MUNICÍPIO DE
SANTA CRUZ DO SUL

VIVER AQUI É BOM DEMAIS

ESTUDO TÉCNICO PRELIMINAR

1 INFORMAÇÕES BÁSICAS
2 DEFINIÇÃO E ESPECIFICAÇÃO DA NECESSIDADE
3 AVALIAÇÃO DAS SOLUÇÕES DISPONÍVEIS
3.1 Infraestrutura Local (on-premises)
3.2 Colocation
3.3 Nuvem Privada
3.3.1 Empresas brasileiras provedoras de serviços de Data Center
3.4 Nuvem Pública
3.4.1 Thema Informática
3.4.2 Serpro Multicloud
3.5 Nuvem Híbrida
3.6 Nuvem Comunitária
3.7 Outros serviços semelhantes no mercado
3.8 Modelos de Serviços - IaaS, PaaS e SaaS
3.9 Virtualização
3.10 Recursos disponíveis em ambientes de Virtualização
3.11 Níveis de Data Center
TIER I: Nível 1 - Infraestrutura Básica
TIER II: Nível 2 - Componentes Redundantes
TIER III: Nível 3 - Manutenção Simultânea
TIER IV: Nível 4 - Tolerante a Falhas
3.12 Cloud Backup e Disaster Recovery
4 ESTIMATIVA DAS QUANTIDADES A SEREM CONTRATADAS
4.1 Quantidade de recursos atualmente contratados
4.2 Quantidade de recursos atualmente utilizados no Data Center próprio
4.3 Total de recursos utilizados atualmente
4.4 Solicitação de atualização tecnológica de ambiente do Sistema Integrado de Gestão Municipal/SIGM/GRP
4.5 Acréscimo Estimado de 20%
4.6 Outros recursos necessários de maneira global
4.6.1 Firewall de Próxima Geração (NGFW) Virtualizado em Alta Disponibilidade
4.6.2 Link dedicado de interconexão entre Data Centers (Replicação e DR)
4.6.3 Link de Internet dedicado
4.6.4 Endereços IP públicos dedicados (IPv4)
4.6.5 Treinamento técnico (20 horas) para equipe de TI
4.7 Tabela de quantitativos totais
5 AVALIAÇÃO DE CUSTOS E LEVANTAMENTO DE MERCADO
5.1 Thema Informática
5.2 Serpro Multicloud

5.3 Portais Públicos e Orçamento prévio solicitado às empresas do ramo
6 IDENTIFICAÇÃO DOS RISCOS RELACIONADOS À CONTRATAÇÃO E ESTRATÉGIAS DE MITIGAÇÃO
7 ESCOLHA DA SOLUÇÃO E JUSTIFICATIVA
8 DESCRIÇÃO DOS REQUISITOS DA CONTRATAÇÃO
8.1 Exigência de Certificações
Certificação Tier III (ou equivalente):
O Risco do "Data Center de Papel"
Certificações ISO (ou equivalente):
Fundamentação Legal:
8.2 Localização da Infraestrutura em Território Nacional
9 DESCRIÇÃO DA SOLUÇÃO COMO UM TODO
10 JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO
11 ALINHAMENTO ENTRE A CONTRATAÇÃO E O PLANEJAMENTO
12 RESULTADOS PRETENDIDOS
13 PROVIDÊNCIAS A SEREM ADOTADAS PREVIAMENTE À CELEBRAÇÃO DO CONTRATO
14 CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES
15 POSSÍVEIS IMPACTOS AMBIENTAIS
16 DECLARAÇÃO DE VIABILIDADE

1 INFORMAÇÕES BÁSICAS

- Área Requisitante: Departamento de TI – Secretaria de Administração e Gestão
- Objeto: Contratação de serviço de nuvem (*cloud computing*) para hospedagem de bancos de dados e sistemas críticos de informática da Prefeitura de Santa Cruz do Sul.
- Prazo de Execução: 24 (vinte e quatro) meses, contados a partir da data da assinatura do termo de início dos serviços, prorrogáveis por sucessivos períodos de 12 (doze) meses, respeitada a vigência máxima decenal, conforme art. 105 e seguintes, da Lei nº 14.133, de 1º de abril de 2021.

2 DEFINIÇÃO E ESPECIFICAÇÃO DA NECESSIDADE

A Prefeitura Municipal de Santa Cruz do Sul, assim como qualquer órgão público, depende amplamente da tecnologia da informação para o desempenho

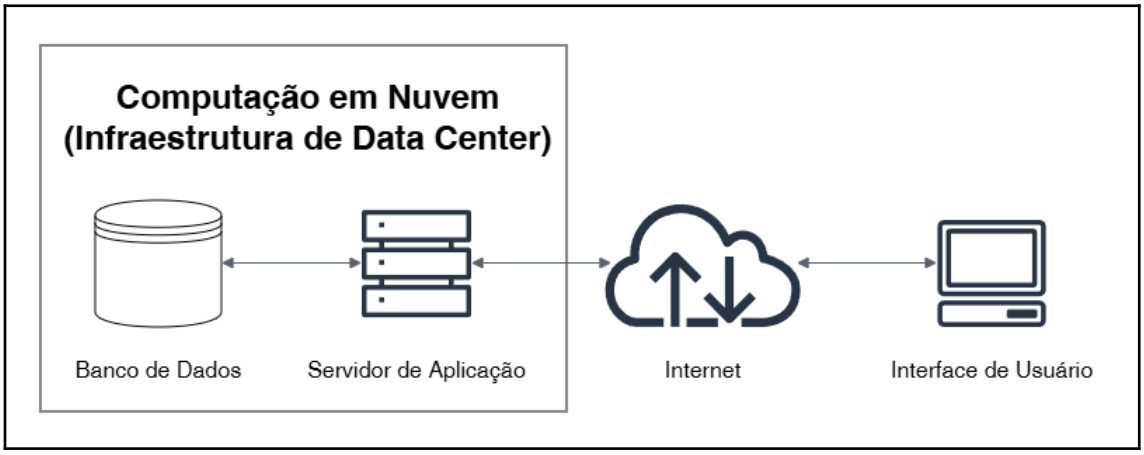
de suas funções administrativas e operacionais. Nesse contexto, o uso de bancos de dados e sistemas informatizados tornou-se um pilar essencial para que o Poder Executivo Municipal ofereça serviços cada vez mais eficientes, acessíveis e transparentes à população.

A transformação digital da administração pública municipal demanda uma infraestrutura tecnológica moderna, escalável e segura, capaz de sustentar os serviços digitais existentes e viabilizar o desenvolvimento de novas soluções. Nesse cenário, a Prefeitura Municipal de Santa Cruz do Sul identifica a necessidade de contratar uma solução de computação em nuvem, com o objetivo de consolidar e evoluir sua estrutura tecnológica, especialmente no que se refere ao Sistema Integrado de Gestão Municipal (SIGM/GRP), atualmente sustentado por um ambiente de nuvem privada contratado em caráter emergencial.

Além da sustentação dos sistemas atualmente em operação, a contratação da nova infraestrutura de nuvem também se mostra necessária para viabilizar a implantação e expansão do processo eletrônico no âmbito da Administração Municipal. A adoção de soluções voltadas à tramitação eletrônica de processos administrativos exige ambiente tecnológico com elevada disponibilidade, segurança, desempenho, capacidade de armazenamento, rotinas de backup, rastreabilidade, controle de acessos e continuidade operacional, uma vez que os documentos e fluxos administrativos passam a depender diretamente da infraestrutura digital para sua criação, tramitação, consulta, guarda e preservação. Dessa forma, a contratação de uma solução de nuvem privada robusta e escalável se torna essencial para a modernização administrativa, redução da tramitação física de documentos, aumento da eficiência dos processos internos e ampliação da transparência e da celeridade na prestação dos serviços públicos.

A Figura 1 ilustra a topologia das camadas básicas que geralmente compõem os sistemas de informática (como o SIGM/GRP) que funcionam e são acessíveis de forma online:

Figura 1 - Topologia básica de uma aplicação web.



A nuvem em operação atualmente hospeda sistemas críticos para o funcionamento da administração municipal, tais como:

- Sistema de Gestão de Recursos Públicos (SIGM/GRP);
- Sistema de Recursos Humanos (ADMRH);
- Sistema de emissão de Nota Fiscal Eletrônica (NFS-e);
- Portais da Transparência e do Servidor público;
- Outros.

Apesar de funcional, o contrato 266/PGM/2024 é temporário, sem respaldo licitatório de longo prazo, o que impõe riscos à continuidade dos serviços e à segurança jurídica da operação. Este contrato contemplava, dentre seus objetos, a contratação do serviço de nuvem privada (Cloud Computing), abrangendo os itens 7, 8, 9 e 10. Todavia, em razão da significativa evolução tecnológica observada nos últimos anos, aliada à elevada complexidade e especificidade técnica inerentes aos serviços de computação em nuvem, a Administração entendeu ser mais adequado promover o desmembramento desse serviço do objeto originalmente contratado, viabilizando sua contratação por meio de procedimento licitatório próprio.

Além dos sistemas atualmente hospedados na nuvem contratada, a Prefeitura ainda mantém, em infraestrutura própria de Data Center instalada no Centro Administrativo 1, outros serviços relevantes, como:

- Site institucional do Município;
- Intranet corporativa;
- Sistema e-SUS;
- Versões de homologação dos sistemas GRP e ADMRH;
- Sistema GEO 360, utilizado para mapeamento e georreferenciamento do cadastro imobiliário (Projeto Mapa da Cidade);
- Serviço de compartilhamento de arquivos;
- Outras soluções de suporte técnico interno.

Esses serviços também deverão ser migrados para a nova infraestrutura

em nuvem, de forma planejada, segura e escalável.

A necessidade dessa migração para uma infraestrutura de nuvem mais robusta se tornou ainda mais evidente após o incidente de segurança cibernética ocorrido em janeiro de 2024, quando um incidente cibernético comprometeu o serviço de compartilhamento de arquivos da Prefeitura, resultando no atraso de diversos trâmites administrativos. O episódio evidenciou fragilidades da infraestrutura local, agravadas pela limitação de investimentos em soluções de segurança, atualização tecnológica e capacitação da equipe técnica do Departamento de TI.

Adicionalmente, as severas consequências das enchentes no Rio Grande do Sul em maio de 2024 evidenciaram a vulnerabilidade de infraestruturas locais diante de desastres naturais e situações de emergência. Nesse contexto, a adoção de soluções de computação em nuvem contribui para a mitigação de riscos operacionais, permitindo que sistemas institucionais e bases de dados críticas permaneçam disponíveis mesmo diante de eventos que possam impactar a infraestrutura tecnológica local da Administração Municipal.

A contratação de uma solução de nuvem permitirá mitigar esses riscos, ao oferecer:

- Maior disponibilidade e tolerância a falhas;
- Observabilidade e monitoramento;
- Escalabilidade elástica, conforme a demanda dos serviços;
- Recuperação de desastres, com backups automatizados e cópias geograficamente redundantes;
- Conformidade com normas de segurança e proteção de dados, como a Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018).

Apesar de já ter desempenhado papel importante no suporte à infraestrutura de tecnologia da informação da Prefeitura de Santa Cruz do Sul, o Data Center local apresenta atualmente diversas limitações técnicas, operacionais e de segurança que comprometem sua capacidade de atender às demandas atuais e futuras da administração pública. Entre os principais fatores que inviabilizam sua continuidade como ambiente para hospedagem de aplicações institucionais críticas, destacam-se:

a) Risco elevado à segurança da informação

O ataque cibernético ocorrido em janeiro de 2024 evidenciou fragilidades na estrutura de segurança do Data Center local. O incidente gerou indisponibilidade de diversos serviços essenciais e expôs a dificuldade da Prefeitura em responder rapidamente a eventos de segurança de grande escala. A inexistência de soluções consolidadas de proteção, como antivírus

nos computadores dos usuários, monitoramento contínuo de ameaças, autenticação multifator e controle de acesso centralizado, torna o ambiente local mais suscetível a novos ataques e falhas.

b) Falta de equipe especializada

A administração municipal não conta, atualmente, com uma equipe técnica dedicada exclusivamente à gestão de infraestrutura de Data Center. Os profissionais da área de TI são da área de análise de sistemas (4 funcionários) e técnicos em informática (3 funcionários), os quais auxiliam nas configurações e manutenção do Data Center local, porém os seus cargos não possuem atribuições e responsabilidades sobre o tema, além de não possuírem qualificações específicas em segurança da informação, administração de servidores, redes avançadas e alta disponibilidade. Essa lacuna compromete a capacidade da Prefeitura de manter, de forma segura e eficiente, um ambiente tecnológico complexo como um Data Center local.

c) Infraestrutura física obsoleta e limitada

Grande parte do parque tecnológico utilizado no Data Center é composto por equipamentos com mais de cinco anos de uso, que não contam com garantias ativas, peças de reposição em pronta entrega, ou mesmo capacidade para suportar atualizações de firmware e software. Além disso, a infraestrutura de energia, refrigeração e conectividade não segue os padrões recomendados para ambientes críticos, como controle de acesso físico, redundância de fontes de energia, controle ambiental automatizado e links de internet com *failover* automático. Não há gerador de energia como fonte alternativa.

d) Baixa escalabilidade

A ampliação da infraestrutura física local para suportar novas aplicações e maior volume de dados requer investimentos elevados em hardware, licenças, espaço físico e energia elétrica. A escalabilidade em Data Centers próprios é lenta, dispendiosa e inflexível. Em contraste, a computação em nuvem oferece escalabilidade elástica, com provisionamento imediato de recursos conforme a demanda, reduzindo o tempo e o custo da expansão.

e) Ausência de continuidade operacional garantida

A Prefeitura não dispõe de um plano de contingência formalizado e testado para desastres envolvendo o Data Center local. Não há replicação geográfica dos dados, nem ambiente alternativo pronto para assumir os serviços em caso de falhas críticas. Essa limitação coloca em risco a continuidade dos serviços públicos digitais em situações emergenciais, como falhas de energia, desastres naturais ou ataques cibernéticos.

Diante do exposto, observa-se a importância da contratação de serviços

de nuvem para que a Prefeitura consiga manter sua governança e prestar serviços mais eficientes e rápidos para sua população.

3 AVALIAÇÃO DAS SOLUÇÕES DISPONÍVEIS

Para fazer este levantamento e avaliar as soluções disponíveis no mercado, foram analisadas licitações com Data de Abertura a partir de 01/01/2025, e os respectivos contratos, das Prefeituras do Rio Grande do Sul, disponíveis no Sistema Licitacon. Também foram consideradas pesquisas no buscador Google e Portal Nacional de Contratações Públicas do Governo Federal.

Um desafio ao pesquisar processos licitatórios relacionados a serviços de computação em nuvem (cloud computing) é a grande variedade de soluções de tecnologia que também são hospedadas em ambientes de nuvem e disponibilizadas por meio da internet, como, por exemplo, sistemas de alarme e videomonitoramento, PABX e telefonia IP, correio eletrônico (e-mail), soluções de colaboração e compartilhamento de arquivos, assim como diferentes tipos de sistemas informatizados, como plataformas de gestão e comércio eletrônico.

3.1 Infraestrutura Local (on-premises)

Até pouco tempo atrás, a maioria das empresas optavam por investir em infraestrutura própria de Data Center para atender às suas necessidades de tecnologia, utilizando computadores e servidores locais para armazenamento de arquivos, acesso e processamento dos dados e instalação de sistemas de informática. Esse modelo, conhecido como on-premises, oferece controle total sobre os recursos computacionais, sendo a escolha predominante para empresas que ainda priorizam segurança e customização.

A criação e implantação de um Data Center próprio implica total controle sobre a infraestrutura, desde o planejamento físico e lógico, aquisição e manutenção de hardware, licenciamento e atualização de softwares, até a implementação de segurança, sistemas de energia e refrigeração. Toda essa infraestrutura se localiza fisicamente nas instalações da organização, e sua gestão é feita internamente pela equipe de TI. Ou seja, essa opção demanda investimentos iniciais elevados em ativos físicos (CAPEX), além de custos operacionais recorrentes (OPEX) para manutenção, pessoal qualificado e atualização tecnológica.

No entanto, com o aumento das demandas por recursos computacionais, como maior capacidade de processamento, armazenamento

escalável e conectividade contínua, muitas organizações passaram a enfrentar desafios relacionados à segurança, aos custos de aquisição e manutenção, e limitações para expandir a infraestrutura rapidamente.

3.2 Colocation

A modalidade de colocation é uma solução estratégica para empresas e órgãos públicos que precisam de um ambiente seguro e altamente disponível para seus próprios servidores e equipamentos de TI. No modelo de colocation, o cliente aluga espaço físico dentro de um Data Center de terceiros, mas mantém total controle sobre seus servidores, sistemas e configurações. O provedor do Data Center, por sua vez, oferece toda a infraestrutura necessária, como:

- Energia elétrica redundante (geradores e nobreaks para evitar quedas de energia).
- Climatização controlada para manter a temperatura ideal dos servidores.
- Segurança física e lógica, com monitoramento 24/7 e controle de acesso rigoroso.
- Alta conectividade, garantindo acesso a múltiplos provedores de internet e links dedicados.

Principais desafios na Contratação do Colocation:

- Custos operacionais: Apesar de reduzir despesas com infraestrutura própria, ainda há custos com deslocamento, manutenção, licenciamento e atualização dos equipamentos.
- Gestão remota: A empresa precisa de equipe técnica capacitada para gerenciar servidores a distância ou contratar serviços extras do provedor.
- Contrato e SLAs: É fundamental analisar os Acordos de Nível de Serviço (SLA), garantindo disponibilidade, suporte técnico e segurança adequados.
- Escalabilidade: Diferente da nuvem, expandir ou substituir servidores exige planejamento e aquisição de novos equipamentos físicos.
- Localização do Data Center: A proximidade do município pode ser um fator importante para minimizar a latência na transferência de dados e facilitar o acesso técnico quando necessário.

O colocation pode ser considerado como alternativa para quem deseja manter controle sobre os seus servidores sem os altos custos de manter um Data Center próprio, mas exige planejamento para garantir que a solução seja viável e eficiente para as necessidades do negócio.

Um exemplo de contratação de colocation pode ser analisado no Contrato 3041/2024 do SEMAE - Serviço Municipal de Água e Esgotos de São Leopoldo. Emergencialmente, devido às enchentes ocorridas em maio de 2024 no Rio Grande do Sul, o órgão teve seu Data Center afetado e seus equipamentos foram transferidos para a infraestrutura de outra empresa contratada, na cidade de Sapiranga.

3.3 Nuvem Privada

A nuvem privada surgiu como uma alternativa estratégica para organizações que desejavam terceirizar sua infraestrutura completa de Data Center e servidores físicos, mas sem renunciar ao controle e aos altos padrões de segurança, característicos de uma infraestrutura própria. Nesse modelo, a instituição contrata um provedor especializado para gerenciar e hospedar uma infraestrutura dedicada exclusivamente às suas operações. Isso permite que a organização aproveite a flexibilidade e a escalabilidade dos serviços terceirizados, ao mesmo tempo que garante conformidade com requisitos específicos de segurança e reduz os custos e desafios associados à manutenção de uma infraestrutura interna.

A nuvem privada aproveita as tecnologias de computação em nuvem, como virtualização, elasticidade, provisionamento e automação, para oferecer maior flexibilidade e eficiência, mantendo a exclusividade do ambiente para um único cliente. Este modelo também costuma ser implementado por organizações que precisam atender às demandas internas do próprio negócio, como provedores de internet ou empresas de telecomunicações, e transformam esse investimento em serviços personalizados para seus clientes corporativos, otimizando recursos e ampliando sua capacidade de atender diferentes necessidades. Essa abordagem permite aos clientes escalar recursos de forma dinâmica e atender a demandas específicas sem a necessidade de adquirir e configurar novos equipamentos manualmente.

Este é o formato atualmente contratado pela Prefeitura junto à empresa Ávato/Brasil Tecpar, desde o Pregão Presencial 030/2019.

3.3.1 Empresas brasileiras provedoras de serviços de Data Center

Ao realizar pesquisas no Sistema Licitacon e no buscador Google, utilizando palavras-chave como “cloud”, “cloud computing”, “private cloud”, “serviços de nuvem”, “nuvem privada”, “nuvem para órgãos públicos”, “Data Center” e “IaaS”, é possível identificar diversas empresas brasileiras que atuam nesse segmento, as quais ofertam serviços de infraestrutura em nuvem e hospedagem de sistemas, por exemplo:

- 2Cloud
  - https://www.2cloud.com.br/solucoes/2cloud-sp3/
- Absam
  - https://absam.io/servidor-dedicado
- Adentro Tecnologia
  - https://www.adentro.com.br/nuvem-privada/
- Algar Telecom
  - https://loja.algartelecom.com.br/empresas/cloudplus/
- Ascenty
  - https://ascenty.com/data-centers/
- Ávato/Brasil TecPar
  - https://www.avato.com.br/cloudedatacenter
- Equinix
  - https://www.equinix.com.br/solutions/cloud-services
- EVEO
  - https://www.eveo.com.br/nuvem-privada/
- HostDime
  - https://www.hostdime.com.br/produtos/cloud-server/
- Nnumbers
  - https://nnumbers.com.br/produtos/one-cloud/
- Open Data Center
  - https://www.opendatacenter.com.br/open-cloud-platform
- Optidata
  - https://www.optidata.com/br/
- Platon
  - https://platon.com.br/platon-cloud
- Sercloud
  - https://sercloud.com.br/solucoes/cloud-computing
- Stefanini
  - https://stefanini.com/pt/solucoes/cloud/
- Teccloud
  - https://cloudprivada.teccloud.com/
- TIVIT
  - https://cloud.tivit.com/
- Under
  - https://under.com.br/datacenter/
- Unifique
  - https://unifique.com.br/para-empresas/cloud
- Vivo / Telefônica Brasil
  - https://vivo.com.br/para-empresas/produtos-e-servicos/digitais/cloud/cloud-plus
- WIH
  - https://wih.com.br/servico/cloud
- Winov
  - https://winov.com.br/

-

Além da presença de diversos fornecedores atuando no segmento, observa-se também a existência de entidades representativas voltadas ao desenvolvimento e à organização do setor de infraestrutura digital no Brasil. Entre elas destacam-se a Associação Brasileira de Data Centers (ABDC), que reúne empresas e especialistas ligados à implantação e operação de Data Centers, e a Abracloud, associação que congrega provedores de serviços de computação em nuvem e infraestrutura digital. Essas entidades atuam na promoção de boas práticas, no desenvolvimento técnico do setor e na interlocução com órgãos públicos e reguladores, contribuindo para o fortalecimento do mercado de data centers e de serviços de nuvem no país.

3.4 Nuvem Pública

A nuvem pública é uma infraestrutura de computação gerenciada por grandes empresas de tecnologia (big techs), como Amazon Web Services (AWS), Google Cloud, Microsoft Azure, Oracle Cloud Infrastructures (OCI), IBM Cloud e Huawei Cloud, e disponibilizada para uso compartilhado por múltiplas organizações em escala global. Esse modelo é amplamente utilizado devido à sua escalabilidade (Hyperscaler), flexibilidade e custo reduzido de implantação, pois elimina a necessidade de investimento inicial em infraestrutura própria. Por ser acessada pela internet, a nuvem pública permite que organizações ampliem ou reduzam rapidamente os recursos de acordo com as demandas, pagando apenas pelo que utilizam.

No entanto, esse tipo de nuvem pode apresentar desafios relacionados ao controle e gestão dos recursos financeiros, especialmente no planejamento orçamentário. A flexibilidade para escalar rapidamente os serviços é uma vantagem, mas, sem o devido acompanhamento, pode gerar custos inesperados ou acima do previsto. Tem sido comum que organizações enfrentam dificuldades em gerenciar os gastos associados à nuvem pública, especialmente em situações de uso intenso ou configurações inadequadas. Para minimizar esses riscos, é necessário não apenas estimar os custos com precisão, mas também monitorar continuamente o consumo e aplicar políticas claras de governança financeira sobre os recursos de TI.

Nos portais institucionais destas big techs, são disponibilizadas ferramentas de calculadora de custos que auxiliam profissionais de TI e engenheiros de software/infraestrutura a estimar e orçar os valores associados à contratação e alocação de serviços e recursos de computação em nuvem, por exemplo:

AWS - https://calculator.aws/

Google Cloud - https://cloud.google.com/products/calculator

Microsoft Azure - https://azure.microsoft.com/pt-br/pricing/calculator/

Oracle Cloud - https://www.oracle.com/br/cloud/costestimator.html

Huawei- https://www.huaweicloud.com/intl/pt-br/pricing/calculator.html#/ecs

IBM - https://www.ibm.com/br-pt/products/cloud/cloud-calculator

No entanto, o uso eficaz dessas calculadoras exige habilidades avançadas sobre arquiteturas e projetos de software, alinhadas ao catálogo de serviços ofertados. Além disso, é importante considerar que as funcionalidades e custos dos serviços podem variar significativamente entre os diferentes provedores, aumentando a complexidade do processo de planejamento.

Dentre os recursos alocados em um serviço de nuvem pública, podem ser citados: capacidade de processamento (CPUs e GPUs virtuais), memória RAM, armazenamento (discos virtuais, armazenamento em blocos, ou soluções como objetos e arquivos), tráfego de rede (entrada e saída de dados), bancos de dados gerenciados, balanceadores de carga, serviços de monitoramento e segurança, além de ferramentas para automação e backup.

Os custos relacionados a estes recursos podem ser variáveis, dependendo do uso real ou de demandas específicas. Por exemplo, o tráfego de saída de dados pode gerar cobranças adicionais em períodos de maior acesso, enquanto o armazenamento pode ter custos flutuantes se forem utilizados recursos como cópias de segurança (snapshots e backups) ou armazenamento de alta performance. Além disso, serviços complementares, como monitoramento, segurança avançada ou banco de dados gerenciado, podem ser ativados conforme necessário, impactando o orçamento final. Por isso, é fundamental monitorar continuamente o consumo e ajustar a configuração para evitar surpresas financeiras.

Essas empresas também operam com programas estruturados de parcerias, revendas e afiliados, permitindo que outras empresas atuem no mercado como revendedores e prestadores de serviços especializados. Esses parceiros, também chamados de “cloud brokers”, são habilitados para comercializar os serviços de nuvem dessas grandes plataformas, oferecendo suporte técnico, consultoria e personalização de soluções para atender às necessidades específicas de diferentes clientes. Esse modelo de parceria amplia o alcance dos serviços de nuvem, ao mesmo tempo que possibilita às empresas locais agregar valor por meio de atendimento mais próximo e suporte técnico especializado, facilitando a adoção da tecnologia por organizações de diversos tamanhos e setores.

3.4.1 Thema Informática

A empresa Thema Informática, atualmente responsável pelo suporte e manutenção do sistema de gestão (GRP) utilizado pela Prefeitura, também se

apresenta como revendedora de serviços da Oracle Cloud Infrastructure, oferecendo uma solução própria de hospedagem em nuvem para o referido sistema.

https://www.thema.inf.br/thema-cloud/

Sob a ótica técnica, observa-se como principal vantagem desse modelo o fato de que a própria desenvolvedora do sistema detém conhecimento aprofundado sobre a arquitetura, requisitos e dependências da aplicação, o que tende a reduzir riscos na implantação, otimizar a configuração do ambiente e agilizar a resolução de incidentes. Esse fator pode contribuir significativamente para a continuidade operacional e estabilidade do sistema, especialmente em cenários de migração para nuvem.

Por outro lado, esse modelo pode implicar em limitações relacionadas à flexibilidade e autonomia da Administração Pública sobre o ambiente tecnológico. A solução ofertada tende a ser dedicada exclusivamente à hospedagem do sistema GRP, podendo dificultar ou restringir a implantação ou integração de outras soluções próprias do Município ou de terceiros. Tal característica pode resultar em maior dependência tecnológica do fornecedor, reduzindo a capacidade de evolução da arquitetura de TI de forma integrada.

Adicionalmente, para viabilizar atividades técnicas por parte da equipe interna do Departamento de TI, como consultas diretas ao banco de dados ou integrações com sistemas internos (como a intranet), pode ser necessária a implementação de mecanismos de conectividade segura, como VPN ou conexão do tipo LAN-to-LAN. Essa necessidade adiciona complexidade operacional e exige cuidados adicionais com segurança da informação.

Dessa forma, embora a solução apresente ganhos relevantes em termos de especialização e suporte, deve-se ponderar os impactos relacionados à flexibilidade, integração e governança do ambiente de tecnologia.

3.4.2 Serpro Multicloud

O Serviço Federal de Processamento de Dados (Serpro) disponibiliza, entre suas soluções, o serviço de Multicloud, no qual atua como intermediador (cloud broker) na contratação e gestão de serviços de nuvem pública junto a diversos provedores de mercado.

https://loja.serpro.gov.br/product/multicloud

Nesse modelo, o Serpro realiza atividades de apoio técnico e consultivo, auxiliando na análise das demandas do órgão contratante e na definição da arquitetura mais adequada, podendo inclusive indicar o provedor de nuvem mais apropriado para cada cenário. Importante destacar que, conforme

entendimento obtido junto ao próprio Serpro, sua atuação não envolve necessariamente a execução direta da implantação das soluções, mas sim o direcionamento técnico e a governança do ambiente contratado.

Como vantagem, destaca-se a possibilidade de contratação por meio de dispensa de licitação, nos termos do artigo 75, Inciso IX, da Lei 14.133 de 01 de abril de 2021, o que pode conferir maior agilidade ao processo. Além disso, o Multicloud tende a oferecer maior flexibilidade, permitindo a adoção de diferentes provedores e a expansão do uso da nuvem para outras demandas da Prefeitura, além do sistema GRP, promovendo uma arquitetura mais aberta e escalável.

Por outro lado, a adoção desse modelo pode resultar em aumento da complexidade na gestão contratual e operacional, uma vez que envolve múltiplos atores: o Serpro como broker, o provedor de nuvem e a empresa Thema Informática como desenvolvedora do sistema. Nesse contexto, o Departamento de TI do Município passa a exercer um papel mais focado na coordenação e interlocução entre as partes, especialmente em atividades como implantação, atualização e suporte do sistema GRP.

Adicionalmente, a separação entre as responsabilidades de cada entidade pode demandar maior maturidade em governança de TI, definição clara de acordos de nível de serviço (SLAs) e processos bem estabelecidos de gestão de incidentes e mudanças.

Assim, o Serpro Multicloud apresenta-se como uma alternativa com maior flexibilidade e potencial de escalabilidade, porém com aumento proporcional na complexidade de gestão e necessidade de coordenação entre diferentes prestadores de serviço.

3.5 Nuvem Híbrida

A nuvem híbrida combina os benefícios das nuvens pública e privada, permitindo que as organizações utilizem cada ambiente de forma estratégica. Nesse modelo, dados e aplicações sensíveis podem ser mantidos em uma nuvem privada, enquanto cargas de processamento menos críticas ou de alto volume são gerenciadas em uma nuvem pública, otimizando custos e desempenho.

Essa abordagem oferece flexibilidade para escalar rapidamente os recursos e maior resiliência, facilitando a continuidade dos negócios em caso de falhas. Contudo, a integração entre os ambientes público e privado exige ferramentas avançadas e equipes capacitadas, além de poder apresentar desafios relacionados à sincronização e ao gerenciamento unificado das

operações.

Um exemplo de projeto de nuvem híbrida pode ser analisado no Contrato 44/2025 do Tribunal de Contas do Estado (TCE) do RS, onde foi contratada a empresa Oracle para prestação de serviços de processamento de banco de dados em nuvem privada, com contingência em nuvem pública. A nuvem privada é baseada na solução “Oracle Exadata Cloud at Customer”, na qual servidores físicos da contratada são instalados no Data Center do próprio TCE, enquanto que a nuvem pública serve como uma solução de redundância em caso de desastres ou incidentes cibernéticos.

3.6 Nuvem Comunitária

Nuvem comunitária é um modelo de serviço de computação em nuvem menos comum, mas que atende a necessidades específicas. Nesse modelo, a infraestrutura de nuvem é compartilhada por um grupo de organizações com objetivos ou requisitos semelhantes, como políticas de segurança, conformidade regulatória ou interesses de mercado.

Essa configuração é geralmente implementada e gerenciada por uma ou mais organizações participantes, ou por um terceiro que atua como provedor. A nuvem comunitária é particularmente útil para setores como governo, saúde ou pesquisa, onde as organizações podem compartilhar custos e recursos de infraestrutura enquanto mantêm controle sobre aspectos críticos, como privacidade e segurança.

3.7 Outros serviços semelhantes no mercado

Um dos serviços mais comuns é a hospedagem de sites, fornecida por diversos provedores que disponibilizam infraestrutura para suportar websites de pequeno, médio e grande porte. Esse serviço pode ser oferecido em diferentes modalidades, como compartilhada ou dedicada, conforme o porte e a demanda do site.

A modalidade VPS (Virtual Private Server) é uma solução de hospedagem em que o cliente tem acesso a um servidor virtualizado, com recursos dedicados e maior controle sobre o sistema operacional e os softwares instalados. Esse modelo é indicado para empresas que precisam de mais flexibilidade e personalização em relação à hospedagem, mas não requerem a infraestrutura de um servidor físico completo.

Além disso, alguns provedores oferecem servidores dedicados, ou bare metal, que são servidores físicos alugados para uso exclusivo de uma organização, sem o compartilhamento de recursos com outros clientes. Esse modelo é ideal para empresas que necessitam de grande capacidade de processamento e armazenamento, com total controle sobre a configuração do servidor.

3.8 Modelos de Serviços - IaaS, PaaS e SaaS

Os modelos de serviço em computação em nuvem oferecem diferentes níveis de abstração e responsabilidades compartilhadas entre o provedor e o cliente. Cada modelo atende a necessidades específicas, permitindo que organizações escolham a abordagem mais alinhada aos seus objetivos.

- **Infraestrutura como Serviço (IaaS)**: Fornece recursos básicos, como servidores virtuais, armazenamento e redes, permitindo maior controle e flexibilidade para o cliente configurar e gerenciar sua infraestrutura, ideal para ambientes complexos ou personalizados.
- **Plataforma como Serviço (PaaS)**: Fornece uma camada adicional de abstração, oferecendo ferramentas de desenvolvimento e gerenciamento de aplicações, o que reduz a necessidade de gerenciar a infraestrutura subjacente, sendo adequado para equipes focadas na criação de software.
- **Software como Serviço (SaaS)**: Entrega aplicações prontas para uso, acessíveis pela internet, como e-mail, hospedagem de sites, armazenamento e compartilhamento de arquivos, ou até sistemas completos de gestão e E-commerce, eliminando a necessidade de instalação ou manutenção, o que o torna especialmente relevante para usuários finais e empresas buscando soluções práticas e rápidas de implementar.

A seguir, uma tabela que ilustra o compartilhamento da responsabilidade pelo gerenciamento de ambientes de computação em nuvem:

Legenda:

Gerenciado pelo Cliente/Contratante
Gerenciado pelo Fornecedor/Provedor

Tabela:

		NUVEM PÚBLICA		
Infraestrutura Local (on premises)	NUVEM PRIVADA	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
Aplicações	Aplicações	Aplicações	Aplicações	Aplicações

Dados	Dados	Dados	Dados	Dados
Bibliotecas e Frameworks	Bibliotecas e Frameworks	Bibliotecas e Frameworks	Bibliotecas e Frameworks	Bibliotecas e Frameworks
Sistema Operacional	Sistema Operacional	Sistema Operacional	Sistema Operacional	Sistema Operacional
Virtualização	Virtualização	Virtualização	Virtualização	Virtualização
Rede e Conectividade	Rede e Conectividade	Rede e Conectividade	Rede e Conectividade	Rede e Conectividade
Infraestrutura e Servidores	Infraestrutura e Servidores	Infraestrutura e Servidores	Infraestrutura e Servidores	Infraestrutura e Servidores

3.9 Virtualização

A virtualização é a base tecnológica que possibilita os serviços de computação em nuvem, permitindo a criação de múltiplas instâncias virtuais a partir de um único recurso físico, como servidores, armazenamento ou redes. Por meio de tecnologias como hipervisores e containers, a virtualização abstrai os recursos físicos, permitindo que eles sejam compartilhados entre diversos usuários ou aplicações de maneira eficiente e segura. Essa abordagem possibilita a alocação dinâmica de recursos, escalabilidade sob demanda e isolamento de ambientes, garantindo que diferentes cargas de processamento possam ser executadas simultaneamente sem interferências.

No contexto da nuvem, a virtualização traz benefícios significativos, como redução de custos operacionais e maior flexibilidade na oferta e gestão de infraestrutura. Provedores de serviços de nuvem utilizam a virtualização para oferecer aos clientes uma ampla gama de opções, desde máquinas virtuais (VMs) configuráveis no modelo IaaS até ambientes altamente otimizados para desenvolvimento no modelo PaaS. Além disso, a virtualização é fundamental para garantir a resiliência e disponibilidade dos serviços, permitindo o balanceamento de carga entre servidores físicos em caso de falhas ou manutenção, com impacto mínimo para os usuários.

3.10 Recursos disponíveis em ambientes de Virtualização

Os principais recursos disponíveis em um ambiente de virtualização são:

- **Máquinas Virtuais (VMs - Virtual Machines)**: É o elemento principal em um ambiente de virtualização, onde o sistema operacional e os aplicativos funcionam de forma independente, integrando e consumindo os outros recursos virtuais alocados.

- **Processamento (CPU - Central Processing Unit)**: Alocação de núcleos de processadores para máquinas virtuais. Gerenciamento da utilização de CPU entre várias VMs para otimizar o desempenho.
- **Memória (RAM - Random Access Memory)**: Distribuição e gerenciamento de memória física entre as VMs. Técnicas como memory ballooning e deduplicação para melhorar a eficiência. Limites e reservas para garantir desempenho consistente.
- **Armazenamento (Storage/Virtual Disks)**: Arquivos que simulam discos rígidos para as VMs. Gerenciamento de volumes e snapshots para backups e restaurações. Provisionamento: Aloca espaço sob demanda para economizar armazenamento.
- **Rede (Network)**: Criação de switches e adaptadores virtuais para conectar as VMs, VLANs para segmentação de tráfego, segurança (firewall virtual), balanceamento de carga e monitoramento de tráfego.

3.11 Níveis de Data Center

A Certificação TIER é uma classificação mundial usada para mensurar o nível da infraestrutura de um Data Center e indica o quanto ele está preparado para lidar com problemas. Foi criado pelo Uptime Institute em meados da década de 1990 para medir e avaliar o quanto a infraestrutura de um Data Center pode atender às demandas de uma organização, classificando a instalação de acordo com 4 níveis, sendo 1 o pior nível e 4 o melhor nível de desempenho.

Quanto a redundância de recursos, os principais componentes avaliados em um Data Center são:

- Fontes de Energia;
- Sistemas de Refrigeração;
- Conexões de Rede;
- Servidores para Armazenamento e Redundância;
- Controles de Acesso Físico;
- Sistemas de Deteção de Incêndio.

TIER I: Nível 1 - Infraestrutura Básica

- Características: Componentes não redundantes; Uma única fonte de energia e refrigeração; Sem cópia de segurança (backup) ou conexões de rede alternativas para sistemas críticos.
- Redundância: Nenhuma.
- Disponibilidade: 99,671% (até 28,8 horas de inatividade por ano).

TIER II: Nível 2 - Componentes Redundantes

- Cumpre todos os requisitos Tier I;

- Características: Componentes críticos redundantes (UPS, geradores, sistemas de refrigeração); Caminho único de distribuição para energia e refrigeração.
- Redundância: N+1 para componentes essenciais (um caminho ativo e um de reserva).
- Disponibilidade: 99,741% (até 22 horas de inatividade por ano).

TIER III: Nível 3 - Manutenção Simultânea

- Cumpre todos os requisitos Tier I e Tier II;
- Características: Permite manutenção sem interrupção dos serviços; Múltiplos caminhos de distribuição para energia e refrigeração, mas apenas um caminho ativo; Todos os componentes são redundantes (N+1).
- Redundância: N+1 para todos os sistemas críticos.
- Disponibilidade: 99,982% (até 1,6 horas de inatividade por ano).

TIER IV: Nível 4 - Tolerante a Falhas

- Cumpre todos os requisitos Tier I, Tier II e Tier III;
- Características: Infraestrutura projetada para suportar falhas de componentes ou sistemas sem afetar as operações; Múltiplos caminhos independentes para energia e refrigeração, todos ativos simultaneamente; Redundância completa em todas as partes (2N+1).
- Redundância: 2N+1, com total tolerância a falhas.
- Disponibilidade: 99,995% (até 26,3 minutos de inatividade por ano).

Embora a classificação TIER III seja frequentemente associada a elevados níveis de disponibilidade da infraestrutura física do Data Center, tal parâmetro deve ser compreendido como referência técnica da robustez, redundância e manutenção simultânea do ambiente físico, não se confundindo automaticamente com o SLA contratual da solução de nuvem a ser entregue à Administração.

A disponibilidade efetiva dos serviços contratados depende também de outros componentes, como plataforma de virtualização, conectividade, firewall, sistemas operacionais, carga de processamento, manutenções programadas e atuação da contratada. Assim, para fins de execução contratual, fiscalização e aplicação de penalidades, será adotado SLA mínimo de 99,9% de disponibilidade mensal da infraestrutura de nuvem contratada, sem prejuízo da exigência de que o Data Center utilizado possua classificação equivalente ou superior ao nível TIER III como requisito mínimo de qualificação técnica.

3.12 Cloud Backup e Disaster Recovery

A gestão de processos de Backup (cópias de segurança) é fundamental para garantir a resiliência cibernética de uma organização, pois garantem a

proteção e a disponibilidade contínua de dados e sistemas críticos, prevenindo perdas irreparáveis causadas por falhas técnicas, ataques cibernéticos ou desastres naturais, e assegurando a continuidade das operações organizacionais.

A Recuperação de Desastres (Disaster Recovery - DR) está diretamente ligada à gestão de Backup, pois ambos os processos têm como objetivo principal assegurar a continuidade das operações em caso de eventos adversos que comprometam a integridade dos dados e sistemas. Enquanto o Backup se concentra na criação e armazenamento de cópias de segurança dos dados, o DR envolve o planejamento e a execução de estratégias para restaurar rapidamente esses dados e sistemas após um incidente, minimizando o tempo de inatividade e os impactos sobre uma organização. Uma estratégia de DR eficaz depende de um sistema de Backup robusto e bem gerenciado, garantindo que as informações necessárias estejam disponíveis para uma recuperação ágil e segura.

Ainda relacionado à Recuperação de Desastres, é importante destacar os conceitos de **RTO** (Recovery Time Objective) e **RPO** (Recovery Point Objective). O RTO define o tempo máximo aceitável de indisponibilidade de um sistema ou serviço após uma falha, estabelecendo a agilidade necessária para que a operação seja restabelecida e os impactos ao negócio sejam minimizados. Já o RPO está ligado à perda de dados tolerável, determinando qual o intervalo máximo entre os backups ou réplicas, de forma a limitar a quantidade de informações que pode ser comprometida em um incidente. Esses indicadores, quando bem definidos, fornecem uma base sólida para o planejamento de estratégias de continuidade e segurança da informação.

Processos de backup na nuvem e em ambiente local apresentam diferenças significativas em termos de custos, escalabilidade e gerenciamento. O backup em ambiente local, utilizando servidores ou dispositivos próprios (como NAS-Network Attached Storage), requer um investimento inicial elevado em hardware, além de custos contínuos com manutenção, energia, pessoal técnico e espaço físico. Por outro lado, oferece controle total sobre os dados e pode ser preferível em cenários que exigem acesso rápido e local. Em contraste, o backup na nuvem elimina a necessidade de infraestrutura local, oferecendo um modelo de pagamento conforme o uso, maior escalabilidade e acesso remoto aos dados. Contudo, depende da conectividade com a internet e do provedor de serviços para a gestão e recuperação dos dados, o que pode implicar considerações adicionais de segurança e conformidade regulatória.

Backup realizado em um ambiente integrado ao serviço de nuvem já contratado (e preferencialmente em armazenamento distinto) é fundamental para fortalecer a segurança dos dados da Prefeitura. Este modelo minimiza a necessidade de transferências frequentes de grandes volumes de dados pela

internet, reduzindo a exposição a riscos como interceptações e ataques cibernéticos durante a transmissão. Além disso, a integração direta com o ambiente de nuvem permite aplicar políticas de segurança consistentes, como criptografia de dados em repouso e em trânsito, controle de acesso baseado em funções, e monitoramento contínuo de ameaças. Assim, a Prefeitura garante que seus dados estejam protegidos dentro de um ecossistema confiável, aumentando a resiliência contra perdas e garantindo a conformidade com as regulamentações de segurança da informação.

A adoção de soluções de Backup na Nuvem (Cloud Backup) tem se mostrado uma prática crescente entre organizações públicas e privadas, devido à sua eficiência e segurança no armazenamento de dados críticos. Diversas empresas brasileiras que atuam no mercado de Cloud também oferecem soluções de Backup na Nuvem. Tecnicamente, os dados de produção e os dados de Backup (dados em repouso) diferem em suas técnicas de armazenamento e gestão. Os dados de produção, que são utilizados ativamente pelas aplicações e usuários, exigem armazenamento de alto desempenho e baixa latência, frequentemente implementado em sistemas de armazenamento primário como SSDs ou conjuntos de discos de alta velocidade, otimizados para acesso rápido e contínuo.

Em contrapartida, os dados de backup, que permanecem em repouso até serem necessários para recuperação, são geralmente armazenados em soluções de armazenamento secundário ou terciário, como fitas magnéticas, discos rígidos de maior capacidade e menor custo, ou armazenamento em nuvem frio (cold storage). Essas soluções priorizam a capacidade e a durabilidade sobre o desempenho, visando reduzir custos e garantir a retenção segura de dados por longos períodos, com acessos esporádicos e planejados.

4 ESTIMATIVA DAS QUANTIDADES A SEREM CONTRATADAS

A estimativa das quantidades a serem contratadas será feita com base no somatório dos recursos atualmente contratados, com os recursos utilizados nos servidores virtualizados e hospedados no Data Center próprio, instalado no primeiro andar do Centro Administrativo 1 da Prefeitura.

4.1 Quantidade de recursos atualmente contratados

Abaixo, o quadro apresenta os quantitativos utilizados atualmente pela Prefeitura, de acordo com o Boletim de Medição do mês de fevereiro de 2025

(anexo 1) e E-mail com o detalhamento técnico de recursos alocados em cada VM (anexo 2), referente ao último contrato **266/PGM/2024**:

Item	Quantidade
vCPU	64
Memória RAM	200 GB
Armazenamento/Storage	8.278 GB
Backup	10.000GB

4.2 Quantidade de recursos atualmente utilizados no Data Center próprio

Nos quantitativos acima não estão sendo consideradas as aplicações que estão hospedadas no Data Center próprio da Prefeitura, é preciso mensurar os recursos que serão necessários em uma futura migração dos serviços atualmente instalados no Data Center local. Servidores de Aplicação patrimônio números 108323,108324 e 108643, solução de virtualização baseada em VMWare.

Abaixo, segue os quantitativos utilizados no **Data Center local**, conforme informação (anexo 3) do Departamento de TI:

Item	Quantidade
vCPU	127
Memória RAM	384 GB
Armazenamento/Storage	10318 GB

4.3 Total de recursos utilizados atualmente

Desta maneira, a previsão de seguintes quantitativo total mensal utilizado de cada recurso, somando a nuvem contratada com Data Center local:

Item	vCPU	Memória	Storage
Quantidade	64 + 127 191	200 + 384 584 GB	8.278 + 10.318 18.596 GB

4.4 Solicitação de atualização tecnológica de ambiente do Sistema Integrado de Gestão Municipal/SIGM/GRP

Além disso, a empresa que presta serviços de suporte e manutenção do sistema GRP – THEMA Informática – enviou para a Prefeitura uma solicitação de atualização de ambiente tecnológico em fevereiro de 2025, ou seja, uma solicitação para que a Prefeitura disponibilize mais recursos (vCPU, Memória e Disco) para rodar o sistema de gestão (anexo 4, página 4). Conforme a empresa THEMA, esta atualização se justifica para: melhorar o desempenho e a disponibilidade dos serviços; aumentar a capacidade de processamento e armazenamento; suportar o crescimento futuro; garantir a escalabilidade; necessidade de atualizar os sistemas operacionais dos servidores virtuais; poder instalar novos patches de segurança nos servidores, para melhorar a segurança dos servidores, a qualidade dos serviços e a capacidade de atender às demandas da Prefeitura.

Resumindo:

- 3 servidores "masters" com: Processador: 8 núcleos; Memória RAM: 8 GB; Disco rígido: 100 GB;
- 5 servidores "workers" com: Processador: 16 núcleos; Memória RAM: 64 GB; Disco rígido: 800GB;
- Total: Processador: 104 núcleos; Memória RAM: 344 GB; Disco rígido: 4.300 GB;

Desta maneira, é necessário somar os novos quantitativos de cada recurso. Isto é, somar apenas a diferença entre os recursos já utilizados pela aplicação SIGM/GRP (sem considerar o banco de dados) na nuvem atualmente contratada (VM “vm-pmscr-grp” no anexo 2) e a nova solicitação da empresa Thema (anexo 4).

A diferença necessária é:

Item	**A) Quantidade Atual (anexo 2)**	**B) Quantidade Solicitada (anexo 4)**	**Diferença (B-A)**
vCPU	24	104	80
Memória	80 GB	344 GB	264 GB

Armazenamento	555 GB	4.300 GB	3.745 GB

Assim, a diferença da tabela acima também deve ser somada ao total de recursos, resultando nos seguintes quantitativos:

Item	**vCPU**	**Memória**	**Armazenamento**
Quantidade	191 + 80 =271	584 + 264 =848 GB	18.596 + 3.745 =22.341 GB

4.5 Acréscimo Estimado de 20%

A tabela acima representa as quantidades atualmente utilizadas de recursos computacionais combinada com a quantidade de recursos solicitada pela THEMA Informática. No entanto, para garantir a continuidade e a escalabilidade dos serviços públicos digitais, é necessário prever uma margem de crescimento. Por isso, **estima-se um acréscimo de, no mínimo, 20%** sobre esses valores, considerando a expansão de sistemas e dados existentes, a possível implantação de novos serviços eletrônicos e o aumento natural de uso por parte de servidores e cidadãos.

Essa previsão é fundamental para assegurar que a infraestrutura contratada possa acompanhar a evolução tecnológica e as necessidades do município. Sendo assim, a tabela de estimativa necessária dos recursos citados é a seguinte:

Item	vCPU	Memória	Armazenamento
Quantidade Mensal Estimada	271 + ~20% 325	848 + ~20% 1.017 GB	22341 + ~20% 26.800 GB

Observação: A contratação deverá ser no modelo IaaS, permitindo alocação sob demanda, com cobrança mensal proporcional ao uso efetivo de cada recurso no mês de referência, evitando a ociosidade de recursos. Em razão disso, os quantitativos acima servem como estimativa para a pesquisa de preços e dimensionamento da infraestrutura mínima esperada. A prefeitura poderá utilizar menos ou mais, dentro dos quantitativos acima citados, conforme necessidade.

4.6 Outros recursos necessários de maneira global

Além dos recursos computacionais básicos como vCPU, memória e armazenamento, é essencial que a solução de nuvem privada contratada contemple também componentes adicionais de infraestrutura e segurança que assegurem o pleno funcionamento, garantindo tanto a conectividade e disponibilidade de acesso quanto a proteção dos dados e a continuidade dos serviços digitais da Prefeitura. Esses recursos complementares — como firewall, links de conexão e endereços IP públicos — são fundamentais para garantir desempenho, resiliência, integridade e governança sobre os ativos de TI.

4.6.1 Firewall de Próxima Geração (NGFW) Virtualizado em Alta Disponibilidade

Para garantir a proteção integral da infraestrutura em nuvem, faz-se necessária a implementação de uma solução de Firewall de Próxima Geração (Next-Generation Firewall – NGFW) dedicada e virtualizada. Ao contrário de soluções restritas apenas à camada de aplicação web, o NGFW atua na inspeção profunda de tráfego nas Camadas de 3 a 7 da rede (baseado no modelo OSI), integrando recursos avançados de segurança como Prevenção contra Intrusões (IPS/IDS), Filtro de Conteúdo/URL, Antivírus de Rede, Inspeção de Tráfego Criptografado (SSL/TLS) e gestão de redes virtuais privadas (VPNs IPsec e SSL). Essa abordagem abrangente assegura a proteção perimetral não apenas das aplicações web (como portais de atendimento, sistemas de protocolo e RH), mas de todos os servidores, bancos de dados e serviços corporativos hospedados no ambiente.

Com o objetivo de eliminar pontos únicos de falha e assegurar a continuidade dos serviços públicos essenciais, a solução de NGFW deve ser provisionada obrigatoriamente em arquitetura de Alta Disponibilidade (HA), operando através de um par redundante de instâncias virtuais (Ativo/Passivo ou Ativo/Ativo) com sincronização contínua de estado das conexões (stateful failover). Para conferir máxima resiliência ao ambiente, as instâncias virtuais do NGFW devem ser alocadas em nós de processamento físicos (hosts) distintos dentro da infraestrutura do Data Center, garantindo que eventuais falhas de hardware não ocasionem a indisponibilidade do perímetro de segurança ou a interrupção dos acessos aos sistemas municipais.

4.6.2 Link dedicado de interconexão entre Data Centers (Replicação e DR)

A contratação de conexão dedicada e privada de alta velocidade de, no mínimo, 100 Mbps (Full Duplex, 1:1) entre os Data Centers primário (Produção) e secundário (Contingência/DR) é indispensável para viabilizar a replicação contínua de dados, a sincronização de bases de dados e o envio automatizado

de backups. Essa interconexão dedicada garante o cumprimento rigoroso dos objetivos de Ponto de Recuperação (Recovery Point Objective - RPO) e Tempo de Recuperação (Recovery Time Objective - RTO) estabelecidos pela Administração Pública, assegurando a continuidade dos negócios e a rápida restauração dos serviços em cenários de desastre. O circuito deverá operar com volume de tráfego de dados ilimitado (sem franquia ou bilhetagem de consumo), suporte a jumbo frames e garantia de latência máxima reduzida (máximo de 40ms) para evitar degradação nas rotinas de sincronismo.

Um link dedicado de 100 Mbps assegura a transferência contínua de até 1 Terabyte (TB) de dados a cada 24 horas de processamento. Trata-se de uma vazão tecnicamente dimensionada para garantir o fluxo ininterrupto de réplicas e backups entre os Data Centers de Produção e Contingência, viabilizando a restauração tempestiva do ambiente e a integridade das bases de dados do Município.

4.6.3 Link de Internet dedicado

A conectividade dedicada com a Internet é o pilar de acesso externo a toda a infraestrutura em nuvem, sendo responsável por suportar as conexões simultâneas de servidores públicos, cidadãos, empresas, sistemas integrados e acessos remotos via VPN. Para assegurar a disponibilidade, a baixa latência e a previsibilidade de desempenho dos serviços digitais municipais (como emissão de NFS-e, portais de atendimento, RH e protocolo), estabelece-se a exigência de link de Internet dedicado de, no mínimo, 100 Mbps (Full Duplex, garantia de banda 1:1), com endereçamento IP público fixo e volume de tráfego de dados ilimitado (sem franquia de download/upload ou cobrança por dados trafegados). A solução deve contar com mitigação nativa contra ataques de negação de serviço (DDoS) e monitoramento contínuo de disponibilidade.

A adoção de um link dedicado de 100 Mbps provê a largura de banda adequada para suportar os picos de tráfego de acesso aos sistemas web (como portais de serviços, RH, contabilidade e protocolo), garantindo a navegação estável dos cidadãos e servidores públicos, assim como conexões via VPN.

4.6.4 Endereços IP públicos dedicados (IPv4)

A disponibilização de endereços IP públicos dedicados é necessária para permitir a publicação e operação segura dos diversos serviços hospedados no ambiente de nuvem, incluindo portais institucionais, sistemas corporativos, integrações externas e demais aplicações que demandem acesso público. A utilização de endereços dedicados possibilita maior flexibilidade na configuração de DNS, certificados digitais, políticas de segurança e mecanismos de monitoramento e auditoria.

4.6.5 Treinamento técnico (20 horas) para equipe de TI

A adoção de uma nova infraestrutura de computação em nuvem exige a capacitação da equipe técnica responsável pela gestão e fiscalização

contratual. A ausência de capacitação específica da equipe técnica acarreta riscos severos de governança, tais como: subaproveitamento dos recursos contratados, vulnerabilidades de segurança por má configuração (ex: exposição de dados), estouro orçamentário por falta de dimensionamento/monitoramento de custos (FinOps) e dependência excessiva (vendor lock-in) do suporte técnico do fornecedor.

A carga horária estimada em 20 (vinte) horas foi dimensionada para cobrir o escopo prático essencial do ambiente customizado que será entregue, sem comprometer excessivamente a rotina operacional da equipe. O treinamento será direcionado a um grupo de no mínimo 05 (cinco) servidores/colaboradores, abrangendo:

- Papéis de Gestão e Fiscalização Contratual: foco em relatórios de uso, controle de custos e acompanhamento de SLA.

- Papéis de Administração e Operação de TI: foco em provisionamento de recursos, rotinas de backup, segurança e monitoramento do ambiente.

O treinamento deverá ser ministrado na modalidade remota (síncrona/ao vivo), por meio de instrutor qualificado, em formato de turma exclusiva (in-company). O conteúdo deve ser predominantemente prático (hands-on), abordando a solução contratada, assim como a plataforma de atendimento e gestão dos recursos. A opção pela modalidade remota reduz custos logísticos (diárias e passagens), otimiza o uso do orçamento e permite a gravação das sessões para consultas futuras pela equipe técnica.

4.7 Tabela de quantitativos totais

Deste modo, a tabela dos totais de quantitativo dos itens que fazem parte da solução como um todo da contratação de IaaS, a ser publicada no termo de referência, é a seguinte:

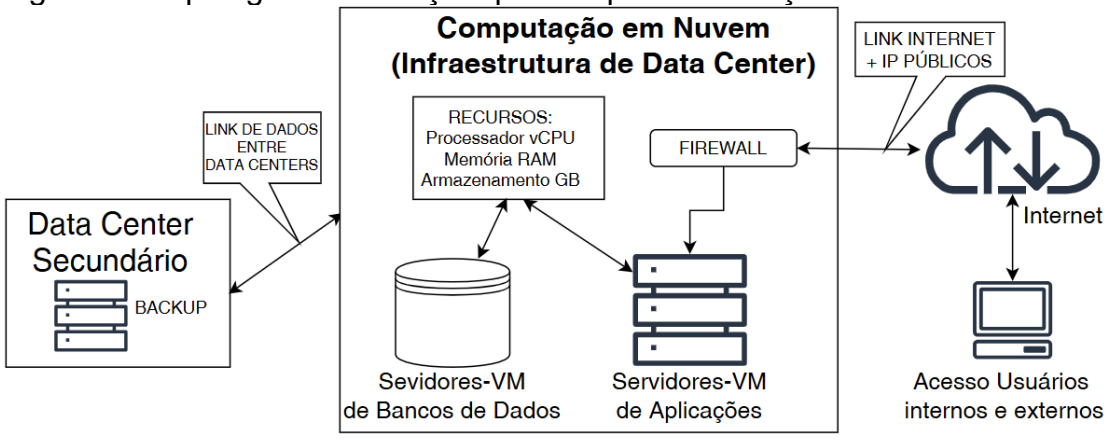
ITEM	DESCRIÇÃO	Unidade de medida	Quantidade Estimada
1	vCPU	Unidade	325
2	Memória RAM (GB)	GB	1017
3	Armazenamento/Storage (produção) em GB	GB	26800
4	Armazenamento/Storage para Backup em GB	GB	26800
5	Firewall de Próxima Geração	Unidade	1

	(NGFW) Virtualizado em Alta Disponibilidade		
6	Link dedicado entre Data Centers (100 Mbps Full Duplex)	Unidade	1
7	Link de Internet dedicado (100 Mbps Full Duplex)	Unidade	1
8	Endereços IP públicos dedicados (IPv4)	Unidade	8
9	Treinamento 20h para equipe TI	Unidade	1

A quantidade estimada de 8 IPs públicos dedicados se justifica pelo fato de haver as seguintes aplicações que necessitam de acesso externo através dos IPs públicos dedicados:

1. GRP Produção
2. ADMRH Produção
3. GEO 360/Mapa da Cidade
4. Site Institucional
5. GRP Homologação
6. ADMRH Homologação
7. Intranet
8. Reserva de 20%.

Figura 2 - Topologia dos serviços que compõem a solução:



Os itens 5 (Firewall), 6 (Link dedicado entre Data Centers) e 7 (Link dedicado de Internet) serão contratados de forma fixa, com fornecimento contínuo e permanente durante a vigência do contrato, enquanto que os itens 1 (vCPU), 2 (Memória RAM-GB), 3 (Armazenamento/Storage produção GB), 4 (Armazenamento/Storage para Backup-GB) e 8 (Endereços IP públicos dedicados-IPv4) serão ativados e fornecidos por demanda, de acordo com a

necessidade da contratante. Por fim, o item 9 (Treinamento 20h) deverá ocorrer em oportunidade única dentro dos 30 (trinta) dias corridos previstos para a Implantação dos Serviços.

5 AVALIAÇÃO DE CUSTOS E LEVANTAMENTO DE MERCADO

Assim como citado anteriormente, é inviável realizar uma comparação direta entre a implantação de uma infraestrutura on premises com a contratação de serviços em nuvem. A Prefeitura atualmente não dispõe de equipe técnica especializada para projetar, dimensionar, implantar e manter adequadamente uma infraestrutura própria de Data Center (on premises), que atenda plenamente às normas técnicas recomendadas. Essa limitação dificulta a correta avaliação das reais necessidades de hardware, bem como a aplicação das melhores práticas de mercado e o cumprimento das normas técnicas recomendadas para garantir segurança, disponibilidade e desempenho. Nesse contexto, a contratação de serviços em nuvem é uma alternativa viável, pois transfere ao provedor a responsabilidade pela operação da infraestrutura, assegurando conformidade técnica e permitindo que a equipe interna concentre esforços em atividades operacionais e de gestão assim como no uso estratégico dos sistemas de informação.

Com base no levantamento de mercado, descrito no item 3 AVALIAÇÃO DAS SOLUÇÕES DISPONÍVEIS, a avaliação de custos foi realizada da seguinte maneira:

5.1 Thema Informática

A empresa Thema Informática Ltda., atual prestadora dos serviços de suporte, manutenção e evolução do Sistema Integrado de Gestão Municipal (GRP) utilizado pela Prefeitura Municipal de Santa Cruz do Sul, também oferece solução de hospedagem em nuvem pública baseada na plataforma Oracle Cloud Infrastructure (OCI), especificamente dimensionada para execução dos sistemas sob sua responsabilidade.

Como principal vantagem desta alternativa, destaca-se o amplo conhecimento técnico da empresa acerca da arquitetura, requisitos de desempenho, segurança, disponibilidade e banco de dados dos sistemas GRP, reduzindo potenciais riscos relacionados à implantação, configuração e operação do ambiente. Além disso, a centralização da infraestrutura e da aplicação sob um mesmo fornecedor pode simplificar os processos de suporte

e diagnóstico de incidentes.

Por outro lado, a contratação da solução de hospedagem vinculada ao fornecedor do sistema pode acarretar maior dependência tecnológica e operacional em relação a um único fornecedor (vendor lock-in), reduzindo a flexibilidade para futuras migrações, integrações ou substituições de serviços. Também foram identificados riscos relacionados à eventual variação de custos decorrentes de componentes contratados em moeda estrangeira ou indexados ao mercado internacional.

Outro aspecto considerado pela Administração refere-se à necessidade de manutenção do acesso da equipe técnica do Departamento de TI aos bancos de dados Oracle utilizados pelos sistemas corporativos, para fins de consulta, integração entre sistemas, geração de relatórios, auditorias, desenvolvimento de soluções complementares e demais atividades inerentes à gestão tecnológica do Município.

Para subsidiar a análise de viabilidade econômica da solução, foram realizadas consultas a contratos administrativos de objetos semelhantes disponíveis no Portal Licitacon-RS, incluindo contratações realizadas pelos Municípios de Caxias do Sul, Lajeado, Passo Fundo, Não-Me-Toque, Santo Antônio da Patrulha e Montenegro. Verificou-se que os valores contratados apresentam variações significativas em função de fatores como porte populacional do município, quantidade de usuários, volume de dados processados, recursos computacionais contratados e escopo dos serviços disponibilizados.

Município	Contrato	Valor Mensal R$
Passo Fundo	2025/579	93.997,65
Caxias do Sul	2024/1000	81.947,56
Lajeado	2023/227	75.047,23
Montenegro	2023/212	35.000,00
Santo Antônio da Patrulha	2024/202	23.000,00
Não-me-toque	2025/158	15.000,00

No âmbito desta pesquisa de mercado, a empresa apresentou proposta comercial no valor mensal de R$ 68.436,44, compatível com valores praticados pela empresa com outros clientes. Registra-se que esta contratação somente poderá ocorrer somente mediante análise jurídica quanto à adequação da

modalidade a ser adotada pela Administração, como por exemplo um novo instrumento contratual específico ou por meio de aditamento ao contrato já existente de suporte e manutenção.

Cabe destacar que a solução ofertada está voltada exclusivamente à hospedagem do Sistema Integrado de Gestão Municipal (GRP) e seus componentes correlatos, não contemplando outros sistemas ou aplicações mantidos pela Prefeitura. Isto é, esta contratação não permitiria a expansão e futura migração dos sistemas e recursos instalados atualmente no Data Center local “on premises” da Prefeitura.

Por outro lado, a proposta prevê a disponibilização de três ambientes distintos, compreendendo um ambiente de produção, um ambiente de homologação destinado à realização de testes e validações, e um ambiente de replicação para fins de contingência, isto é, para recuperação dos serviços em caso de falha ou indisponibilidade do ambiente principal. Tal característica agrega valor à solução ao proporcionar maior segurança operacional, suporte ao processo de atualização dos sistemas e melhoria na estratégia de continuidade dos serviços.

5.2 Serpro Multicloud

Considerando a possibilidade de contratação direta com fundamento no artigo 75, inciso IX, da Lei nº 14.133/2021, foram realizadas tratativas com o Serviço Federal de Processamento de Dados (Serpro) para avaliação da solução Serpro Multicloud como alternativa para hospedagem dos sistemas corporativos da Prefeitura.

Em razão do Sistema Integrado de Gestão Municipal (GRP) ser desenvolvido em linguagem Java e utilizar banco de dados Oracle, constatou-se, em análise preliminar, a viabilidade técnica de contratar a nuvem OCI (Oracle Cloud Infrastructure). Em um segundo momento, a solução Multicloud também possibilitaria a contratação de mais serviços de nuvem pública para atender a diferentes demandas e projetos futuros da Administração, como por exemplo a migração dos serviços que hoje estão instalados no Data Center local.

Para obtenção da proposta comercial do Serpro Multicloud, foi necessário o preenchimento de planilha técnica contendo informações detalhadas sobre a infraestrutura pretendida, incluindo recursos computacionais, armazenamento, banco de dados, tráfego de rede e demais componentes utilizados para estimativa de consumo. Em razão desta complexidade, foram listados inicialmente apenas os recursos necessários para implantação do Sistema Integrado de Gestão Municipal (GRP) em ambiente de

produção. Sendo assim, foi estimado um consumo de 37.821,05 unidades de CSB, resultado em um valor total de R$ 66.943,26. Considerando todos os itens abaixo da proposta, que são faturados por demanda, o orçamento mensal pode chegar ao total de R$ 108.495,79:

- CSB — Cloud Service Brokerage: corretagem de serviços em nuvem e operação da plataforma multinuvem;
- CSM — Cloud Service Management: suporte continuado à infraestrutura de nuvem;
- CGPS — Cloud Generic Professional Service: consultoria técnica para atividades correlatas.

Também foram consultadas e analisadas as contratações realizadas por outros órgãos públicos do Estado do Rio Grande do Sul (RS), incluindo o Tribunal de Justiça, a Defensoria Pública e a Prefeitura Municipal de Bagé, verificando-se a utilização da plataforma em cenários semelhantes de infraestrutura tecnológica. Verificou-se que o modelo comercial adotado pelo Serpro utiliza a métrica denominada Cloud Services Brokerage (CSB), unidade própria utilizada para consolidação e faturamento dos recursos consumidos. A conversão entre os recursos efetivamente utilizados (processamento, memória, armazenamento, tráfego de rede e demais serviços) e a unidade CSB demanda análise técnica detalhada, tornando mais complexa a estimativa prévia dos custos e o acompanhamento financeiro da contratação.

A unidade CSB apresenta um valor unitário tabelado de R$ 1,77. Isto é, o mesmo valor unitário é fixado para todos os clientes, porém a quantidade de CSB varia conforme o levantamento das demandas e necessidades apresentadas pelo órgão contratante.

Abaixo, a comparação da unidade CSB entre os contratos analisados:

Cliente	Contrato	Quantidade estimada CSB
Tribunal de Justiça	14/2025	50.138.613,77
Defensoria Pública	63/2023	342.619,84
Prefeitura de Bagé	150/2025	1.313,55

Por se tratar de solução baseada em nuvem pública, parte dos custos poderá estar sujeita a fatores externos de mercado, incluindo eventuais variações de preços praticados pelos provedores internacionais de infraestrutura em nuvem, o que pode impactar a previsibilidade financeira de

longo prazo.

Também foram identificados desafios relacionados à governança operacional da solução, especialmente quanto à definição de responsabilidades entre os diferentes atores envolvidos, incluindo o Serpro, o provedor de nuvem, a empresa Thema responsável pelo sistema de gestão municipal e a equipe técnica da Prefeitura. Essa característica pode exigir mecanismos adicionais de coordenação, monitoramento e gestão contratual para garantir a adequada prestação dos serviços.

5.3 Portais Públicos e Orçamento prévio solicitado às empresas do ramo

Foram realizadas consultas aos portais públicos (PNCP e Licitacon/TCE-RS) para levantamento de valores e contratos vigentes, relacionados aos itens do objeto. Foram utilizadas as seguintes palavras-chave: data center, nuvem, vcpu, vram, hospedagem, cloud, colocation, storage, VCPU, backup, link, curso, treinamento.

Também foi solicitado orçamento prévio, acompanhado da minuta do Termo de Referência, às empresas listadas no item 3.3 Nuvem Privada, que foram encontradas em buscadores e portais de compras públicas na Internet.

Conforme a Planilha Orçamentária em anexo, e considerando a ativação de todos os recursos previstos sob demanda, a estimativa do valor total da contratação é R$ 2.127.538,20.

Abaixo, os valores estimados de cada serviço:

Cód. Sistema	Cód. CATSER	Item	Descrição	Unidade medida	Quantidade Mensal	Valor Unitário Mensal R$	Valor Total Mensal
53683	26050	1	vCPU	Unidade	325	44,13	14.342,25
53684	26050	2	Memória RAM (GB)	GB	1017	28,11	28.587,87
53685	26050	3	Armazenamento/Storage (produção) em GB	GB	26800	0,84	22.512,00
53686	26050	4	Armazenamento/Storage para Backup em GB	GB	26800	0,46	12.328,00
53682	27014	5	Firewall de Próxima Geração (NGFW) Virtualizado em Alta Disponibilidade	Unidade	1	5.589,79	5.589,79
64314	26476	6	Link dedicado entre Data Centers (100 Mbps Full Duplex)	Unidade	1	2.105,48	2.105,48

64315	26484	7	Link de Internet dedicado (100 Mbps Full Duplex)	Unidade	1	2.149,78	2.149,78
64316	27014	8	Endereços IP públicos dedicados (IPv4)	Unidade	8	56,73	453,84
11900	3840	9	Treinamento 20h para equipe TI	Unidade	1	13.881,96	N/D
VALOR TOTAL MENSAL - MÊS 1 COM TREINAMENTO							R$ 101.950,97
VALOR TOTAL MENSAL - MESES 2 A 24							R$ 88.069,01
VALOR TOTAL GLOBAL							R$ 2.127.538,20

6 IDENTIFICAÇÃO DOS RISCOS RELACIONADOS À CONTRATAÇÃO E ESTRATÉGIAS DE MITIGAÇÃO

Para avaliar os riscos em contratações de serviços de nuvem privada, foram identificados os principais eventos que podem afetar o contrato e gerar desequilíbrio econômico-financeiro:

a) Interrupção dos serviços da nuvem: Instabilidade ou queda nos servidores contratados.

- Impacto Potencial: Indisponibilidade dos sistemas críticos;
- Estratégia de Mitigação: Monitoramento contínuo dos serviços pela equipe de TI e/ou da contratada. Acompanhamento do SLA. Aplicação de penalidades em caso de descumprimento contratual.

b) Divergência de responsabilidades entre fornecedores: Possibilidade de transferência de responsabilidade entre a empresa fornecedora da infraestrutura em nuvem e a empresa Thema, responsável pela manutenção e suporte ao Sistema de Gestão (GRP) instalado, dificultando a identificação e resolução de incidentes.

Impacto Potencial: Atraso na solução de falhas, indisponibilidade prolongada dos sistemas e prejuízo à continuidade dos serviços.

Estratégia de Mitigação: Definição contratual de responsabilidades, exigência de cooperação técnica entre os fornecedores, disponibilização de logs e evidências técnicas, e coordenação das atividades pela equipe de TI da Prefeitura.

c) Dependência da empresa Thema para migração e implantação:

Necessidade de atuação da empresa Thema para instalação, configuração, homologação e entrada em produção dos sistemas corporativos na infraestrutura de nuvem contratada.

Impacto Potencial: Atrasos na implantação da solução, prorrogação de cronogramas e postergação do início da operação dos serviços.

Estratégia de Mitigação: Planejamento antecipado das atividades de migração, definição de cronograma integrado entre as partes envolvidas, acompanhamento pela equipe de TI e formalização das responsabilidades de cada participante do processo.

d) Crescimento das demandas além da infraestrutura contratada: Aumento do uso dos recursos da nuvem por novos sistemas ou usuários.

- Impacto Potencial: Falta de recursos computacionais, degradação de desempenho;
- Estratégia de Mitigação: Uso do modelo IaaS sob demanda. Planejamento de ampliação dentro da margem legal (até 25%) e previsão de novo processo licitatório, se necessário.

e) Falhas na comunicação entre a nuvem e a rede da Prefeitura: Problemas na integração entre a infraestrutura de nuvem e os acessos locais.

- Impacto Potencial: Lentidão ou falha no acesso remoto aos sistemas;
- Estratégia de Mitigação: Monitoramento da conectividade e da latência. Acompanhamento do link dedicado e dos IPs públicos. Intervenções técnicas com o fornecedor sempre que necessário;

f) Risco de perda de dados ou falha no backup: Problemas na execução ou recuperação dos backups.

- Impacto Potencial: Perda de dados críticos ou dificuldade de restauração após falha;
- Estratégia de Mitigação: Fiscalização periódica da rotina de backup contratada. Testes de restauração. Auditoria e registro das evidências de backup;

g) Incidentes de segurança cibernética: Acesso não autorizado, vazamento de dados, ataques DDoS ou ransomware.

- Impacto Potencial: Comprometimento da integridade ou sigilo de informações públicas e pessoais;
- Estratégia de Mitigação: Verificação contínua das medidas de segurança (firewall, autenticação, criptografia, antivírus, etc.). Acompanhamento

dos relatórios de vulnerabilidade. Previsão contratual de resposta a incidentes;

h) Descumprimento de cláusulas contratuais pelo fornecedor: Entregas abaixo do previsto em termos de disponibilidade, suporte ou segurança.

- Impacto Potencial: Prejuízos operacionais e administrativos à Prefeitura;
- Estratégia de Mitigação: Acompanhamento do contrato por servidor designado como fiscal. Aplicação das penalidades previstas. Registros formais de não conformidades;

i) Atraso no suporte técnico ou falha na resolução de chamados: Respostas lentas ou superficiais da equipe do fornecedor, especialmente em situações críticas.

- Impacto Potencial: Prolongamento de falhas, paralisação dos serviços ao cidadão;
- Estratégia de Mitigação: Cobrança do SLA de atendimento e resolução. Definição de níveis de criticidade dos chamados. Verificação de canais de atendimento 24x7.

j) Dificuldade para migrar dados ao fim do contrato (portabilidade): Resistência do fornecedor ou problemas técnicos ao entregar os dados da Prefeitura.

- Impacto Potencial: Dificuldade de continuidade em novo ambiente. Perda ou aprisionamento de dados. Garantia contratual de portabilidade dos dados em formato aberto e com documentação;
- Estratégia de Mitigação: Execução assistida da migração no fim do contrato, com cronograma;

7 ESCOLHA DA SOLUÇÃO E JUSTIFICATIVA

Após análise técnica das alternativas disponíveis para a sustentação e evolução da infraestrutura de TI da Prefeitura Municipal de Santa Cruz do Sul, definiu-se pela contratação de uma solução de computação em nuvem privada, no modelo IaaS (Infraestrutura como Serviço), por apresentar o melhor equilíbrio entre desempenho, segurança, escalabilidade, gestão e conformidade com as necessidades da Administração Pública.

Considerando a natureza dinâmica dos serviços de infraestrutura em nuvem e a necessidade de garantir escalabilidade, elasticidade e otimização de custos, justifica-se a adoção de um modelo de contratação com quantitativos estimados, sem fixação de teto ou piso de utilização, e com pagamento

vinculado exclusivamente aos recursos efetivamente consumidos durante a vigência contratual. Além disso, nos casos em que houver aumento ou redução de recursos no decorrer do mês, o cálculo da remuneração deverá ser realizado de forma proporcional ao número de dias em que os recursos permaneceram alocados, tomando como base a data da efetiva alocação (no caso de aumento de recursos) ou a data de solicitação (no caso de diminuição de recursos).

Esse modelo é o mais adequado para atender à realidade da Administração Pública, especialmente diante de cenários que demandam constante adaptação da infraestrutura, como:

- Atualizações tecnológicas de sistemas estratégicos, que podem alterar os requisitos de CPU, memória e armazenamento de forma imprevisível ao longo do tempo;
- Adoção de novos sistemas ou funcionalidades por diferentes órgãos e setores da Prefeitura, que exigem alocação pontual de recursos computacionais;
- Crescimento progressivo de uso, diante do aumento do volume de dados, usuários e serviços digitalizados;
- Capacidade de resposta rápida a picos de demanda, evitando a necessidade de superdimensionamento prévio e ociosidade de recursos.

Dessa forma, a contratação com base em estimativas garante previsibilidade orçamentária, controle do gasto público, e eficiência operacional, ao mesmo tempo em que preserva a flexibilidade necessária para a evolução tecnológica da infraestrutura municipal.

Também foram avaliadas as seguintes opções, com os respectivos motivos de descarte:

a) Infraestrutura própria (Data Center local – on premises): descartada em função de limitações estruturais, ausência de mecanismos avançados de segurança, carência de pessoal técnico especializado para operação em regime 24/7 e histórico recente de indisponibilidades causadas por ataques cibernéticos e fenômenos climáticos extremos. A manutenção dessa alternativa representaria um elevado risco à continuidade dos serviços públicos digitais.

b) Colocation (hospedagem física de servidores da Prefeitura em Data Center de terceiros): embora ofereça benefícios em termos de segurança física e infraestrutura elétrica e climática, esta modalidade ainda exigiria aquisição e manutenção de hardware próprio, além da responsabilização da Prefeitura por toda a camada de virtualização, sistema operacional e gerenciamento da infraestrutura. Tal cenário demandaria equipe técnica interna mais robusta, o que atualmente não está disponível.

c) Nuvem pública (AWS, Azure, Google Cloud, Oracle, etc.): embora tecnicamente viável, apresentou obstáculos quanto à contratação por meio de licitação pública, cobrança em moeda estrangeira, complexidade na precificação, ausência de faturas nacionais com validade fiscal e exigências de conformidade quanto à localização dos dados em território nacional, além de limitação quanto à personalização de políticas de segurança.

d) Nuvem híbrida: apresenta complexidade excessiva de implantação e gerenciamento, além de exigir integração constante entre ambientes distintos. Demandaria investimentos iniciais e operacionais elevados, além de maturidade técnica não compatível com a estrutura atual da Prefeitura.

A escolha pela nuvem privada no modelo IaaS justifica-se tecnicamente por reunir as seguintes vantagens:

- Alojamento em Data Center profissional, certificado, com controle de acesso, climatização, redundância elétrica e conectividade de alto desempenho;
- Entrega sob demanda de recursos computacionais (vCPUs, memória, storage), com escalabilidade e elasticidade conforme o consumo real, permitindo ajuste dinâmico de capacidade conforme a evolução dos serviços municipais;
- Controle da infraestrutura lógica (virtualização), possibilitando que a equipe de TI da Prefeitura realize a gestão de máquinas virtuais, redes, firewalls e ambientes de homologação/produção, sem dependência de gestão física;
- Segurança da informação baseada em padrões de mercado, com backup automatizado, criptografia, segmentação de rede, autenticação e possibilidade de auditoria de acessos;
- Atendimento a requisitos da Lei Geral de Proteção de Dados (LGPD), com possibilidade de armazenamento integral dos dados em território nacional;
- Melhor custo-benefício frente às demais alternativas, considerando o tempo de implantação, risco operacional, disponibilidade, suporte técnico e modelo de cobrança por uso.

Além disso, o modelo IaaS facilita a atuação dos nossos fornecedores de software (como a THEMA Informática), que poderão realizar a implantação e manutenção dos sistemas diretamente no ambiente contratado, sem a necessidade de intermediação técnica por parte da Prefeitura, o que garante maior agilidade na entrega dos serviços.

Portanto, a contratação de nuvem privada sob demanda, no modelo IaaS, representa a solução tecnicamente mais adequada, eficiente, segura e sustentável para garantir a continuidade e expansão dos serviços digitais

prestados pelo Município de Santa Cruz do Sul.

8 DESCRIÇÃO DOS REQUISITOS DA CONTRATAÇÃO

A solução de computação em nuvem privada a ser contratada deverá contínua, segura, escalável e gerenciável, às demandas atuais e futuras da Prefeitura Municipal de Santa Cruz do Sul. O Contrato deverá ser por demanda com previsão de quantidades estimadas e pagamento por consumo efetivo.

A contratação visa garantir a hospedagem de sistemas críticos e serviços digitais como:

- Sistema Integrado de Gestão de Recursos Públicos (GRP);
- Sistema de Administração de Recursos Humanos (ADMRH);
- Portal do Servidor;
- Portal da Transparência;
- Site institucional da Prefeitura;
- Intranet;
- Ambientes de homologação;
- Sistema GEO 360;
- PEC/e-SUS;
- Outras soluções que venham a ser desenvolvidas ou implementadas.

Dessa forma, os requisitos mínimos da solução contratada incluem:

a) Infraestrutura sob demanda (IaaS):

- Disponibilização de recursos computacionais virtualizados (CPU, memória, armazenamento e rede) sob demanda, conforme necessidade da Prefeitura.
- Possibilidade de redimensionamento dos recursos com agilidade, de forma escalável e conforme consumo real.

b) Alta disponibilidade e redundância:

- SLA mínimo de 99,9% de disponibilidade mensal, com previsão de descontos ou penalidades em caso de descumprimento.
- Infraestrutura hospedada em Data Centers certificados, preferencialmente com padrões internacionais (como TIER III, ou superior, ou alternativamente a empresa deverá apresentar outra documentação que comprove o atendimento aos controles objetivos da respectiva norma/certificação).

- Redundância de energia, conectividade e sistemas críticos, com tolerância a falhas.

c) Segurança da informação:

- Proteção contra ataques cibernéticos com ferramentas de segurança como firewall, IDS/IPS, antivírus corporativo e criptografia de dados.
- Proteção contra ataques de negação de serviço (DDoS): A solução contratada deverá incluir mecanismos automáticos e escaláveis de mitigação de ataques DDoS, com capacidade de detecção, contenção e resposta em tempo real. O fornecedor deverá garantir a continuidade do serviço mesmo em situações de ataques volumétricos, assegurando alta disponibilidade dos sistemas da Prefeitura.
- Monitoramento contínuo da infraestrutura com alertas em tempo real.
- Autenticação segura, com suporte a autenticação multifator (MFA).
- Acesso à nuvem através de IPs públicos fixos, IPv4, os quais precisam ser dedicados e exclusivos, devidamente registrados em nome do fornecedor, para garantir segurança e estabilidade.
- Conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e demais legislações aplicáveis à administração pública.
- Certificações ISO 27001, 27017 e 27018 (ou alternativamente a empresa deverá apresentar outra documentação que comprove o atendimento aos controles objetivos da respectiva norma/certificação).

d) Suporte técnico e gestão:

- Suporte técnico 24x7, com atendimento em português, e canais de contato disponíveis por telefone, e-mail e portal de chamados, sem custo adicional.
- Portal de gerenciamento com acesso administrativo para a equipe de TI da Prefeitura, com visualização e monitoramento em tempo real dos recursos alocados.

e) Migração e interoperabilidade:

- Suporte à migração dos dados e sistemas atualmente em funcionamento na nuvem emergencial.
- Garantia de compatibilidade com as 4 licenças Oracle já adquiridas pelo Município (Database Standard Edition 2).
- Garantia de compatibilidade com os sistemas desenvolvidos por terceiros, como o GRP e o ADMRH da empresa THEMA Informática.
- Acesso remoto seguro para prestadores de serviço homologados, mediante autenticação e controle de acesso.

f) Continuidade e portabilidade dos dados:

- A contratada deverá assegurar, contratualmente, o fornecimento de todos os dados e imagens de máquinas virtuais da Prefeitura, mediante solicitação formal, a qualquer tempo, de forma completa e em formato compatível com soluções de virtualização padrão de mercado.
- Os dados deverão ser entregues por meio digital ou por mídia externa, conforme escolha da contratante, sem cobrança adicional.

g) Localização da hospedagem:

- A infraestrutura contratada deverá estar fisicamente hospedada no Brasil, com Data Centers situados em território nacional, conforme as diretrizes da LGPD e de soberania de dados.

h) Backup e recuperação:

- Mecanismo automatizado de backup completo dos ambientes virtuais, com:
- Retenção mínima de 4 dias para backup diário e pelo menos 30 dias para backup semanal dos bancos de dados, replicados em Data Center secundário.
- Capacidade de recuperação granular (por arquivo, volume ou VM completa).
- Armazenamento do backup em infraestrutura separada ou com redundância geográfica.
- Procedimentos documentados de restauração de dados, com garantia de prazos máximos de recuperação (RTO e RPO definidos).

i) Canal de comunicação segura e integração com a Infraestrutura de rede da Prefeitura.

j) Distância entre Data Centers para política de Disaster Recovery (DR):

- Para garantir a eficácia da estratégia de continuidade de negócios e recuperação de desastres (Disaster Recovery) da Prefeitura Municipal, a solução contratada deverá prever a existência de um ambiente de contingência geograficamente distinto do ambiente principal de produção, em distância suficiente para minimizar o risco de perda dos dados da Prefeitura em caso de desastres naturais ou eventos de grande impacto.

A separação geográfica entre os Data Centers deverá considerar fatores como:

- Risco de enchentes, deslizamentos de terra e outros desastres ambientais;
- Falhas de infraestrutura elétrica ou de telecomunicações em uma mesma área regional;

- Incêndios, atos de vandalismo ou sabotagem;
- Eventos climáticos extremos, como os que atingiram o Estado do Rio Grande do Sul em 2024.

Portanto, essa exigência é essencial para garantir a disponibilidade, integridade e resiliência das informações institucionais, alinhada às diretrizes de governança digital, segurança da informação e continuidade de serviços públicos críticos.

8.1 Exigência de Certificações

Considerando a natureza crítica dos serviços a serem contratados, que envolvem a hospedagem de sistemas essenciais para o funcionamento da Prefeitura Municipal de Santa Cruz do Sul, torna-se imprescindível assegurar a qualidade, a disponibilidade e a segurança das infraestruturas utilizadas.

Certificação Tier III (ou equivalente):

A certificação Tier III, emitida pelo Uptime Institute, atesta que o Data Center possui infraestrutura redundante capaz de garantir alta disponibilidade, segurança física e continuidade operacional, requisitos indispensáveis para a manutenção dos serviços públicos eletrônicos.

De forma semelhante, a certificação TIA-942 Rated-3 garante que um Data Center foi projetado e construído com infraestrutura altamente resiliente, exigindo múltiplos caminhos de distribuição (energia e refrigeração) e componentes redundantes, permitindo que qualquer manutenção ou falha seja tratada sem interrupção nos serviços.

Todavia, visando não restringir a competitividade do certame, será admitida, alternativamente, a apresentação de documentação técnica que demonstre o atendimento aos requisitos de disponibilidade, redundância e manutenção simultânea previstos na classificação Tier III, ainda que a certificação formal não tenha sido obtida.

O Risco do "Data Center de Papel"

No mercado de infraestrutura de TI e computação em nuvem, certificações como as emitidas pelo Uptime Institute (Tier III/IV) e pela norma ANSI/TIA-942 (Rated 3/4) tornaram-se o padrão ouro. No entanto, muitos gestores e comissões de contratação desconhecem que ambas as metodologias dividem seus selos em duas fases distintas: a de Projeto (Design) e a de Instalação Construída (Facility). A certificação de Design atesta exclusivamente que a engenharia no papel foi bem desenhada e atende aos requisitos teóricos de redundância. O problema surge quando editais aceitam o selo de Design de forma isolada, criando a perigosa brecha do "Data Center de papel".

A brecha ocorre porque um projeto de engenharia pode ser aprovado e homologado pelo órgão certificador sem que a obra tenha sido concluída, ou pior, sem que os testes práticos de carga de energia, climatização e failover tenham sido realizados in loco. Na prática, uma licitante pode apresentar um selo Tier III Design referente a um prédio que ainda está em construção, que sofreu alterações arquitetônicas não homologadas para cortar custos durante a obra, ou cuja manutenção simultânea dos geradores jamais foi posta à prova. Confiar apenas na promessa do papel coloca em risco direto os sistemas críticos da Administração Pública, que podem ser hospedados em uma estrutura com pontos únicos de falha ocultos.

Para blindar os certames públicos sem restringir a competitividade — já que a auditoria presencial de Facility é um processo longo e de alto custo —, a solução técnica não é banir as certificações de Design, mas sim exigir condicionantes de operação real. O Termo de Referência deve prever que, caso a licitante opte por comprovar sua qualificação mediante certificação de Design, o documento seja compulsoriamente acompanhado de laudos de engenharia (com ART/RRT) ou relatórios de auditoria independente que comprovem que a instalação física foi integralmente executada conforme o projeto e encontra-se em plena operação comercial. Trata-se de uma medida simples que separa o marketing da engenharia real e garante a continuidade do serviço público.

Certificações ISO (ou equivalente):

A exigência de certificação ISO 27001 se justifica pela necessidade de assegurar que a contratada adote práticas reconhecidas internacionalmente para a gestão da segurança da informação, garantindo a proteção da confidencialidade, integridade e disponibilidade dos dados da Prefeitura de Santa Cruz do Sul.

Alternativamente, para assegurar a competitividade do certame, será permitido que a licitante demonstre, mediante documentação formal (como políticas, procedimentos, outras certificações e/ou outros documentos internos), o atendimento aos objetivos e controles estabelecidos nestas normas internacionais.

Fundamentação Legal:

Nesse contexto, certificações reconhecidas no mercado, como Uptime Institute Tier Certification of Constructed Facility – Tier III ou superior, ANSI/TIA-942 Facility/Constructed Facility – Rated-3 ou superior, ISO 27001 e certificações correlatas de segurança da informação, constituem meios idôneos para demonstrar que a infraestrutura e os processos adotados pela licitante ou pelo Data Center utilizado observam padrões técnicos compatíveis com a criticidade do objeto.

Todavia, a Administração reconhece que a exigência exclusiva de certificações formais específicas, como condição única de habilitação, pode restringir indevidamente a competitividade do certame, afastando empresas tecnicamente aptas que, embora não possuam determinada certificação formal, sejam capazes de demonstrar, por outros meios objetivos, o atendimento aos requisitos técnicos necessários à adequada execução contratual.

Assim, em atenção aos princípios da competitividade, isonomia, proporcionalidade, eficiência e seleção da proposta apta a gerar o resultado de contratação mais vantajoso, opta-se por admitir, alternativamente às certificações formais, a apresentação de certificações similares ou documentação técnica equivalente, desde que suficiente para demonstrar, de forma objetiva, o atendimento aos requisitos mínimos estabelecidos no Termo de Referência.

Essa opção encontra alinhamento com o entendimento consolidado pelo Tribunal de Contas da União no Acórdão nº 1605/2009 – Plenário, segundo o qual exigências de qualificação técnica ou critérios relacionados à capacidade do licitante devem guardar correlação técnica, pertinência e proporcionalidade com o objeto contratado, não podendo resultar em restrição indevida à competitividade ou exigir comprovações que não indiquem, necessariamente, maior capacidade para a execução do serviço.

Dessa forma, as certificações indicadas no Termo de Referência não são tratadas como finalidade em si mesmas, mas como meios de comprovação de que a licitante, a infraestrutura utilizada ou o ambiente de Data Center atendem aos níveis mínimos de segurança, disponibilidade, redundância, continuidade e governança exigidos pela Administração.

Para assegurar objetividade na análise, a documentação técnica equivalente deverá ser apresentada por meio de matriz de correspondência entre os requisitos exigidos e os documentos comprobatórios apresentados, indicando o requisito atendido, o documento correspondente, a página ou item específico em que o requisito é demonstrado e o responsável técnico pelas informações prestadas.

Poderão ser aceitos, conforme o caso, laudos técnicos, relatórios de auditoria, políticas de segurança da informação, planos de continuidade, planos de resposta a incidentes, procedimentos operacionais, evidências de controles implementados, certificações correlatas, contratos de colocation, declarações técnicas, diagramas de infraestrutura, relatórios de testes, documentos de comissionamento, registros de manutenção e demais documentos formais que permitam à Administração verificar objetivamente o atendimento aos requisitos estabelecidos.

Não serão aceitas, isoladamente, declarações genéricas de conformidade, materiais meramente comerciais, apresentações institucionais

ou documentos que não permitam verificar, de forma objetiva, a aderência da solução aos requisitos técnicos mínimos exigidos.

Dessa forma, busca-se equilibrar a necessidade de proteção dos sistemas e dados críticos da Administração Municipal com a preservação da ampla competitividade do certame, permitindo a participação de licitantes tecnicamente qualificadas, desde que comprovem, por certificação formal ou por documentação técnica equivalente, a sua capacidade de atender aos requisitos de segurança, disponibilidade, continuidade operacional e proteção de dados necessários à execução do objeto.

8.2 Localização da Infraestrutura em Território Nacional

A exigência de que os ambientes de produção e de contingência (backup) estejam localizados fisicamente em território nacional justifica-se pela natureza crítica dos sistemas a serem hospedados, os quais suportam atividades essenciais da Administração Municipal e envolvem o tratamento de dados institucionais, administrativos, financeiros, fiscais, funcionais e pessoais.

A manutenção da infraestrutura em território brasileiro contribui para reduzir riscos relacionados à transferência internacional de dados, conflitos de jurisdição, dificuldades de fiscalização, acesso a informações por autoridades estrangeiras, execução de medidas contratuais, rastreabilidade de incidentes, auditoria técnica e cumprimento das obrigações previstas na legislação brasileira, especialmente a Lei Geral de Proteção de Dados Pessoais.

Além dos aspectos jurídicos, de governança e de proteção de dados, a localização da infraestrutura em território nacional possui relevância técnica para o desempenho da solução, especialmente quanto à latência de comunicação entre os usuários, sistemas locais da Prefeitura, fornecedores externos, bancos de dados e aplicações hospedadas no ambiente de nuvem.

Os sistemas corporativos da Administração Municipal possuem operação contínua e dependem de comunicação frequente entre usuários, aplicações, bancos de dados, integrações, serviços web, rotinas de autenticação, consultas, gravações e transmissões de dados. Nesses cenários, a latência elevada pode impactar diretamente a experiência dos usuários, o tempo de resposta dos sistemas, a execução de rotinas administrativas, a integração com sistemas locais e a eficiência dos serviços digitais disponibilizados à população.

A localização dos Data Centers em território nacional tende a proporcionar menor latência média de acesso, maior previsibilidade de desempenho e melhor qualidade de comunicação com a infraestrutura de rede utilizada pela Prefeitura, quando comparada a ambientes hospedados em outros países ou regiões geográficas mais distantes. Esse aspecto é especialmente relevante para sistemas transacionais, bancos de dados,

serviços internos, portais públicos e aplicações que demandam resposta rápida e estabilidade de conexão.

A exigência também contribui para a adequada execução das estratégias de continuidade dos serviços, backup e recuperação de desastres, uma vez que a comunicação entre o ambiente principal, o ambiente secundário e a rede da Administração depende de enlaces com desempenho compatível com os objetivos de RPO e RTO estabelecidos na contratação.

Ressalta-se que essa exigência não restringe a participação de empresas em razão de sua nacionalidade, tampouco impede a participação de provedores nacionais ou internacionais, desde que a infraestrutura efetivamente utilizada para a prestação dos serviços esteja localizada no Brasil e atenda aos requisitos técnicos, operacionais, de segurança, desempenho e disponibilidade definidos no Termo de Referência.

Dessa forma, a exigência busca preservar a segurança jurídica, a governança, a continuidade operacional, a proteção dos dados públicos, a capacidade de fiscalização da Administração e o desempenho adequado dos sistemas hospedados, mostrando-se proporcional à criticidade dos serviços contratados e compatível com o interesse público envolvido.

9 DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

Assim como ilustrado na Figura 2, a solução a ser contratada consiste na disponibilização, por meio de serviços de computação em nuvem privada (modelo IaaS - Infraestrutura como Serviço), de uma infraestrutura virtualizada, escalável e sob demanda, capaz de hospedar os sistemas corporativos críticos e os serviços digitais da Prefeitura Municipal de Santa Cruz do Sul, com garantia de segurança, disponibilidade, desempenho e conformidade legal.

Essa solução compreende:

- A infraestrutura contratada deverá suportar a execução dos bancos de dados Oracle e módulos do sistema de gestão (GRP), bem como possibilitar a migração gradual de serviços atualmente mantidos no Data Center próprio da Prefeitura, compreendendo, principalmente sítio institucional, Intranet, PEC/e-SUS e demais aplicações corporativas.
- Ambiente de nuvem privada em Data Center certificado e localizado no Brasil, com recursos de computação virtualizados (vCPUs, memória RAM, armazenamento em SSD), com escalabilidade sob demanda, a serem gerenciados pela equipe de TI da Prefeitura.
- Conectividade segura e estável, com IPs públicos dedicados e exclusivos e canais de comunicação compatíveis com a estrutura de

rede já existente na Prefeitura, possibilitando integração com sistemas legados, fornecedores e acesso remoto quando necessário.

- Serviços de backup automatizado, snapshots, e ferramentas de restauração rápida em caso de falhas, conforme política de continuidade dos serviços.
- Camadas de segurança, incluindo firewall virtual de aplicação, segmentação de rede, controle de acesso, autenticação forte e ferramentas de monitoramento e auditoria.
- Gestão simplificada da infraestrutura virtual, permitindo que a Prefeitura monitore em tempo real os servidores virtuais, sem depender diretamente da contratada.
- Atendimento aos requisitos da Lei Geral de Proteção de Dados (LGPD) e demais normas de segurança da informação, com suporte técnico contínuo e SLA de alta disponibilidade.

A solução será contratada com base em consumo estimado, mas com previsão de elasticidade, permitindo à Prefeitura escalar os recursos contratados conforme a evolução da demanda.

A entrega da solução será feita de forma progressiva e em conformidade com a migração dos sistemas, sob acompanhamento da equipe técnica municipal e dos fornecedores de software, que realizarão as implantações diretamente na infraestrutura contratada.

10 JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO

A presente contratação tem por objeto a aquisição de uma solução integrada de infraestrutura como serviço (IaaS) em nuvem privada, envolvendo recursos computacionais, armazenamento, conectividade, segurança e suporte técnico, que operam de forma conjunta e interdependente.

Embora os itens estejam discriminados para fins de medição e controle de consumo (vCPU, memória, storage, IPs, links, firewall, etc.), não é tecnicamente viável, nem operacionalmente possível, que esses componentes sejam fornecidos de forma fracionada por empresas distintas, como, por exemplo, contratar processadores de uma empresa, memória de outra e armazenamento de uma terceira.

A infraestrutura de nuvem funciona como um ambiente unificado, gerenciado por uma única camada de virtualização e orquestração, que exige compatibilidade plena, integração total e responsabilidade técnica centralizada. Além disso, o modelo de contratação é baseado em provisionamento sob

demanda, com cobrança por consumo real — o que demanda uma plataforma única de gestão e controle, impossível de ser operada de forma fragmentada entre diferentes fornecedores.

Importa destacar que, conforme levantamento realizado em editais recentes de contratação de nuvem pública e privada (modelo IaaS), nenhuma licitação desse tipo adota parcelamento do objeto, justamente por se tratar de uma solução tecnicamente indivisível.

Assim, o objeto licitado é, por natureza, impassível de divisão em lotes, sob pena de comprometer sua integridade, segurança, desempenho, viabilidade técnica e contratual. Por exemplo, é tecnicamente inviável criar uma máquina virtual cujos principais componentes (CPU, memória ou armazenamento) sejam fornecidos por diferentes empresas.

11 ALINHAMENTO ENTRE A CONTRATAÇÃO E O PLANEJAMENTO

A presente contratação é fruto da necessidade de ambiente para hospedagem de aplicações que estão alinhadas diretamente ao objetivo estratégico “Fortalecer o Governo Digital para modernizar a Gestão, desburocratizar os processos e prestar serviços de forma ágil e eficiente”, definido no inciso VIII, do Art. 4º, da Lei 8.652, de 2021, a qual dispõe sobre o PPA 2022-2025.

O objeto da contratação está previsto no Plano de Contratações Anual de 2026, ID nº 597.

12 RESULTADOS PRETENDIDOS

Com a contratação de uma solução de computação em nuvem privada (modelo IaaS), a Prefeitura Municipal de Santa Cruz do Sul espera alcançar os seguintes resultados:

a) Continuidade e estabilidade dos serviços digitais essenciais

Garantia da operação contínua e confiável de sistemas críticos como o SIGM/GRP, ADMRH, Portal da Transparência, sistema de emissão de notas fiscais, site institucional, Intranet e outras soluções digitais em uso ou em desenvolvimento, com alto nível de disponibilidade e desempenho.

b) Maior segurança da informação e proteção contra incidentes cibernéticos

Redução de riscos de indisponibilidade, vazamentos ou perdas de dados por meio da adoção de uma infraestrutura com padrões avançados de

segurança, proteção contra ataques externos, backup automatizado e conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD).

c) Modernização e escalabilidade da infraestrutura de TI

Superação das limitações do Data Center físico da Prefeitura, com capacidade elástica de crescimento conforme a demanda, evitando investimentos excessivos em equipamentos físicos e infraestrutura local.

d) Economia e eficiência na gestão de recursos públicos

Otimização dos investimentos em tecnologia por meio do provisionamento sob demanda (pay-as-you-go), evitando ociosidade de recursos e permitindo maior previsibilidade e controle de custos.

e) Aprimoramento da governança e da gestão tecnológica municipal

Possibilidade de gestão centralizada, monitoramento de desempenho, acesso remoto e controle sobre os recursos computacionais utilizados, fortalecendo a atuação estratégica da equipe de TI da Prefeitura.

f) Fortalecimento da capacidade de resposta a emergências e incidentes

Redução do tempo de recuperação (RTO) e da perda aceitável de dados (RPO) em caso de falhas, com infraestrutura que suporte planos de continuidade e recuperação de desastres.

g) Facilidade de integração com prestadores de serviços externos

Criação de um ambiente seguro e estruturado que permita o acesso remoto aos sistemas por empresas terceirizadas (como a empresa THEMA), garantindo desempenho e segurança no suporte e na manutenção dos sistemas hospedados.

h) Base tecnológica sustentável para a transformação digital do município

Criação de uma plataforma tecnológica moderna e confiável para suportar o desenvolvimento e a digitalização de novos serviços públicos, fortalecendo a eficiência administrativa e a prestação de serviços ao cidadão.

13 PROVIDÊNCIAS A SEREM ADOTADAS PREVIAMENTE À CELEBRAÇÃO DO CONTRATO

- Não há providências a serem adotadas anteriormente à celebração do contrato.

14 CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

a) Contrato 68/PGM/2025

- Fornecedor: THEMA INFORMATICA LTDA
- Objeto: Contratação de solução para a manutenção do Sistema de Gestão Integrado Municipal (GRP).

b) Contrato 266/PGM/2024

- Fornecedor: BRASIL TECPAR SERVIÇOS DE TELECOMUNICAÇÃO S.A.
- Objeto: Contratação de empresa referente à locação de infraestrutura de rede para comunicação, visando a interligação de unidades, conexão de internet, firewall, wifi e cloud para o Município.

c) Contrato 225/PGM/2023

- Fornecedor: ORACLE DO BRASIL SISTEMAS LTDA
- Objeto: Contratação de Serviços de Suporte Técnico de Software (licenças do banco de dados) Oracle Database Standard Edition 2 - Processor Perpetual.

d) Contrato 100/PGM/2023

- Fornecedor: TOPOCART - TOPOGRAFIA ENGENHARIA E AEROLEVANTAMENTOS
- Objeto: Contratação de serviços técnicos em tecnologia da informação no que tange ao suporte técnico, assessoria continuada, manutenção e atualização do atual sistema de informações geográficas (SIG) GEO360 do Município.

15 POSSÍVEIS IMPACTOS AMBIENTAIS

Dada a natureza do objeto que se pretende adquirir, não se verifica impactos ambientais na implantação da solução objeto.

16 DECLARAÇÃO DE VIABILIDADE

Após análise técnica, mercadológica e jurídica, declara-se plenamente viável a contratação de uma solução de infraestrutura como serviço (IaaS) em nuvem privada, conforme detalhado neste Estudo Técnico Preliminar.

A contratação proposta está em consonância com os princípios da economicidade, eficiência, escalabilidade e segurança da informação, e visa

estabelecer uma base tecnológica robusta e flexível, capaz de sustentar a evolução digital da Prefeitura Municipal de Santa Cruz do Sul pelos próximos anos.

Trata-se de um serviço comum, nos termos do inciso XIII do art. 6º da Lei nº 14.133/2021, uma vez que os padrões de desempenho e qualidade dos recursos a serem contratados — como vCPU, memória, armazenamento, largura de banda, disponibilidade mínima, e certificações técnicas — podem ser objetivamente definidos no edital, com base em especificações amplamente praticadas pelo mercado de tecnologia da informação.

A contratação será realizada sob demanda, com pagamento proporcional ao consumo efetivo, o que garante flexibilidade e previsibilidade orçamentária, permitindo que a Prefeitura adéque a capacidade da infraestrutura conforme o crescimento ou a readequação dos serviços públicos digitais.

Adicionalmente, a viabilidade da contratação também se sustenta no fato de que diversas empresas no mercado nacional oferecem esse tipo de solução, conforme verificado em pesquisas de contratações similares, sem prejuízo à competitividade. A modalidade escolhida para a licitação será o pregão eletrônico, que assegura transparência, ampla concorrência e celeridade processual.

Mais do que uma medida técnica ou contratual, esta contratação representa uma estratégia essencial para assegurar a continuidade dos serviços públicos digitais, garantindo que sistemas críticos — como o GRP, o ADMRH, a emissão de documentos, o portal da transparência, o site institucional, a Intranet, e-SUS e outras soluções em homologação e desenvolvimento — permaneçam disponíveis de forma segura e estável, mesmo diante de falhas, ataques cibernéticos ou eventos extremos.

Com isso, a Prefeitura assegura não apenas a eficiência da sua gestão interna, mas também o pleno acesso dos cidadãos, servidores e empresas aos serviços públicos de forma digital, 24 horas por dia, sete dias por semana, consolidando um modelo de administração mais moderno, transparente e alinhado aos princípios da transformação digital do setor público.

Diante do exposto, conclui-se que a solução proposta é tecnicamente viável, juridicamente adequada e estrategicamente necessária, representando a melhor alternativa para sustentar os serviços públicos digitais e promover a continuidade das políticas públicas de inovação e governança digital.

17 ANEXOS

1 – Boletim de Medição mês de fevereiro 2025 – Contrato 266/PGM/2024.

2 – Lista de recursos utilizados nas VMs na nuvem atualmente contratada.

3 – Tabela de recursos utilizados nas VMs do Data Center local.

4 – Solicitação da THEMA Informática de Atualização de Ambiente Tecnológico.

5 – Proposta THEMA Cloud.

6 – Proposta Serpro Multicloud.

7 - Planilha Orçamentária

18 RESPONSÁVEIS

Álvaro dos Santos Neuwald – 13931 Agente Administrativo	Ricardo Voigt – 11953 Programador

DESPACHO DA AUTORIDADE SUPERIOR

Com base nas informações apresentadas neste Estudo Técnico Preliminar, autorizo a Elaboração do Termo de Referência para a licitação de contratação de serviço de nuvem privada (cloud computing), no modelo IaaS (Infrastructure as a Service) para hospedagem de bancos de dados e sistemas críticos (próprios e contratados) da Prefeitura de Santa Cruz do Sul.

Santa Cruz do Sul, 08 de Setembro de 2026.

Matheus Luis Ferreira
Secretário Municipal de Administração e Gestão