAGAMENTO

6.1 O pagamento decorrente da concretização do objeto será efetuado pelo contratante após a comprovação da entrega do objeto nas condições exigidas, mediante atestação do responsável e apresentação dos documentos fiscais atualizados, no prazo de até 30 (trinta) dias.

6.2 A nota fiscal/fatura deverá ser emitida pela contratada em inteira conformidade com as exigências legais contratuais, especialmente as de natureza fiscal.

6.3 Identificada pelo contratante qualquer divergência na nota fiscal/fatura, deverá devolvê-la à contratada para que sejam feitas as correções necessárias, sendo que o prazo estipulado acima será contado somente a partir da reapresentação do documento desde que devidamente sanado o vício.

6.4 Os pagamentos devidos pelo contratante serão efetuados por meio de depósito ou transferência eletrônica em conta bancária a ser informada pela contratada, preferencialmente do Banco do Brasil, ou, eventualmente, por outra forma que vier a ser convencionada entre as partes, vedando-se o pagamento por meio de boleto bancário.

6.5 Uma vez paga a importância discriminada na nota fiscal/fatura, a contratada dará ao contratante plena, geral e irretratável, quitação dos valores nela discriminados, para nada mais vir a reclamar ou exigir a qualquer título, tempo ou forma.

7 DO PRAZO DE VIGÊNCIA DO CONTRATO E DO REAJUSTE

7.1 O prazo do contrato será de 12 (doze) meses contados da data de sua assinatura, com possibilidade de renovação.

7.2 Os preços poderão ser reajustados com base no índice de Preços ao Consumidor Amplo (IPCA) ou outro que vier a substituí-lo, observado o intervalo não inferior a 12 (doze) meses contados da data limite fixada para a apresentação da proposta.

8 DO MODELO DE GESTÃO DO CONTRATO

8.1 O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e das Leis pertinentes, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

8.2 Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

8.3 As comunicações entre o Consórcio e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

8.4 O Consórcio poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

8.5 Após a assinatura do contrato ou instrumento equivalente, o Consórcio poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

8.6 A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos.

8.7 O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração.

8.8 O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados.

8.9 Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção.

8.10 O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso.

8.11 No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato.

8.12 O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou à prorrogação contratual.

8.13 O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência.

8.14 O fiscal administrativo do contrato verificará a manutenção das condições de habilitação da contratada, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário.

8.15 Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência.

8.16 O gestor do contrato coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração.

8.17 O gestor do contrato acompanhará a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotará os problemas

que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais.

8.18 O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações.

8.19 O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções.

8.20 O fiscal administrativo do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou prorrogação contratual.

8.21 O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração.

8.22 O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

8.23 O contratado deverá manter preposto aceito pela Administração no local do serviço para representá-lo na execução do contrato.

9 DA DISPONIBILIDADE ORÇAMENTÁRIA E FINANCEIRA PARA A DESPESA

9.1 As despesas decorrentes desta contratação correrão por conta das dotações orçamentárias indicados pelo setor contábil.

10 DAS CONDIÇÕES GERAIS

10.1 O Consórcio ICISMEP reserva para si o direito de não aceitar ou receber qualquer serviço/produto em desacordo com o previsto no Termo de Referência, ou em desconformidade com as normas legais ou técnicas pertinentes ao objeto.

São Joaquim de Bicas/MG, 31 de outubro de 2025.

João Gabriel Miranda de Souza
Tecnologia da Informação
ICISMEP

VERIFICAÇÃO DAS ASSINATURAS

Código para verificação: 8F19-C939-DEBF-FBB6

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

JOÃO GABRIEL MIRANDA DE SOUZA (CPF 030.XXX.XXX-74) em 31/10/2025 15:25:44 GMT-03:00
Papel: Parte
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

Para verificar a validade das assinaturas, acesse a Central de Verificação por meio do link:

https://icismep.1doc.com.br/verificacao/8F19-C939-DEBF-FBB6