UNIVERSIDADE FEDERAL DO SUL E SUDESTE DO PARÁ

Estudo Técnico Preliminar 24/2026

1. Informações Básicas

Número do processo: 23479.005193/2026-11

2. Descrição da necessidade

Contratação de empresa especializada na prestação de serviços de infraestrutura de Tecnologia da Informação como Serviço.

A presente contratação tem por objetivo atender à necessidade institucional de provimento de **infraestrutura computacional de missão crítica**, destinada a suportar o **Novo Sistema de Gestão de Processos Seletivos do CEPS/UNIFESSPA**, assegurando condições adequadas de disponibilidade, desempenho, segurança, continuidade e recuperação dos serviços envolvidos.

A solução requerida não se restringe ao fornecimento convencional de hospedagem ou de servidor dedicado. Trata-se da disponibilização de **ambiente integrado de Infraestrutura como Serviço (IaaS – Infrastructure as a Service)**, contemplando recursos computacionais dimensionados para a demanda, isolamento de recursos, conectividade IP dedicada, mecanismos de segurança perimetral, monitoramento contínuo, serviços de **SOC e SIEM**, backup corporativo e suporte técnico permanente, em regime compatível com a criticidade dos serviços institucionais.

A demanda foi estruturada com base em requisitos técnicos e operacionais indispensáveis à garantia da **continuidade, integridade, disponibilidade, confidencialidade e segurança** dos serviços públicos relacionados aos processos seletivos, especialmente nos períodos de maior concentração de acessos, tais como abertura e encerramento de inscrições, processamento de dados, divulgação de resultados e demais etapas que demandem elevado volume de requisições simultâneas.

Nesse contexto, eventual indisponibilidade, degradação de desempenho ou inadequação da infraestrutura computacional poderá comprometer diretamente a execução das atividades do CEPS, ocasionando indisponibilidade do sistema, atrasos na execução dos cronogramas, perda ou indisponibilidade de dados, dificuldades de acesso pelos usuários e riscos à regularidade e à confiabilidade dos processos seletivos, além de possíveis impactos à imagem institucional da Universidade.

A necessidade apresentada demanda, portanto, uma infraestrutura computacional em modelo IaaS capaz de atender, de forma integrada, aos requisitos de **desempenho, disponibilidade, segurança, conectividade, monitoramento, proteção de dados, continuidade e suporte técnico**. Sob a perspectiva de conectividade e engenharia de tráfego, a localização da infraestrutura deverá considerar a necessidade de comunicação eficiente com a região Norte, especialmente com o campus da UNIFESSPA em Marabá/PA, buscando-se, quando tecnicamente disponível, rotas de comunicação eficientes, conectividade adequada e baixa latência, de modo a contribuir para a responsividade dos sistemas utilizados pela Instituição.

No que se refere à infraestrutura física, busca-se provedor que disponha de **Data Center com elevado nível de disponibilidade e redundância**, compatível com a criticidade dos serviços a serem hospedados, bem como mecanismos de segurança e continuidade operacional respaldados por certificações e padrões reconhecidos no mercado. Nesse sentido, requisitos relacionados à disponibilidade da instalação, manutenção concorrente, redundância de componentes críticos, segurança física e lógica e capacidade de recuperação de incidentes constituem elementos relevantes para a adequada prestação do serviço.

A opção por uma solução integrada de infraestrutura dedicada decorre da necessidade de garantir **performance previsível, isolamento de recursos, disponibilidade, monitoramento 24x7, resposta tempestiva a incidentes e mecanismos de proteção e recuperação de dados**, reduzindo os riscos associados à indisponibilidade ou à degradação dos serviços. A arquitetura e os requisitos especificados foram definidos considerando as características do caso concreto, os requisitos de segurança da informação e de proteção de dados e a legislação aplicável, especialmente a **Lei nº 14.133/2021** e a **Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD)**.

Dessa forma, a contratação não se caracteriza como mera aquisição de infraestrutura computacional padronizada, mas como a disponibilização de um **conjunto integrado de recursos, serviços e mecanismos de suporte**, dimensionado para atender a uma necessidade institucional específica e a um ambiente de elevada criticidade. A solução deverá proporcionar condições adequadas para a execução estável e segura dos serviços, com redução dos riscos operacionais, maior previsibilidade da infraestrutura e preservação da continuidade das atividades administrativas e finalísticas relacionadas aos processos seletivos.

Conforme registrado no **Documento de Formalização da Demanda (DFD)**, a infraestrutura atualmente utilizada pela unidade apresenta sinais de obsolescência e opera próxima aos seus limites de capacidade, elevando os riscos de instabilidade, especialmente durante os períodos de maior demanda. O cenário atual pode resultar em indisponibilidade durante etapas críticas dos processos seletivos, vulnerabilidades relacionadas ao armazenamento e processamento de dados e incompatibilidades com os requisitos técnicos do novo sistema.

Ainda segundo o DFD, a necessidade apresenta caráter prioritário em razão do cronograma dos processos seletivos previstos para **agosto e dezembro de 2026**, para os quais foi estimado volume de acessos simultâneos superior à capacidade atualmente disponível na infraestrutura utilizada pelo CEPS. Esse cenário evidencia a necessidade de adoção de medida capaz de ampliar, de forma tempestiva, a capacidade computacional disponível e reduzir os riscos de indisponibilidade durante a execução dos certames.

Paralelamente, a UNIFESSPA possui o **Processo Administrativo nº 23479.004076/2026-31**, em andamento, destinado à aquisição de ativos de Infraestrutura de Tecnologia da Informação e Comunicação (TIC) para o Datacenter institucional. O referido processo contempla a modernização dos recursos de processamento e armazenamento, implantação de solução hiperconvergente, infraestrutura de backup, racks, servidores remotos, além de outros componentes necessários à atualização da infraestrutura tecnológica institucional.

A necessidade de modernização estrutural decorre, entre outros fatores, da proximidade do limite de capacidade de armazenamento do Datacenter, da idade avançada de parcela significativa dos equipamentos, da existência de ativos com garantia expirada ou próxima do término de sua vida útil e dos riscos associados à manutenção do cenário atual, especialmente quanto à ocorrência de falhas críticas, indisponibilidade de serviços e eventual perda de dados.

Embora a contratação definitiva dos ativos de TIC para o Datacenter institucional constitua a solução estrutural destinada à modernização da infraestrutura da Universidade, **sua conclusão e implantação não ocorrerão em prazo compatível com a necessidade imediata apresentada pelo CEPS**. Isso decorre da complexidade técnica e administrativa do objeto, da amplitude do escopo, das etapas necessárias à adequada instrução processual, análise das alternativas, seleção da solução, contratação, entrega, instalação, configuração, testes e posterior entrada em produção dos novos equipamentos.

Nesse cenário, a contratação da infraestrutura em modelo IaaS apresenta-se como **medida temporária e transitória**, destinada a suprir a necessidade imediata de capacidade computacional do CEPS enquanto a solução estrutural do Datacenter institucional não é concluída e disponibilizada para utilização.

A adoção dessa medida permitirá disponibilizar, em prazo compatível com o cronograma dos processos seletivos, ambiente computacional adequado para a **implantação, configuração, testes e operação do Novo Sistema de Gestão de Processos Seletivos**, contribuindo para a redução dos riscos de indisponibilidade e para a continuidade dos serviços públicos relacionados aos certames já planejados.

Assim, a contratação pretendida deve ser compreendida como **solução de caráter temporário, excepcional e complementar à modernização definitiva do Datacenter institucional**, não representando substituição ou sobreposição à aquisição dos ativos de TIC prevista no Processo nº 23479.004076/2026-31. Sua finalidade é assegurar a continuidade e a disponibilidade dos serviços do CEPS durante o período necessário à conclusão e implantação da infraestrutura permanente da UNIFESSPA.

2.1 Situação atual do datacenter e dos ativos de TI

O Datacenter institucional opera em arquitetura hiperconvergente Nutanix, com cluster composto por quatro *hosts* físicos, em gerações de hardware distintas (G5 e G7), sendo que a maior parte da infraestrutura ativa pertence à geração G5, com cerca de 8 a 9 anos de ciclo tecnológico.

Embora o ambiente de processamento e armazenamento ainda apresente desempenho estável, o uso de memória RAM se encontra em estado crítico, com três dos quatro *hosts* operando acima de 91% de utilização, o que reduz significativamente a margem operacional para tolerância a falhas, redistribuição de cargas e expansão de serviços.

A capacidade de armazenamento encontra-se próxima do limite, com crescimento constante da demanda; além disso, parte dos servidores do Datacenter e dos Campi externos está em fim de vida útil, com garantias e suporte técnico expirados, o que eleva a exposição a falhas críticas e riscos de indisponibilidade e perda de dados.

Nesse contexto, a contratação de IaaS apresenta-se como medida transitória, especializada e tecnicamente estruturada para viabilizar a implantação, os testes e a operação assistida do Novo Sistema de Gestão de Processos Seletivos, reduzindo riscos enquanto não se conclui a modernização definitiva.

2.2 Impacto da não contratação.

- A ausência da contratação poderá ocasionar:

  interrupção de inscrições;

  lentidão ou indisponibilidade do sistema;

  risco à integridade dos dados dos candidatos;

  perda ou inconsistência de informações;

retrabalho das equipes;

comprometimento do cronograma dos certames;

necessidade de contingenciamento operacional;

prejuízo à imagem institucional;

risco à lisura e à continuidade do serviço público.

3. Área requisitante

Área Requisitante	Responsável
Centro de Processos Seletivos - Ceps.	Jairo Belchior Freitas Oliveira

4. Necessidades de Negócio

A necessidade do negócio consiste em prover **infraestrutura computacional adequada, estável, segura e dimensionada à demanda** para suportar o Novo Sistema de Gestão de Processos Seletivos do CEPS/UNIFESSPA, assegurando níveis compatíveis de **disponibilidade, desempenho, integridade, segurança e continuidade operacional** para as atividades institucionais relacionadas à realização dos certames.

A infraestrutura atualmente disponível não apresenta capacidade suficiente para absorver, de forma segura e confiável, a demanda prevista para o novo sistema, especialmente nos períodos de maior concentração de acessos e processamento, tais como **abertura e encerramento das inscrições, processamento de dados, análise de recursos, divulgação de resultados e demais etapas dos processos seletivos**. A limitação dos recursos computacionais existentes, associada à obsolescência de parte da infraestrutura, aumenta a exposição a riscos de lentidão, instabilidade, indisponibilidade dos serviços e comprometimento da integridade ou disponibilidade dos dados, podendo afetar diretamente a execução das atividades finalísticas do CEPS.

Diante desse cenário, torna-se necessária a disponibilização de uma **infraestrutura como serviço (IaaS)**, dimensionada para as necessidades do sistema e capaz de oferecer recursos computacionais adequados, conectividade apropriada, mecanismos de segurança perimetral, backup, monitoramento contínuo, serviços de **SOC e SIEM** e suporte técnico permanente. Esses recursos são necessários para proporcionar maior previsibilidade de desempenho, capacidade de resposta a incidentes e condições adequadas de continuidade e recuperação dos serviços.

A contratação também busca assegurar que a operação do novo sistema ocorra em ambiente compatível com os requisitos institucionais de **segurança da informação e proteção de dados**, observando a legislação aplicável e os princípios que regem a Administração Pública, especialmente a continuidade do serviço público, a eficiência e o interesse público.

Assim, a necessidade identificada não se limita à ampliação da capacidade computacional atualmente disponível, mas envolve a disponibilização de **ambiente tecnológico adequado à criticidade e às características operacionais dos processos seletivos**, de modo a reduzir riscos de interrupção, assegurar condições de funcionamento do sistema durante os períodos de maior demanda e proporcionar maior confiabilidade à execução das atividades institucionais do CEPS/UNIFESSPA.

5. Necessidades Tecnológicas

5.1 A solução de TIC a ser contratada deverá prover ambiente integrado de infraestrutura como serviço (IaaS), apto a suportar a implantação, os testes, a operação assistida e a entrada em produção do Novo Sistema de Gestão de Processos Seletivos do CEPS/UNIFESSPA, bem como de serviços institucionais correlatos que exijam elevado nível de disponibilidade, desempenho previsível, segurança da informação e suporte operacional contínuo

5.2 Requisitos funcionais da solução

A solução deverá prover ambiente integrado de IaaS apto a suportar implantação, testes, operação assistida e entrada em produção do Novo Sistema de Gestão de Processos Seletivos e de serviços correlatos.

Deverá contemplar, no mínimo:

- 3 servidores dedicados Bare Metal, cada um com 2 processadores físicos, 40 núcleos totais, 128 GB de memória RAM DDR4, 2 SSD NVMe de 2 TB em RAID 1, sistema operacional Linux e porta de rede dedicada de 1 Gbps;
- 1 bloco de endereçamento IPv4 público /28, com 14 endereços utilizáveis, compatível com a publicação dos serviços institucionais.
- 2 switches de 24 portas 10 Gbps, necessários à composição da arquitetura de conectividade e alta disponibilidade do ambiente.
- solução de segurança perimetral baseada em firewall de próxima geração (NGFW), em arquitetura de alta disponibilidade, com funcionalidades compatíveis com inspeção, controle de tráfego e proteção unificada contra ameaças.O serviço de SOC & SIEM integra a arquitetura de proteção da solução e se justifica pela necessidade de ampliar a capacidade de detecção, prevenção e resposta a incidentes de segurança, complementando os mecanismos já previstos de firewall, monitoramento contínuo, backup e suporte 24x7.
- licenças e serviços necessários ao funcionamento e atualização da camada de segurança;
- gerenciamento operacional 24x7;
- backup corporativo para os 3 servidores físicos, com armazenamento de 4.000 GB em território nacional;
- serviço de gerenciamento operacional 24x7, com apoio técnico especializado e franquia mensal de horas para atuação em nível de sistema operacional e serviços correlatos.
- serviço de monitoramento contínuo, com dashboard, alertas e mecanismos de resposta a incidentes, inclusive por canais eletrônicos e telefônicos, conforme configuração contratada.
- Serviço de SOC & SIEM , com monitoramento especializado de eventos de segurança, esclarecimento e análise de logs, detecção de ameaças, geração de alertas, apoio à resposta a incidentes e fortalecimento da governança de segurança da informação, em regime compatível com a criticidade do ambiente institucional.
- setup, implantação, configuração, testes e operação assistida.
- Segurança e conformidade com normas regulatórias: A necessidade de adesão estrita à Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709 /2018) demanda que o Data Center contratado possua as certificações ISO/IEC 27001 (Segurança da Informação), ISO/IEC 27017 e 27018 (Segurança em Nuvem) e, notadamente, a ISO/IEC 27701 (Gestão de Privacidade da Informação), atestando a governança de dados by design.
- "Manutenção Concorrente" (Concurrent Maintainability), com energia elétrica e climatização redundantes (UPS, geradores, rotas A/B). O SLA de 99,98% de infraestrutura garante tolerância a falhas extremas.
- Eficiência operacional e custo-benefício: A terceirização (outsourcing) de IaaS elimina a necessidade de gestão física de hardware, substituição de componentes depreciados e custos com expansão de rede local, transformando despesas de capital (CAPEX) em despesas operacionais (OPEX) altamente controláveis.

5.3 Requisitos de desempenho e capacidade

A solução deverá entregar desempenho compatível com ambiente de missão crítica, sem compartilhamento dos principais recursos computacionais com outros clientes, de modo a assegurar previsibilidade de performance e redução de degradações causadas por concorrência de uso (noisy neighbors). A arquitetura Bare Metal mostra-se adequada ao perfil de carga do CEPS, especialmente para rotinas de inscrição, processamento de resultados, tratamento de recursos e guarda de documentos digitais associados aos certames.
A infraestrutura deverá suportar crescimento ordinário da demanda institucional, bem como absorver cargas simultâneas superiores à capacidade atualmente disponível no ambiente local, considerando o aumento previsto de acessos nos processos seletivos de 2026.

5.4 Requisitos de conectividade e rede

A solução deverá disponibilizar conectividade dedicada de, no mínimo, 1 Gbps, com tráfego ilimitado ou política equivalente que não comprometa o uso institucional ordinário. Também deverá fornecer bloco IPv4 público compatível com a necessidade de publicação de serviços, integração entre componentes e segregação lógica dos ambientes.
A arquitetura de rede deverá ser compatível com o desenho proposto para operação em alta disponibilidade, incluindo componentes de borda, comutação e segregação de tráfego entre camadas da solução.

5.5 Requisitos de segurança e proteção de dados

A solução deverá contemplar mecanismos compatíveis com proteção perimetral avançada, mitigação de ameaças e monitoramento de segurança SOC & SIEM, incluindo firewall de próxima geração em alta disponibilidade, gerenciamento unificado de ameaças e controles de acesso compatíveis com a criticidade do ambiente.

O ambiente deverá estar hospedado em datacenter com controles de acesso físico, monitoramento operacional, segurança física, conectividade redundante, energia adequada e climatização compatível com a continuidade do serviço. A operação deverá observar os princípios de confidencialidade, integridade e disponibilidade das informações, em conformidade com a Lei Geral de Proteção de Dados e com a Política de Segurança da Informação da contratante.

5.6 Backup, recuperação e continuidade

A solução deverá incluir serviço de backup corporativo com capacidade compatível com a proteção dos servidores físicos previstos, retenção em infraestrutura nacional e mecanismos aptos à restauração em caso de falha operacional ou incidente. O objetivo é assegurar proteção dos dados institucionais, resiliência do ambiente e suporte à continuidade do serviço público.

Além do backup, a solução deverá prever suporte a plano de contingência, rotinas de transição e encerramento contratual com restituição dos dados, revogação de acessos e eliminação segura das informações remanescentes na infraestrutura da contratada

5.7 Monitoramento, suporte e operação especializada

A contratada deverá fornecer monitoramento contínuo 24x7 da infraestrutura, da conectividade, dos componentes de segurança e dos ativos computacionais, com emissão de alertas e produção de relatórios mensais de disponibilidade, desempenho e incidentes. O suporte técnico deverá operar em regime 24x7x365, com tempo máximo de resposta de até 60 minutos para incidentes críticos.

A operação deverá incluir canais formais de atendimento, sistema de registro de chamados e equipe tecnicamente capacitada para atuação sobre os componentes da solução, inclusive em nível de sistema operacional, segurança e serviços correlatos.

5.8 Requisitos de implantação

A solução deverá ser entregue em estado operacional, com todos os recursos provisionados, testados e acessíveis à equipe técnica da UNIFESSPA. O prazo de ativação da proposta de referência é de até 15 dias úteis, enquanto o ciclo de implantação previsto no TR admite setup físico e lógico em até 30 dias úteis, compreendendo provisionamento dos servidores, configuração das sub-redes, implantação da segurança perimetral e criação das políticas de backup.

A contratada deverá, ainda, apresentar plano de implantação, manutenção preventiva e contingência, detalhando as etapas técnicas de entrada em operação do ambiente.

5.9 Data Center e certificações

O ambiente deverá estar sediado em território nacional, em Data Center profissional com padrão compatível com operação de missão crítica, redundância elétrica, climatização de precisão, segurança física, conectividade redundante e monitoramento.

Deverá possuir certificação de design construtivo Tier III pelo Uptime Institute, com capacidade de manutenção concorrente, observando-se o escopo, a validade e as limitações expressas no certificado apresentado.

Como evidências de capacidade e governança, deverão ser consideradas, conforme escopo e validade:

- ISO 9001;
- ISO/IEC 20000-1;
- ISO 22301;
- ISO/IEC 27001;
- ISO/IEC 27017;
- ISO/IEC 27018;
- ISO/IEC 27701.

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

6.1 Requisitos legais

O processo de contratação deverá observar a Constituição Federal, a Lei nº 14.133/2021, a Instrução Normativa SGD/ME nº 94/2022, a Instrução Normativa SEGES/ME nº 65/2021, a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), bem como os demais normativos aplicáveis à contratação de soluções de TIC no âmbito da Administração Pública Federal.

A solução deverá ser compatível com o planejamento institucional, inclusive com as demandas registradas no PCA, com o PDTIC vigente e com as diretrizes de segurança da informação, governança e continuidade operacional adotadas pela UNIFESSPA.

6.1.1 Do enquadramento na portaria 5.950/2023 e Portaria SGD/MGI nº 1.070/2023

A contratação pretendida consiste na disponibilização de **infraestrutura de Tecnologia da Informação e Comunicação como Serviço (IaaS – Infrastructure as a Service)**, destinada ao atendimento de necessidade institucional específica da UNIFESSPA, para suporte ao Novo Sistema de Gestão de Processos Seletivos do CEPS.

O objeto possui como núcleo a disponibilização de **recursos computacionais dedicados e serviços de infraestrutura gerenciada**, abrangendo processamento, conectividade, segurança perimetral, backup, monitoramento contínuo, serviços de SOC e SIEM e suporte técnico, em ambiente dimensionado de acordo com os requisitos de disponibilidade, desempenho, segurança e continuidade operacional estabelecidos para o sistema.

Embora a solução possa utilizar tecnologias de virtualização e elementos característicos de ambientes de computação em nuvem, a contratação está estruturada primordialmente para prover **capacidade computacional e serviços gerenciados de infraestrutura**, não envolvendo, como objeto principal, atividades de desenvolvimento, manutenção ou sustentação de software.

Da mesma forma, o objeto não consiste simplesmente na contratação de capacidade computacional genérica, mas na disponibilização de um **ambiente integrado de infraestrutura e serviços especializados**, com requisitos específicos de segurança, monitoramento, proteção de dados, disponibilidade e suporte, necessários ao funcionamento de sistema institucional de elevada criticidade.

Nesse sentido, o enquadramento da contratação deverá considerar a **natureza efetiva do objeto e os serviços que o compõem**, bem como as disposições normativas aplicáveis às contratações de TIC. Não se caracteriza, portanto, como contratação de serviços de desenvolvimento, manutenção ou sustentação de software, matéria disciplinada pela **Portaria SGD/MGI nº 1.070/2023**, uma vez que tais atividades não integram o objeto pretendido.

Quanto às normas aplicáveis aos serviços de computação em nuvem e demais soluções de TIC, deverão ser observados, conforme sua pertinência ao caso concreto, os requisitos, diretrizes e boas práticas estabelecidos pela regulamentação vigente, inclusive aqueles relacionados à segurança da informação, proteção de dados, gestão de riscos, continuidade e níveis de serviço.

Assim, para fins de planejamento e instrução processual, a contratação deve ser caracterizada como **solução de infraestrutura de TIC em modelo IaaS, com serviços gerenciados e componentes de segurança da informação**, destinada a prover ambiente computacional adequado para a operação do Novo Sistema de Gestão de Processos Seletivos do CEPS/UNIFESSPA, observando-se a legislação aplicável e as normas específicas vigentes para as contratações de TIC.

6.2 Requisitos de garantia e suporte técnico

A contratada deverá garantir níveis mínimos de serviço compatíveis com a criticidade da solução, observando-se, como referência, disponibilidade mensal de 99,98% para a infraestrutura de datacenter (energia e climatização), 99,50% para rede e conectividade IP, e tempo máximo de resposta de até 60 minutos para incidentes críticos.

Em caso de descumprimento dos níveis de serviço pactuados, deverão ser previstos mecanismos de medição, glosa ou abatimento proporcional, nos termos do Termo de Referência e do contrato, de modo a assegurar controle de desempenho e responsabilização contratual.

6.3 Critérios de Sustentabilidade

Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os seguintes requisitos, que se baseiam no Guia Nacional de Contratações Sustentáveis:

Diretrizes Gerais e Conformidade Normativa: A execução dos serviços de infraestrutura como serviço (IaaS) e hospedagem (Data Center) deverá observar estritamente o princípio do desenvolvimento nacional sustentável, insculpido no art. 5º da Lei nº 14.133/2021, bem como as diretrizes estabelecidas pelo Guia Nacional de Contratações Sustentáveis e pela Política de Sustentabilidade do Poder Judiciário/Executivo. A Contratada deverá comprovar a adoção de práticas corporativas que garantam a responsabilidade socioambiental ao longo de todo o ciclo de vida da prestação tecnológica.

Eficiência Energética e Matriz Renovável: A infraestrutura do Data Center (padrão Tier III) deverá ser operada sob métricas rigorosas de eficiência energética, evidenciadas por um baixo índice PUE (Power Usage Effectiveness). Exige-se a adoção de tecnologias de refrigeração de precisão

(confinamento de corredores frios/quentes) e a utilização prioritária de fontes de energia limpa e renovável. Notadamente, a operação da Contratada baseada em usina solar fotovoltaica própria atende de forma cabal a este requisito, reduzindo a dependência de combustíveis fósseis e matrizes poluentes.

Gestão do Ciclo de Vida e Logística Reversa: Durante as manutenções físicas e eventuais substituições de hardware (componentes de Bare Metal, switches ou firewalls) decorrentes de falhas operacionais, a Contratada deverá aplicar diretrizes de logística reversa. Os componentes eletrônicos substituídos deverão ter destinação final ambientalmente adequada, em conformidade com a Política Nacional de Resíduos Sólidos (Lei nº 12.305/2010), priorizando a reciclagem de e-lixo (e-waste) e a exclusão de substâncias perigosas (diretiva RoHS).

Desmaterialização e Governança Digital: A gestão documental do contrato, abrangendo a emissão de relatórios de uptime, faturamento, registros de Acordo de Nível de Serviço (SLA) e tratativas do Centro de Operações de Rede (NOC), ocorrerá de forma integralmente digital (paperless), abstendo-se do uso de papel e insumos de impressão. O acesso a painéis de monitoramento dar-se-á exclusivamente via dashboards em portais web autenticados.

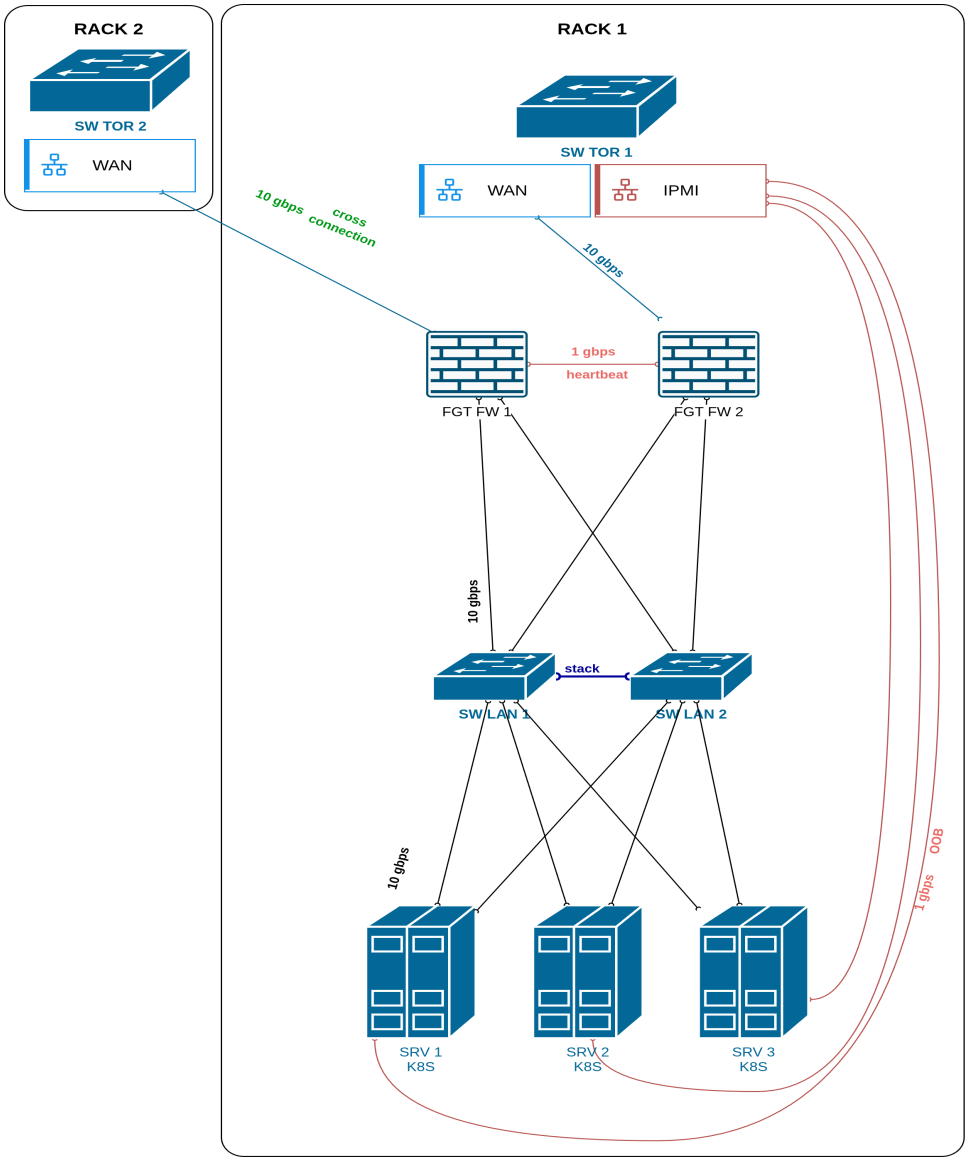
7. Estimativa da demanda - quantidade de bens e serviços

Infraestrutura necessária para atendimento da demanda

Considerando a situação atual da infraestrutura do Datacenter institucional, a limitação operacional identificada no ambiente hiperconvergente em uso, a proximidade do esgotamento da capacidade de memória e armazenamento, bem como a urgência associada ao cronograma dos processos seletivos de 2026, mostra-se necessária a contratação de solução de infraestrutura de Tecnologia da Informação como Serviço (IaaS), em caráter transitório, para assegurar a continuidade das atividades do CEPS e a entrada em produção do Novo Sistema de Gestão de Processos Seletivos.

O modelo proposto também se mostra aderente ao cenário institucional, pois possibilita a rápida disponibilização do ambiente, sem a necessidade de aguardar a conclusão do processo estrutural de modernização do Datacenter da UNIFESSPA, que já se encontra em curso, mas ainda não apresenta condições de atender, em tempo hábil, à demanda imediata do CEPS.

Infraestrutura necessária para manter os serviços funcionando:

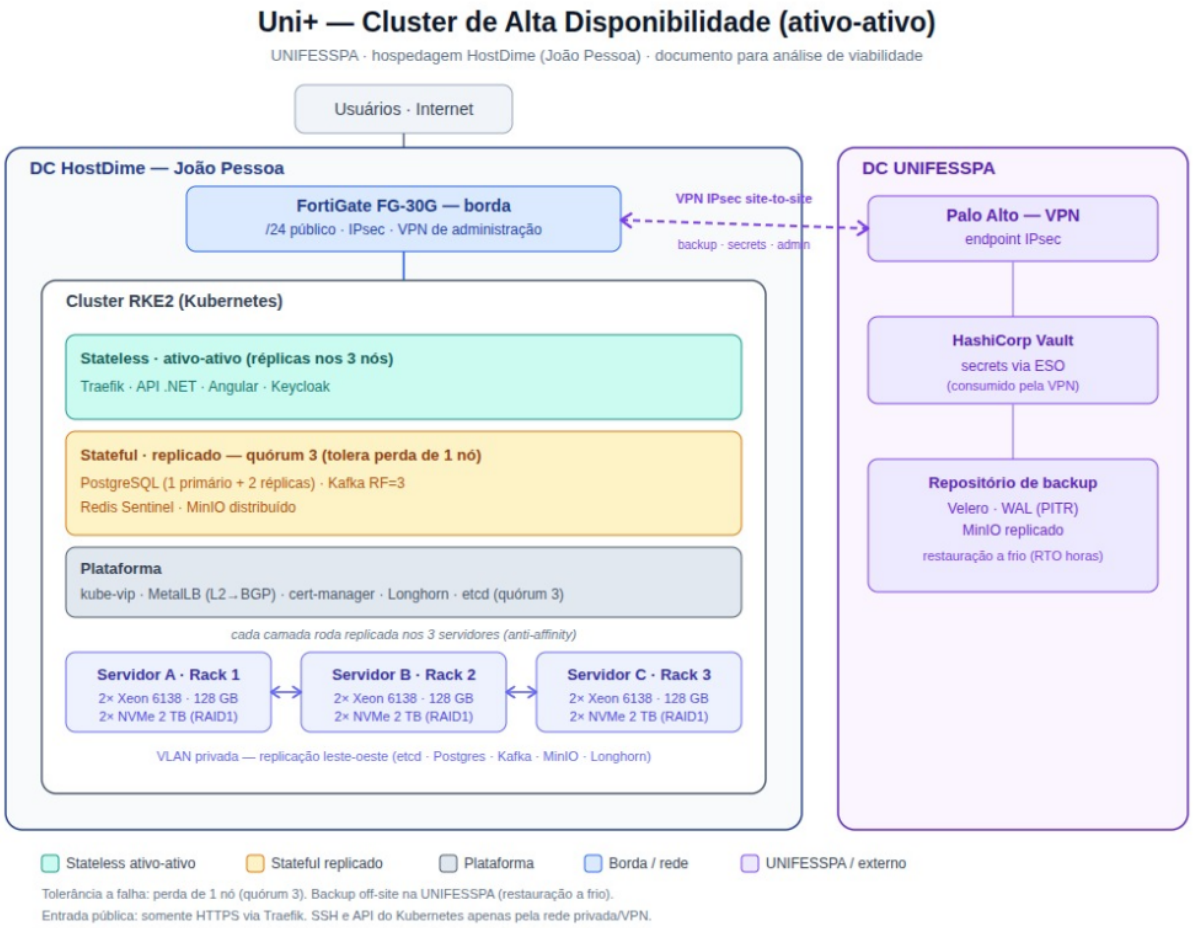


A necessidade da contratação não se resume à locação isolada de hardware, hospedagem ou conectividade, mas à disponibilização de solução integrada de infraestrutura de TIC, composta por recursos dedicados de computação, conectividade IP, segurança perimetral, monitoramento, SOC & SIEM, backup corporativo e suporte contínuo, estruturados para atendimento simultâneo de requisitos operacionais, de disponibilidade, de segurança e de continuidade vinculados à necessidade institucional da UNIFESSPA.

A contratação pretendida fundamenta-se, portanto, na necessidade de prover solução integrada de infraestrutura de tecnologia da informação como serviço (IaaS), com recursos dedicados de computação, conectividade IP, segurança perimetral, backup corporativo e suporte contínuo, indispensáveis à operação do Novo Sistema de Gestão de Processos Seletivos do CEPS/UNIFESSPA. A solução foi definida com base em requisitos técnicos, de segurança e de disponibilidade compatíveis com a criticidade do serviço institucional, não se confundindo com contratação genérica de hospedagem ou de servidor isolado.

Diante da combinação específica de requisitos operacionais, de segurança, de conectividade, de backup e de suporte, entende-se configurada a inviabilidade de solução padronizada que não atenda, de forma simultânea e integral, às condições do caso concreto. A escolha do fornecedor deverá ser demonstrada por documentação técnica e pesquisa de mercado que comprovem a aderência da solução ofertada às necessidades da Administração e a compatibilidade do preço com o mercado.

A imagem abaixo ilustra o funcionamento da infraestrutura proposta pela empresa HostDime, evidenciando a organização dos componentes de computação, conectividade, segurança e continuidade operacional.



Quantitativos estimados

A estimativa da demanda foi elaborada com base na **modelagem das necessidades institucionais**, considerando os recursos necessários para garantir a continuidade, a estabilidade, a disponibilidade e o pleno funcionamento dos serviços relacionados ao Novo Sistema de Gestão de Processos Seletivos do CEPS/UNIFESSPA.

Para o dimensionamento da solução, foi utilizada como referência a **proposta comercial apresentada para disponibilização da infraestrutura necessária ao atendimento das necessidades do CEPS**, considerando os requisitos técnicos e operacionais definidos pela equipe de planejamento da contratação.

A partir da análise da demanda e dos requisitos estabelecidos, foram dimensionados os recursos e serviços necessários à adequada operação do ambiente computacional, contemplando os seguintes itens:

Item	Descrição resumida	Und.	Quantidade
1	Servidor Dedicado 2 CPU - Xeon Gold 6138	Und	3
2	Switch 24 portas 10 Gbps	Und	2
3	Bloco de IP /28 (BRA)	Und	1
4	Firewall - FN-FG-30G (Hardware)	Und	2
5	Firewall FN-FC-10-FG30G-950-02-12 (Licença)	Serv	2
6	Gerenciamento Full (24x7)	Serv	1
7	Acronis Backup (Workload) - storage inicial	Serv	1
8	Monitoramento Customizado (Adicional)	Serv	5
9	Acronis Backup (Workload) - storage ampliado	Serv	1
10	Setup (pagamento único)	Serv	1
11	Serviço de SOC & SIEM	Serv	1
11.1	SOC HDBR - UNIX Systems	Und	33
11.2	SOC HDBR - Firewalls External (GW)	Und	2

11.3	SOC HDBR - Switches	Und	2
11.4	SOC HDBR - VPN	Und	2
11.5	SOC HDBR - 51 a 200 EPS	Und	1
11.6	SOC HDBR - Storage contratado (pacote de 100 GB)	Und	4

Dessa forma, torna-se necessária a contratação de empresa especializada na prestação de serviços de infraestrutura de Tecnologia da Informação como Serviço (Infrastructure as a Service - IaaS), compreendendo o provimento de clusters de computação Bare Metal, conectividade IP dedicada, segurança perimetral avançada (NGFW), vault de backup corporativo, monitoramento SOC & SIEM e telemetria/suporte contínuo (NOC 24x7).

O escopo abrange a alocação de ativos lógicos e lógico-físicos em ambiente de missão crítica, no Data Center da Contratada, o qual dispõe de certificação construtiva Tier III (Uptime Institute) e de matriz de certificações operacionais e de Segurança da Informação da família ISO/IEC.

8. Levantamento de soluções

Foram identificadas, em tese, as seguintes soluções para atendimento da necessidade institucional:

Solução	Descrição
Solução 1	Manutenção da infraestrutura atual
Solução 2	Aquisição de servidor próprio para instalação local (on-premise)
Solução 3	Contratação de empresa especializada na prestação de serviços de infraestrutura de Tecnologia da Informação como Serviço
Solução 4	Contratação de infraestrutura em nuvem pública sob demanda

Contratações Públicas Similares

Órgão Contratante	Objeto do Contrato	Ano	Instrumento
CREA-PB	Serviços gerenciados de TI, com colocation, segurança de perímetro, armazenamento em nuvem privada, backup, firewall, monitoramento e suporte técnico.	2024	Contrato nº 19/2024.
SEBRAE/PB	Adequação da arquitetura de TIC para ampliar disponibilidade, segurança, armazenamento, backup, monitoramento e suporte avançado.	2022	Contrato nº 032-A/2022, firmado por inexigibilidade de licitação.
Tribunal de Justiça da Paraíba	Serviços de colocation e interconexão em datacenter, com foco em alta disponibilidade, segurança e conformidade regulatória.	2025	Contrato nº 030/2025, decorrente de inexigibilidade de licitação.
Polícia Militar da Paraíba	Infraestrutura de TIC como serviço, com servidores dedicados, IPs, switches, firewall, backup, monitoramento e gerenciamento.	2025	Contrato nº 0023/2025, firmado por inexigibilidade nº 0005/2025-AC.
Polícia Civil da Paraíba	Armazenamento de dados em nuvem privada e colocation, em ambiente de alta criticidade e longo prazo.	2025	Termo de Contrato Administrativo nº 0065 /2025/PCPB, decorrente de inexigibilidade nº 012/2025.

Existência de Software Livre ou Público

Não foram identificadas soluções compatíveis no catálogo de softwares públicos do Governo Federal que atendam aos requisitos da contratação.

Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil)

Não se aplica, pois o objeto da contratação não contempla funcionalidades relacionadas à identificação digital, autenticação ou certificação eletrônica.

9. Análise comparativa de soluções

Foram consideradas, para atendimento da necessidade do CEPS, as seguintes alternativas: manutenção da infraestrutura atualmente disponível; aquisição de servidor próprio para instalação local; contratação de solução de infraestrutura de Tecnologia da Informação como Serviço (IaaS) em datacenter terceirizado; e contratação de infraestrutura em nuvem pública.

A análise comparativa leva em consideração a situação atual da infraestrutura institucional, a urgência da demanda, o prazo necessário para disponibilização da solução, a complexidade de implantação, os riscos operacionais, a aderência técnica ao caso concreto e o impacto sobre a continuidade do serviço público.

9.1 Alternativa 1 – Manutenção da infraestrutura atual

A manutenção do cenário atual apresenta como principal vantagem a ausência de contratação imediata e, consequentemente, de desembolso financeiro adicional no curtíssimo prazo. Contudo, essa alternativa não se mostra apta a atender à necessidade do CEPS, uma vez que a infraestrutura vigente já opera com limitações relevantes de memória, armazenamento e margem de expansão, além de apresentar risco concreto de instabilidade em períodos de pico.

O diagnóstico institucional registra que o ambiente encontra-se próximo do limite operacional, com exposição a indisponibilidade, vulnerabilidade de dados e incompatibilidade com a carga esperada para os certames de 2026. Assim, a manutenção exclusiva da infraestrutura atual preserva os riscos já identificados, sem oferecer resposta adequada ao aumento de demanda nem às exigências de continuidade e segurança do novo sistema.

9.2 Alternativa 2 – Aquisição de servidor próprio

A aquisição de equipamento próprio representa solução patrimonialmente mais estruturante, por gerar ativo permanente e ampliar a autonomia administrativa sobre o ambiente computacional. Em tese, essa alternativa pode contribuir para redução de despesas recorrentes no longo prazo e está alinhada à estratégia institucional mais ampla de modernização da infraestrutura de TIC.

Entretanto, embora tecnicamente desejável como solução definitiva, a aquisição não se mostra adequada para atendimento imediato da demanda do CEPS. O processo de compra exige planejamento, especificação, seleção da solução, contratação, entrega, instalação, configuração, testes e entrada em produção, etapas que não se compatibilizam com a urgência do cronograma dos processos seletivos previstos para 2026.

Além disso, a solução definitiva estruturante para o Datacenter institucional já se encontra em fase de planejamento e instrução em processo próprio, o que reforça o caráter transitório da necessidade atual e reduz a conveniência de aquisição imediata de ativo isolado para suprimento temporário da demanda.

9.3 Alternativa 3 – Contratação de solução IaaS em datacenter terceirizado

A contratação de solução de infraestrutura de TIC como serviço apresenta como principal vantagem a rapidez de disponibilização do ambiente, fator decisivo diante da urgência do CEPS. A proposta analisada indica prazo de ativação compatível com a necessidade institucional, permitindo provisionamento e entrada em operação em tempo oportuno para apoiar migração, testes e operação assistida do novo sistema.

Sob a perspectiva operacional, essa alternativa reduz significativamente o tempo entre a contratação e a efetiva disponibilização do ambiente, viabilizando recursos dedicados de computação, conectividade IP, segurança perimetral, backup corporativo e monitoramento contínuo em uma única arquitetura contratual.

Como desvantagem, a contratação não gera ativo patrimonial para a Administração e implica dependência de fornecedor externo durante a vigência contratual. Ainda assim, tais limitações mostram-se proporcionais e administrativamente aceitáveis no contexto atual, pois a solução pretendida atua como medida transitória de continuidade enquanto não é concluído o processo estrutural de modernização da infraestrutura institucional.

9.4 Alternativa 4 – Contratação de infraestrutura em nuvem pública

A contratação em nuvem pública possui vantagens conhecidas, como elasticidade, escalabilidade e possibilidade de expansão sob demanda. Em tese, trata-se de solução moderna e tecnicamente adequada para cenários de consumo variável.

Contudo, para o caso concreto, essa alternativa tende a exigir maior esforço de definição arquitetural, ajustes de segurança, governança, integração e administração do ambiente, além de potencial variabilidade de custos conforme o perfil de uso. No cenário analisado, a nuvem pública não se mostra mais simples nem mais célere do que a solução IaaS dedicada previamente dimensionada, especialmente diante da necessidade de previsibilidade, integração dos componentes e ativação em prazo compatível com os certames previstos.

9.5 Conclusão da análise comparativa

À luz da situação atual da infraestrutura, da urgência da demanda e do contexto institucional, a contratação de solução de infraestrutura de TIC como serviço mostra-se a alternativa mais adequada para o atendimento imediato da necessidade do CEPS. A manutenção da infraestrutura atual não elimina os riscos já identificados; a aquisição de equipamento próprio, embora desejável como solução definitiva, não se conclui em tempo hábil; e a infraestrutura em nuvem pública, embora tecnicamente possível, envolve maior complexidade de governança e custo no cenário analisado.

Dessa forma, a locação/contratação de ambiente dedicado destaca-se por reunir rapidez de ativação, previsibilidade de custos, aderência técnica à demanda, menor complexidade de implantação e capacidade de funcionar como solução transitória até a consolidação da modernização definitiva da infraestrutura institucional.

9.6 Quadro sintético

Solução	**Vantagens**	**Desvantagens**	**Adequação à urgência**
Manutenção da infraestrutura atual	Sem contratação imediata.	Mantém riscos atuais, não suporta crescimento e compromete a estabilidade.	Baixa.
Aquisição de servidor próprio	Gera ativo patrimonial e autonomia de longo prazo.	Maior prazo de contratação, entrega e implantação.	Média/Baixa.
Solução IaaS em datacenter terceirizado	Implantação rápida, custo previsível, solução transitória e menor complexidade.	Não gera ativo e depende de fornecedor externo.	Alta.
Infraestrutura em nuvem pública	Elasticidade e escalabilidade.	Maior complexidade, custo variável e maior exigência de governança.	Média.

10. Registro de soluções consideradas inviáveis

Considera-se inviável, para a necessidade imediata do CEPS, a manutenção exclusiva da **infraestrutura atualmente disponível Solução 1**, uma vez que o ambiente institucional já opera com restrição severa de memória, crescimento contínuo de armazenamento e ativos em fim de vida útil, o que compromete a expansão segura do ambiente e aumenta o risco de indisponibilidade em períodos críticos.

Também não se revela viável, como solução imediata, a adoção exclusiva da **aquisição de servidores próprios - solução 2** sem medida transitória, pois a modernização estrutural do Datacenter institucional depende de processo mais amplo, já em andamento, cuja conclusão não ocorrerá em prazo compatível com o cronograma dos certames previstos para 2026.

A contratação exclusiva de infraestrutura em nuvem pública solução sob demanda, embora tecnicamente possível, foi considerada menos adequada no caso concreto em razão da maior complexidade de modelagem, necessidade de ajustes arquiteturais, governança mais intensiva, potencial variabilidade de custos e esforço adicional de administração, quando comparada a uma solução IaaS dedicada, previamente dimensionada e de rápida ativação.

11. Análise comparativa de custos (TCO)

A pesquisa de preços foi realizada com base em fontes distintas, priorizando contratações públicas similares registradas no Portal Nacional de Contratações Públicas — PNCP, complementadas por proposta comercial obtida diretamente com fornecedor. O procedimento adotado não consistiu na simples transcrição dos valores encontrados, mas na análise individualizada de cada contratação, com a finalidade de identificar, dentro dos respectivos contratos, os itens efetivamente similares aos serviços pretendidos pela Administração.

Essa cautela foi necessária porque as contratações consultadas apresentam objetos compostos, com diferentes níveis de abrangência, quantitativos, unidades de medida, prazos de vigência, requisitos técnicos e modelos de execução. Assim, foram selecionados somente os componentes compatíveis, total ou parcialmente, com a solução planejada, especialmente os serviços de infraestrutura como serviço — IaaS, implantação ou setup e serviço gerenciado de SOC/SIEM.

A pesquisa foi estruturada em conformidade com a necessidade descrita no Estudo Técnico Preliminar, na Especificação Técnica e no Termo de Referência, que definem uma solução integrada composta por infraestrutura computacional dedicada, conectividade, switches, segurança perimetral, backup, monitoramento, suporte técnico e serviços de segurança cibernética. O objeto não se confunde com uma contratação isolada de hospedagem, conectividade, servidor dedicado ou monitoramento, razão pela qual foi indispensável realizar o filtro técnico dos contratos analisados.

Metodologia utilizada

Para cada contratação pública consultada, foram examinados o objeto, o termo de referência, a composição dos itens, as condições de execução, os quantitativos, a unidade de fornecimento, a vigência contratual e os valores correspondentes. Após essa análise, foram identificados os itens com maior aderência às características da contratação pretendida.

O filtro aplicado considerou, entre outros, os seguintes critérios:

- Similaridade do serviço contratado com o objeto planejado.
- Compatibilidade entre a unidade de fornecimento e a unidade prevista na contratação.
- Correspondência entre os quantitativos e capacidades técnicas.
- Inclusão de infraestrutura, suporte, monitoramento, segurança, backup ou implantação.
- Regime de prestação continuada ou execução em parcela única.
- Prazo de vigência e periodicidade de faturamento.
- Existência de componentes que pudessem ser individualizados sem distorcer o preço.
- Necessidade de exclusão de itens estranhos ou não comparáveis ao objeto.

Os documentos destacados em laranja correspondem aos trechos e itens identificados como pertinentes à formação do preço estimado. O destaque teve a finalidade de facilitar a conferência, a rastreabilidade e a vinculação entre o valor utilizado na pesquisa e o documento originário que lhe dá suporte.

A documentação comprobatória foi anexada ao processo (documentos 42-45) justamente para demonstrar a origem dos preços, permitir a conferência dos valores considerados e evidenciar que os dados não foram utilizados de forma genérica ou dissociada do conteúdo dos contratos analisados.

Composição dos preços

A pesquisa resultou na seguinte composição:

Item	Descrição	Quantidade	Unidade	Valor unitário estimado	Valor total estimado
1	Solução integrada de infraestrutura de TIC como serviço — IaaS	60	Mensal	R$ 13.249,48	R$ 794.968,80
2	Setup de implantação da solução	1	Unidade	R$ 7.056,57	R$ 7.056,57
3	Serviço gerenciado de SOC/SIEM	30	Mensal	R$ 4.700,00	R$ 141.000,00
	Total estimado da contratação				**R$ 943.025,37**

Memória de cálculo

- Item 1: 60 meses × R$ 13.249,48 = **R$ 794.968,80**.
- Item 2: 1 unidade × R$ 7.056,57 = **R$ 7.056,57**.
- Item 3: 30 meses × R$ 4.700,00 = **R$ 141.000,00**.
- Total: R$ 794.968,80 + R$ 7.056,57 + R$ 141.000,00 = **R$ 943.025,37**.

Os valores constam do relatório de pesquisa de preços e do quadro sintético de preços estimados, documentos que devem ser considerados conjuntamente para fins de formalização do preço de referência.

Item 1 — Infraestrutura como Serviço

Para o Item 1, foram considerados quatro preços válidos, resultantes de proposta comercial e de contratações públicas localizadas em sistemas oficiais de governo. Os valores corrigidos identificados foram de R$ 12.339,77, R$ 12.444,95, R$ 13.936,05 e R$ 14.277,16.

A média simples dos preços válidos foi de R$ 13.249,48, valor utilizado como estimativa unitária mensal. O coeficiente de variação indicado no relatório foi de 7,55%, demonstrando dispersão relativamente reduzida entre os preços considerados e conferindo maior consistência ao valor médio adotado.

A similaridade do item decorre da presença conjunta de servidores dedicados, conectividade, switches, endereçamento IP, firewall, licenças, suporte, gerenciamento, backup e monitoramento. A proposta comercial da DIMENOC, por exemplo, apresentou a composição detalhada desses componentes, incluindo três servidores dedicados, switches de 10 Gbps, bloco IPv4, firewalls, gerenciamento 24x7, backup, monitoramento e demais elementos necessários à solução.

Também foi analisado o contrato celebrado pelo SEMAE de São Leopoldo, cujo objeto contempla serviços em nuvem no modelo IaaS, ambiente de datacenter virtual, hospedagem, redundância, alta disponibilidade, segurança, escalabilidade e resiliência, com vigência de 60 meses. Embora o escopo não seja integralmente idêntico ao da contratação pretendida, o contrato apresenta aderência suficiente em relação à infraestrutura como serviço e aos requisitos de continuidade e disponibilidade, razão pela qual foi utilizado como referência após o devido filtro técnico.

Item 2 — Setup de implantação

Para o Item 2, foram identificados quatro valores, dos quais três foram considerados válidos após a análise de consistência. Os preços válidos foram de R$ 5.994,00, R$ 6.940,52 e R$ 8.235,20.

O valor de R$ 15.734,25 foi classificado como excessivamente elevado e excluído da formação do preço estimado. Considerados os três preços válidos, a média simples resultou em R$ 7.056,57, valor adotado como estimativa unitária para a execução do setup.

O item compreende atividades que não se confundem com a prestação mensal da infraestrutura, abrangendo implantação, configuração, integração, testes, documentação e disponibilização inicial da solução. A separação desse componente evita que os custos de mobilização e implantação sejam indevidamente diluídos ou incorporados ao preço mensal continuado.

A pesquisa demonstrou, ainda, que a proposta comercial da DIMENOC apresentou valor específico de R$ 6.000,00 para o setup, o que confirma a existência de referência de mercado para a contratação desse serviço como parcela única.

Item 3 — SOC/SIEM

Para o Item 3, foram identificados quatro preços, sendo três considerados válidos e um excluído por apresentar valor excessivamente elevado. Os preços válidos foram de R$ 4.700,00, R$ 9.300,00 e R$ 4.408,00.

O valor de R$ 10.994,00 foi classificado como excessivamente elevado, conforme os critérios estabelecidos no relatório de pesquisa. Após a exclusão, o valor considerado para a estimativa foi de R$ 4.700,00 mensais, correspondente à mediana dos preços válidos e ao valor apresentado na proposta comercial analisada.

O serviço pesquisado envolve monitoramento e análise de eventos de segurança, coleta e correlação de logs, detecção de ameaças, classificação de alertas, comunicação de incidentes e apoio à resposta, abrangendo sistemas Unix/Linux, firewalls, switches, VPNs, capacidade de processamento de eventos e armazenamento de logs.

A proposta comercial utilizada como referência apresentou a composição do SOC/SIEM com cobrança global mensal de R$ 4.700,00, além do detalhamento dos elementos monitorados, como sistemas Unix, firewalls, switches, VPNs, capacidade de 51 a 200 EPS e armazenamento contratado.

Tratamento dos contratos similares

A utilização de contratos públicos similares foi considerada adequada porque permite observar preços efetivamente praticados ou contratados pela Administração Pública em objetos de natureza tecnológica semelhante. Entretanto, os valores não foram utilizados de forma automática, uma vez que cada contratação possui particularidades próprias.

O contrato do SEMAE de São Leopoldo, por exemplo, possui valor global de R$ 1.602.823,20 e preço mensal variável ao longo da vigência, além de contemplar infraestrutura em nuvem, colocation, backup, storage e requisitos específicos de datacenter. Por essa razão, sua utilização exigiu a identificação dos componentes efetivamente comparáveis, sem transferir para a presente contratação custos relativos a itens não previstos ou com características distintas.

Da mesma forma, o contrato da Câmara Municipal de Barreiras apresenta solução de conectividade híbrida com link dedicado, conexão via satélite, rádio digital, proteção Anti-DDoS, monitoramento NOC/SOC e bloco de IP público. Embora contenha elementos relacionados à conectividade e à segurança, não corresponde integralmente à solução IaaS ou ao SOC/SIEM pretendido, motivo pelo qual seus dados somente podem ser aproveitados nos aspectos tecnicamente compatíveis, e não como preço global da contratação.

Já o contrato do Município de Natal contempla suporte, manutenção sistêmica, infraestrutura em nuvem, backups e armazenamento, mas também inclui módulos de software e treinamentos presenciais. Dessa forma, os valores foram analisados de maneira segregada, evitando que componentes de desenvolvimento, licenciamento, manutenção de sistema ou capacitação fossem confundidos com os serviços de infraestrutura e segurança objeto desta contratação.

Esse procedimento preserva a comparabilidade, evita a formação de preços com base em objetos heterogêneos e demonstra que os valores foram extraídos somente dos componentes que guardam correspondência técnica e operacional com a solução planejada.

Conclusão da análise

Diante da análise realizada, conclui-se que a pesquisa de preços apresenta coerência com o objeto definido no ETP, na Especificação Técnica e no Termo de Referência, pois:

- Foram utilizadas contratações públicas similares divulgadas no PNCP e em sistemas oficiais de governo.

- Cada contratação foi analisada individualmente antes da utilização dos respectivos valores.
- Foi realizado filtro técnico para identificar os serviços efetivamente similares.
- Foram desconsiderados itens estranhos, incompatíveis ou sem correspondência suficiente com o objeto.
- Os destaques em laranja permitem localizar, nos documentos anexos, os itens utilizados na composição do preço.
- Os contratos e demais documentos comprobatórios foram anexados ao processo para assegurar a rastreabilidade e a conferência dos preços.
- Foram aplicados critérios de validação, exclusão de valores excessivos e definição da medida estatística adequada.
- O preço estimado global resultante foi de R$ R$ 943.025,37, sendo R$ 13.249,48 mensais para o Item 1, R$ 7.056,57 para o Item 2 e R$ 4.700,00 mensais para o Item 3.

Assim, os valores adotados podem ser utilizados como referência para a contratação, sem prejuízo da avaliação das propostas que vierem a ser apresentadas no procedimento competitivo, uma vez que a pesquisa representa uma estimativa de mercado baseada em referências documentais e não constitui garantia de que os preços finais da licitação serão idênticos aos valores estimados.

12. Descrição da solução de TIC a ser contratada

12.1 A solução foi estruturada em grupo único, composto por três itens funcionalmente relacionados, em razão da integração operacional entre a infraestrutura de TIC, as atividades de implantação e o monitoramento de segurança. A modelagem busca assegurar a unidade funcional do objeto, a adequada responsabilização pela execução, a continuidade dos serviços e a preservação da competitividade no procedimento licitatório.

A contratação compreende serviços continuados de infraestrutura de Tecnologia da Informação e Comunicação — TIC, em modelo de Infraestrutura como Serviço (Infrastructure as a Service — IaaS), serviço de implantação inicial e serviço gerenciado de Centro de Operações de Segurança — SOC, com Gestão de Informações e Eventos de Segurança — SIEM.

A solução destina-se à disponibilização de ambiente computacional seguro, dedicado, resiliente e continuamente monitorado para suporte aos sistemas institucionais da UNIFESSPA, especialmente aqueles relacionados aos processos seletivos e aos demais serviços cuja indisponibilidade possa comprometer a continuidade do serviço público, a segurança da informação, a integridade dos dados e a confiabilidade institucional.

A solução será composta pelos seguintes itens:

12.2 Item 1 — Solução integrada de infraestrutura de TIC como serviço — IaaS

O Item 1 compreende a prestação continuada de solução integrada de infraestrutura de TIC como serviço — IaaS, destinada à hospedagem e sustentação dos workloads institucionais da UNIFESSPA. A solução deverá operar em ambiente de missão crítica, hospedado em território nacional, e incluir todos os recursos, licenças, equipamentos, serviços, suporte e mão de obra necessários ao seu funcionamento integral.

O Item 1 consolida os componentes de infraestrutura que devem funcionar de maneira integrada, abrangendo capacidade computacional dedicada, conectividade, switches de rede, endereçamento IP público, segurança perimetral, licenças e suporte, gerenciamento técnico, backup corporativo e monitoramento. A composição da solução visa assegurar desempenho previsível, disponibilidade, escalabilidade, segurança e proteção dos ativos institucionais, sem necessidade de expansão imediata da infraestrutura física própria da Universidade.

Para fins de execução e faturamento, os componentes abaixo integram uma única solução mensal. Assim, não será admitida cobrança adicional por servidores, equipamentos, licenças, tráfego, endereçamento IP, backup, armazenamento, monitoramento, suporte, manutenção, substituição de hardware ou outros elementos indispensáveis ao atendimento do escopo contratado.

a) Servidores dedicados Bare Metal

A solução deverá disponibilizar 3 servidores dedicados Bare Metal, de uso exclusivo da UNIFESSPA, cada um com os seguintes requisitos mínimos:

- Dois processadores físicos, ou arquitetura equivalente ou superior, com desempenho agregado mínimo equivalente ao parâmetro de dois processadores Intel Xeon Gold 6138 e, no mínimo, 40 núcleos físicos por servidor.
- 128 GB de memória RAM DDR4 ou tecnologia superior.

- Duas unidades SSD NVMe de 2 TB cada, configuradas em RAID 1 por software, hardware ou solução tecnicamente equivalente que assegure redundância contra falha de uma unidade.

- Sistema operacional Ubuntu Server 24.04 LTS, versão LTS posterior ou distribuição Linux equivalente, previamente autorizada pela UNIFESSPA quando necessária.
- Porta de rede de 1 Gbps, com tráfego ilimitado ou solução tecnicamente equivalente que não imponha franquia de dados, cobrança adicional por uso ordinário ou limitação incompatível com a operação dos sistemas institucionais.
- Acesso administrativo root, ou mecanismo equivalente de administração plena, para a equipe formalmente autorizada pela UNIFESSPA, após a conclusão do setup e observados os controles de segurança aplicáveis.
- Recursos dedicados, vedado o compartilhamento de CPU, memória, armazenamento ou recursos críticos com outros clientes.
- Substituição de componentes defeituosos, incluindo memória, processador, unidades de armazenamento, fontes e demais componentes essenciais, em até 24 horas da identificação da falha ou abertura do chamado, sem ônus adicional à contratante.

b) Switches de rede

A solução deverá incluir 2 switches de rede, ou arquitetura equivalente, para integração dos servidores, dos firewalls e dos demais componentes da infraestrutura.

Cada switch deverá possuir, no mínimo:

- 24 portas de 10 Gbps, ou capacidade equivalente ou superior.
- Capacidade de operação em arquitetura Top-of-Rack, ou solução equivalente que assegure desempenho, disponibilidade e organização adequados do tráfego interno.
- Gerenciamento remoto seguro.
- Suporte a VLAN, agregação de links, segmentação lógica, redundância e demais recursos necessários à integração da solução.
- Manutenção, atualização, substituição e suporte sob responsabilidade da contratada durante toda a vigência.

c) Bloco IPv4 público

A solução deverá incluir 1 bloco IPv4 público /28, contendo 16 endereços, dos quais no mínimo 14 deverão estar disponíveis para utilização pela UNIFESSPA.

O fornecimento deverá contemplar roteamento, delegação, documentação e suporte operacional, de modo a permitir a publicação dos serviços institucionais, a comunicação externa e a segregação lógica dos componentes da solução.

d) Segurança perimetral em alta disponibilidade

A solução deverá incluir 2 appliances de firewall de próxima geração — NGFW, ou solução tecnicamente equivalente, configurados em cluster de alta disponibilidade, com failover automático ou mecanismo equivalente.

A camada de segurança perimetral deverá possuir capacidade compatível com a banda contratada, o volume de conexões previsto e os requisitos de disponibilidade do ambiente, contemplando, no mínimo:

- Inspeção e controle de tráfego.
- Aplicação de políticas de acesso e segmentação.
- NAT e publicação segura de serviços.
- VPN segura.
- Prevenção, detecção ou mitigação de intrusões e ameaças.
- Proteção anti-DDoS própria ou integração com serviço equivalente.
- Administração segura, controle de acesso e trilha de auditoria.
- Registro e exportação de eventos para integração com a solução de SOC & SIEM.
- Atualização de firmware, correções de vulnerabilidades, assinaturas e bases de segurança durante toda a vigência.

- Testes documentados de failover, na implantação e sempre que solicitado pela UNIFESSPA.

e) Licenças, assinaturas e suporte de firewall

Deverão estar incluídas todas as licenças, subscrições, assinaturas, atualizações, garantias e serviços de suporte necessários à utilização plena dos firewalls e de suas funcionalidades de segurança durante toda a vigência contratual.

A eventual referência comercial a modelo, SKU ou fabricante constante da pesquisa de preços deverá ser considerada exclusivamente como parâmetro de capacidade e funcionalidade. Serão aceitas soluções equivalentes ou superiores que comprovem aderência integral aos requisitos técnicos, de desempenho, segurança e disponibilidade estabelecidos neste Termo de Referência e na Especificação Técnica.

f) Gerenciamento técnico e NOC 24x7

A contratada deverá disponibilizar serviço de gerenciamento técnico e Centro de Operações de Rede — NOC, em regime de atendimento 24 horas por dia, 7 dias por semana e 365 dias por ano.

O serviço deverá contemplar, no mínimo:

- Atendimento técnico 24x7x365, por meios eletrônicos e telefônicos.
- Operação assistida dos servidores, sistemas operacionais, conectividade, switches, componentes de segurança, backup e monitoramento, conforme a matriz de responsabilidades definida pela UNIFESSPA.
- Franquia mínima de 10 horas mensais para configurações em nível de sistema operacional, ajustes, troubleshooting, otimizações e atividades correlatas.
- Sistema estruturado de abertura, acompanhamento e encerramento de chamados, abrangendo incidentes, problemas, mudanças e requisições.
- Registro das atividades executadas, responsáveis, horários, evidências, providências adotadas e resultados.
- Escalonamento técnico para incidentes críticos.
- Apoio à fiscalização contratual e à elaboração dos relatórios mensais de execução.

g) Backup corporativo

A solução deverá incluir serviço de backup corporativo para proteção dos 3 servidores físicos integrantes da infraestrutura, incluindo licenças, gerenciamento, suporte, políticas de backup, relatórios e capacidade de armazenamento mínima de 4.000 GB.

A solução de backup deverá:

- Proteger integralmente os 3 servidores físicos contratados.
- Disponibilizar armazenamento total mínimo de 4.000 GB em infraestrutura sob responsabilidade da contratada.
- Manter o destino de backup em local distinto do ambiente produtivo principal e em território nacional.
- Permitir a definição de políticas de frequência, retenção, restauração, exclusões e janelas de execução, de acordo com as necessidades da UNIFESSPA.
- Disponibilizar criptografia dos dados em trânsito e em repouso, quando tecnicamente aplicável.
- Permitir restauração de arquivos, diretórios, volumes e sistemas, de acordo com as funcionalidades da solução ofertada.
- Registrar os resultados de execução, falhas, retenções, restaurações, capacidade utilizada e capacidade disponível.
- Realizar testes de restauração, no mínimo trimestralmente ou conforme estabelecido no plano de continuidade, emitindo as respectivas evidências.
- Emitir relatórios mensais sobre o status dos backups, falhas identificadas, providências corretivas, restaurações realizadas e utilização do armazenamento.

Os componentes de proteção de workloads e de capacidade de armazenamento de backup integram o preço mensal único do Item 1, não sendo objeto de faturamento separado.

h) Monitoramento de infraestrutura

A solução deverá incluir monitoramento contínuo dos componentes críticos da infraestrutura, incluindo servidores, conectividade, switches, firewalls, armazenamento, backup e demais ativos definidos pela UNIFESSPA.

O serviço de monitoramento deverá contemplar:

- Dashboard autenticado ou mecanismo equivalente para visualização de métricas, eventos e alertas relevantes.
- Monitoramento de disponibilidade, desempenho, capacidade, utilização de CPU, memória, armazenamento, interfaces de rede, serviços críticos e demais indicadores aplicáveis.
- Alertas por correio eletrônico, sistema eletrônico, SMS, ligação telefônica, aplicativo de mensagens ou canais definidos no plano de comunicação.
- Capacidade de monitorar, no mínimo, 5 dispositivos adicionais além dos componentes básicos da solução.
- Registro de abertura, tratamento, escalonamento e encerramento dos eventos detectados.
- Integração com o NOC e, quando aplicável, com o SOC & SIEM.
- Emissão de relatórios mensais de disponibilidade, incidentes, eventos relevantes e ações adotadas.

12.3 Item 2 — Setup de implantação

O Item 2 corresponde à etapa não recorrente de implantação da solução de infraestrutura prevista no Item 1. Trata-se de serviço de pagamento único, necessário à preparação do ambiente para início da operação, compreendendo o provisionamento dos recursos físicos e lógicos, a configuração da rede e do endereçamento, a implantação da segurança perimetral em alta disponibilidade, a ativação das rotinas de backup e monitoramento, os testes de funcionamento e a entrega da documentação técnica inicial.

O prazo máximo para conclusão do setup será de até 30 dias úteis, contados da emissão da Ordem de Serviço, admitida a oferta de prazo inferior pela contratada, desde que preservados todos os requisitos de qualidade, segurança e aceite.

O serviço de setup deverá contemplar, no mínimo:

- Provisionamento físico e lógico dos servidores dedicados Bare Metal.
- Instalação, atualização e configuração inicial do sistema operacional.
- Configuração do armazenamento, da redundância dos discos, das interfaces e dos parâmetros básicos de segurança.
- Configuração dos switches, uplinks, VLANs, sub-redes, segmentação lógica e bloco IPv4 público /28.
- Implantação dos firewalls NGFW em alta disponibilidade, incluindo cluster, failover, rotas, NAT, políticas iniciais, VPNs, logs e controles de acesso.
- Habilitação e configuração das licenças, assinaturas e serviços de segurança.
- Implantação das políticas iniciais de backup, configuração do destino de armazenamento, retenção, criptografia e testes de restauração.
- Configuração do monitoramento, dashboards, sensores, alertas e integração com o NOC.
- Preparação dos mecanismos necessários à integração das fontes de logs e eventos com o serviço de SOC & SIEM do Item 3.
- Entrega controlada das credenciais administrativas dos servidores e das interfaces de gestão de firewall à equipe autorizada pela UNIFESSPA.
- Execução de testes de conectividade, desempenho, redundância, failover, firewall, rotas, backup, restauração, monitoramento e alertas.
- Entrega de diagrama lógico, inventário de ativos, endereçamento, matriz de acessos, relatório de testes, plano de manutenção preventiva e plano de contingência.
- Realização de reunião inicial de alinhamento com a equipe de fiscalização e os responsáveis técnicos designados pela UNIFESSPA.

O pagamento do Item 2 ocorrerá em parcela única, somente após a conclusão das atividades, a apresentação das evidências dos testes, a entrega da documentação técnica exigida e o ateste da fiscalização técnica.

12.4. Item 3 — Serviço gerenciado de SOC & SIEM

O Item 3 complementa a solução com serviço gerenciado de Centro de Operações de Segurança — SOC e Gestão de Informações e Eventos de Segurança — SIEM, voltado ao monitoramento centralizado, à coleta, normalização, correlação, armazenamento e análise de logs, à detecção de ameaças, à classificação de alertas e ao apoio à resposta a incidentes de segurança.

O serviço será prestado durante 30 meses e deverá abranger, no mínimo, as seguintes fontes e capacidades:

Componente monitorado ou capacidade	Quantidade mínima	Unidade de referência
Sistemas UNIX/Linux monitorados	33	ativo
Firewalls externos/gateways monitorados	2	ativo
Switches monitorados	2	ativo
VPNs ou concentradores VPN monitorados	2	ativo
Capacidade de processamento de eventos	Entre 51 e 200	EPS
Armazenamento de logs	400	GB

O armazenamento mínimo de 400 GB corresponde à capacidade de 4 pacotes de 100 GB. Os quantitativos de ativos, EPS e armazenamento constituem requisitos mínimos de capacidade e de composição do preço mensal do Item 3, não sendo admitida cobrança separada ou em duplicidade por esses elementos dentro dos limites contratados.

A contratada deverá, no mínimo:

- Coletar, normalizar, correlacionar, indexar e armazenar logs dos ativos e fontes definidos.
- Operar o monitoramento de segurança em regime compatível com os níveis de serviço contratados.
- Identificar, classificar e priorizar alertas por severidade, criticidade, impacto, urgência e categoria.
- Comunicar incidentes críticos à UNIFESSPA em até 60 minutos da identificação do evento ou da confirmação do alerta crítico.
- Registrar os incidentes e manter acompanhamento por meio de sistema de tickets, portal, correio eletrônico ou outro mecanismo formal definido pela UNIFESSPA.
- Produzir relatórios mensais de eventos, alertas, incidentes, fontes monitoradas, capacidade de EPS, armazenamento utilizado, indicadores de atendimento e recomendações de melhoria.
- Manter trilhas de auditoria, integridade dos logs, controles de acesso e evidências necessárias à investigação de incidentes.
- Apoiar a investigação, a contenção, a mitigação, a recuperação e a resposta a incidentes, dentro dos limites de responsabilidade previstos no contrato.
- Disponibilizar à fiscalização informações, relatórios e evidências necessárias ao acompanhamento da execução e à transição contratual.

A contratada do Item 3 deverá integrar o SOC & SIEM às fontes de logs e eventos disponibilizadas na solução de infraestrutura. A contratada responsável pelos Itens 1 e 2 deverá cooperar para disponibilizar os mecanismos técnicos necessários à integração, tais como conectividade, Syslog, APIs, agentes, coletores, regras de firewall, portas, rotas, acessos controlados e documentação pertinente, observados os princípios de segurança, necessidade de conhecimento e privilégio mínimo.

12.5 CICLO DE VIDA DO OBJETO:

12.5.1 Fase de Implantação: Compreende o provisionamento físico e lógico dos servidores Bare Metal, a configuração das sub-redes (bloco /28), o deploy dos firewalls em Alta Disponibilidade (HA) e a criação das políticas de backup. Este setup deverá ocorrer em até 30 (trinta) dias úteis.

12.5.2. Disponibilizar espaço físico padronizado em datacenter certificado (mínimo Tier III), para a prestação dos serviços à UNIFESSPA;

12.5.3. Estabelecer a infraestrutura elétrica redundante (UPS, gerador, PDU gerenciável), climatização de precisão, segurança física e conectividade com dupla abordagem;

12.5.4. Elaborar e entregar plano de manutenção preventiva e plano de contingência.

12.5.5 Fase de Operação: Abrange o monitoramento contínuo (24x7) de ativos, conectividade, segurança perimetral (UTM/NGFW) e a gestão de incidentes operada pelo NOC da Contratada, visando assegurar os indicadores de Acordo de Nível de Serviço (SLA).

12.5.6. Garantir o funcionamento ininterrupto da infraestrutura, com atendimento aos Acordos de Nível de Serviço (SLA) definidos em contrato;

12.5.7. Fornecer suporte técnico 24x7x365, com tempo máximo de resposta de até 60 minutos para incidentes críticos;

12.5.8. Realizar monitoramento proativo, emissão de alertas e relatórios mensais de disponibilidade, desempenho e incidentes;

12.5.9. Assegurar a integridade, confidencialidade e disponibilidade das informações e conexões, em conformidade com a Lei Geral de Proteção de Dados (LGPD), ISO 27001 e ISO 27701.

12.5.10 Fase de Transição e Encerramento: Contempla a rotina de desmobilização ao final do contrato. A Contratada deverá viabilizar o *take-out* seguro dos dados, garantindo o apagamento irreversível (*wipe* criptográfico) dos discos físicos (NVMe), para proteção de informações sigilosas da Universidade.

12.5.11. Executar plano de transição previamente aprovado pela UNIFESSPA, com prazo máximo de 90 (noventa) dias corridos;

12.5.12. Restituir todos os dados operacionais da UNIFESSPA, sem retenção de informações ou impedimentos de acesso;

12.5.13. Encerrar os acessos, remover perfis de usuários e entregar todos os registros técnicos, relatórios, diagramas e documentações relevantes;

12.5.14. Cumprir integralmente os requisitos de sigilo, segurança da informação e confidencialidade.

12.5.15. Durante todo o ciclo de vida da contratação, deverão ser observadas práticas sustentáveis e alinhadas às normas da Administração Pública, tais como:

12.5.15.1. Otimização do consumo energético do datacenter;

12.5.15.2. Redução de resíduos sólidos mediante uso de documentação digital e logística reversa para materiais substituídos;

12.5.15.3. Utilização de tecnologias eficientes e certificações ambientais;

12.5.15.4. Adoção de diretrizes previstas pela UNIFESSPA.

Tabela de quantitativos

Item	Descrição resumida	Und.	Quantidade
1	Servidor Dedicado 2 CPU - Xeon Gold 6138	Und	3
2	Switch 24 portas 10 Gbps	Und	2
3	Bloco de IP /28 (BRA)	Und	1
4	Firewall (Hardware)	Und	2
5	Firewall (Licença)	Serv	2
6	Gerenciamento Full (24x7)	Serv	1
7	Backup corporativo (Workload) - storage inicial	Serv	1
8	Monitoramento Customizado (Adicional)	Serv	5
9	Backup corporativo (Workload) - storage ampliado	Serv	1
10	Setup (pagamento único)	Serv	1
11	Serviço de SOC & SIEM	Serv	1
11.1	SOC HDBR - UNIX Systems	Und	33
11.2	SOC HDBR - Firewalls External (GW)	Und	2
11.3	SOC HDBR - Switches	Und	2
11.4	SOC HDBR - VPN	Und	2
11.5	SOC HDBR - 51 a 200 EPS	Und	1
11.6	SOC HDBR - Storage contratado (pacote de 100 GB)	Und	4

13. Estimativa de custo total da contratação

Valor (R$): 943.025,37

O custo estimado da contratação é de **R$ 943.025,37 (novecentos e quarenta e três mil, vinte e cinco reais e trinta e sete centavos),** conforme os valores unitários e totais constantes do Quadro Sintético de Preços Estimados.

14. Justificativa técnica da escolha da solução

14.1 Benefícios esperados

A contratação deverá proporcionar:

- disponibilidade de ambiente computacional dedicado e supervisionado;
- desempenho previsível, com redução de interferências decorrentes de compartilhamento indiscriminado de recursos;
- maior estabilidade de conectividade e publicação dos serviços institucionais;
- ampliação da capacidade de absorção de picos de acesso;
- segurança perimetral, monitoramento e detecção de eventos;
- backup corporativo, restauração e proteção de dados institucionais;
- suporte 24x7 e resposta coordenada a incidentes;
- previsibilidade de custos e redução da necessidade de aporte imediato em ativos físicos;
- apoio à migração, aos testes, à operação assistida e à entrada em produção do Novo Sistema de Gestão de Processos Seletivos;
- mitigação de riscos à continuidade do serviço público e à lisura dos certames.

14.2 Crescimento da demanda e eficiência operacional

O volume e a complexidade dos dados acadêmicos, administrativos e relacionados aos processos seletivos encontram-se em expansão. A infraestrutura deve absorver novos fluxos de trabalho sem interrupção dos serviços e sem investimentos iniciais elevados em ativos próprios.

A solução em IaaS, sob gerenciamento técnico especializado, reduz a necessidade de gestão física de hardware, substituição de componentes depreciados, expansão local de rede e manutenção de ativos legados. O modelo converte parte relevante das despesas de capital em despesas operacionais previsíveis, com níveis de serviço, responsabilidades e mecanismos de fiscalização definidos contratualmente.

14.3 Segurança, conformidade e disponibilidade

A solução deverá observar a Lei nº 13.709/2018, a Política de Segurança da Informação da UNIFESSPA e os princípios de confidencialidade, integridade, disponibilidade, rastreabilidade, necessidade e proteção de dados pessoais.

O ambiente deverá possuir controles compatíveis com segurança da informação, privacidade, continuidade de negócios, monitoramento, gestão de incidentes, SOC & SIEM, backup e restauração.

A infraestrutura dedicada, operada em ambiente de alta disponibilidade, deverá assegurar redundância de energia, climatização, conectividade e controles de acesso físico, reduzindo riscos de falhas e sustentando a operação dos sistemas críticos.

14.1 Justificativa para a vigência plurianual

A vigência plurianual é tecnicamente adequada e economicamente vantajosa diante da natureza continuada do serviço de gerenciamento e supervisão de infraestrutura de TIC, da necessidade de continuidade do ambiente e da conveniência de evitar sucessivas transições de curto prazo em operação crítica.

A proposta comercial prevê vigência de até 60 meses para os item 1 e de 30 meses para o item 2 . A infraestrutura principal apresenta custo de implantação, provisionamento, integração e alocação inicial que pode ser diluído em prazo mais extenso, reduzindo o impacto mensal e favorecendo a previsibilidade orçamentária.

A vigência plurianual deverá observar o art. 106 da Lei nº 14.133/2021, com demonstração da maior vantagem econômica, indicação de créditos orçamentários e previsão contratual de extinção sem ônus nas hipóteses legais aplicáveis.

A solução também se justifica pelo cenário transitório da infraestrutura institucional. Embora esteja em curso processo de modernização do Data Center próprio, não há previsão segura de conclusão em prazo compatível com a necessidade imediata do CEPS.

A prorrogação futura não constitui direito subjetivo da contratada. Dependerá da permanência da necessidade administrativa, da vantajosidade econômica, da qualidade da execução, da disponibilidade de recursos e da decisão motivada da autoridade competente.

14.14 Justificativa para o não parcelamento

A solução possui natureza integrada e funcionalmente indivisível composta por: Servidores, switches, conectividade, firewall, backup, monitoramento, SOC & SIEM e suporte devem operar sob arquitetura e supervisão coordenadas para produzir o resultado técnico finalístico.

O parcelamento aumentaria o número de interfaces contratuais, fragmentaria responsabilidades, dificultaria a gestão de incidentes, ampliaria riscos de incompatibilidade, reduziria a efetividade da fiscalização e poderia elevar os custos totais da solução.

A não adoção do parcelamento decorre, portanto, da necessidade de preservar a integração operacional, a continuidade do serviço, a responsabilidade técnica coordenada e a eficiência da gestão contratual.

14.15 Justificativa das exigências de qualificação econômico-financeira

A qualificação econômico-financeira tem por finalidade demonstrar que a futura contratada possui capacidade patrimonial e financeira suficiente para suportar as obrigações assumidas durante a execução do contrato, preservando a continuidade do serviço público e reduzindo riscos de interrupção, insolvência, descapitalização ou incapacidade de manutenção da infraestrutura disponibilizada.

No caso concreto, a exigência possui especial relevância porque o objeto compreende prestação continuada e crítica, com infraestrutura de Data Center, servidores dedicados, switches, firewall, licenças, conectividade, backup, monitoramento, NOC, SOC & SIEM e suporte técnico 24x7. A contratada deverá manter, durante toda a vigência, recursos tecnológicos, equipe especializada, processos operacionais, capacidade de reposição de componentes, obrigações perante fabricantes e fornecedores, controles de segurança, rotinas de backup e resposta a incidentes.

A eventual incapacidade econômico-financeira da contratada comprometeria diretamente a disponibilidade da solução e poderia resultar em degradação de serviços, atraso na substituição de ativos, descontinuidade de suporte, falha de renovação de licenças, insuficiência de recursos para resposta a incidentes, perda de capacidade de backup ou interrupção de componentes essenciais ao ambiente computacional do CEPS.

Por esse motivo, as exigências de qualificação econômico-financeira são adequadas, pertinentes, proporcionais ao risco da contratação e vinculadas à necessidade de assegurar a execução integral do objeto.

As exigências econômico-financeiras previstas são compatíveis com:

- o caráter continuado do serviço;
- a vigência plurianual da infraestrutura principal;
- a criticidade operacional do ambiente de processos seletivos;
- a necessidade de suporte e monitoramento ininterruptos;
- a manutenção de recursos dedicados e de alta disponibilidade;
- a obrigação de substituição de hardware em prazo reduzido;
- os níveis mínimos de serviço contratados;
- a manutenção de licenças, backup, conectividade, segurança e SOC & SIEM;
- a necessidade de continuidade e transição segura ao término contratual.

A documentação contábil, a certidão negativa de falência, os índices financeiros e o patrimônio líquido mínimo subsidiário são, portanto, instrumentos adequados para verificar a capacidade da futura contratada de manter, com estabilidade econômica, todos os recursos necessários à execução do objeto.

Tais exigências não substituem a demonstração de notória especialização, mas a complementam, pois asseguram que a empresa tecnicamente apta também possui condições econômico-financeiras para suportar a execução do serviço durante sua vigência.

14.16 Justificativa para a Exigência de Qualificação Técnica

A exigência de qualificação técnica na presente licitação decorre da natureza crítica, continuada e integrada dos serviços de infraestrutura de Tecnologia da Informação como Serviço – IaaS objeto da contratação, destinados a suportar o Novo Sistema de Gestão de Processos Seletivos do CEPS /UNIFESSPA e demais serviços institucionais de elevada criticidade.

A solução compreende a disponibilização e operação continuada de ambiente de infraestrutura em modelo IaaS, abrangendo servidores dedicados Bare Metal, conectividade IP dedicada, switches, segurança perimetral por firewall de próxima geração em alta disponibilidade, backup corporativo, monitoramento de infraestrutura, gerenciamento técnico e operação de NOC em regime 24x7, além de serviço gerenciado de SOC/SIEM para coleta, correlação, análise de logs, detecção de ameaças e apoio à resposta a incidentes de segurança.

A contratação não se confunde com fornecimento isolado de hospedagem, conectividade ou servidores, mas consiste em solução integrada de infraestrutura e serviços gerenciados, com requisitos objetivos de desempenho, disponibilidade, segurança, continuidade e suporte técnico, operando em ambiente de missão crítica, com SLA de infraestrutura de datacenter de 99,98% mensal, disponibilidade de rede de 99,50% mensal e tempo máximo de resposta de 60 minutos para incidentes críticos.

Nesse contexto, a qualificação técnica mostra-se necessária e proporcional para assegurar que a futura contratada possua capacidade operacional comprovada para:

- implantar, operar e manter infraestrutura dedicada de TIC em ambiente de datacenter profissional, com certificação Tier III ou equivalente, garantindo redundância de energia, climatização, segurança física e conectividade;
- prover e gerenciar servidores dedicados Bare Metal, switches, conectividade IP, segurança perimetral NGFW, backup corporativo e monitoramento contínuo, em conformidade com os níveis mínimos de serviço estabelecidos;
- operar NOC em regime 24x7x365, com equipe técnica capacitada, sistema estruturado de tickets, escalonamento para incidentes críticos e atendimento a prazos de resposta compatíveis com a criticidade dos serviços;
- executar serviço gerenciado de SOC/SIEM, com coleta, normalização, correlação e análise de logs, detecção e classificação de alertas, comunicação de incidentes e apoio à resposta a eventos de segurança;
- cumprir requisitos de segurança da informação, proteção de dados e continuidade de negócios, em conformidade com a LGPD, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 e ISO/IEC 27701, conforme aplicável ao escopo;
- executar plano de implantação (setup) em até 30 dias úteis, incluindo provisionamento físico e lógico, configuração de rede e segurança, implantação de backup e monitoramento, testes de funcionamento e entrega de documentação técnica;
- conduzir rotinas de transição e encerramento contratual, com restituição integral dos dados, eliminação segura de informações remanescentes e desmobilização do ambiente em até 90 dias corridos.

A ausência de comprovação de experiência prévia em serviços de complexidade equivalente elevaria significativamente os riscos de indisponibilidade, falhas de implantação, descumprimento de SLA, comprometimento da segurança da informação e prejuízos à continuidade dos processos seletivos, com impactos diretos à lisura dos certames, à imagem institucional e ao interesse público.

A qualificação técnica, portanto, não tem por finalidade restringir indevidamente a competição, mas assegurar que os licitantes possuam capacidade efetiva para executar serviços de infraestrutura de TIC em ambiente crítico, com requisitos de disponibilidade, segurança, monitoramento, suporte e resposta a incidentes compatíveis com as necessidades do CEPS/UNIFESSPA, em estrita observância aos princípios da legalidade, impessoalidade, moralidade, publicidade, eficiência, competitividade e seleção da proposta mais vantajosa.

Dessa forma, a exigência de atestados de capacidade técnica que demonstrem experiência em serviços similares, de complexidade tecnológica e operacional equivalente ou superior, mostra-se pertinente, proporcional e suficiente à execução do objeto, nos termos do art. 67 e seguintes da Lei nº 14.133/2021, devendo ser admitida a comprovação por serviços que envolvam gerenciamento, operação, suporte, monitoramento ou supervisão de infraestrutura de TIC, incluindo ambientes IaaS, servidores dedicados, conectividade, segurança perimetral, backup, NOC e SOC/SIEM, vedada a exigência de marca, modelo, fabricante ou experiência exclusiva em tecnologia proprietária.

14.17 da adoção do Sistema de Registro de Preços

Não se aplica a presente contratação

15. Justificativa econômica da escolha da solução

Sob a perspectiva econômica, a solução apresenta custo previamente dimensionado, pagamento mensal previsível e escopo técnico claramente definido, o que favorece planejamento orçamentário e controle da execução contratual. Em comparação com alternativas que exigiriam aquisição patrimonial, expansão física local, licenciamento adicional, esforço de implantação ou custos variáveis de consumo, a solução IaaS dedicada apresenta melhor relação entre custo, prazo e risco para o atendimento transitório da demanda.

16. Benefícios a serem alcançados com a contratação

A contratação deverá proporcionar:

- disponibilidade de ambiente computacional dedicado e supervisionado;
- desempenho previsível, com redução de interferências decorrentes de compartilhamento indiscriminado de recursos;
- maior estabilidade de conectividade e publicação dos serviços institucionais;
- ampliação da capacidade de absorção de picos de acesso;
- segurança perimetral, monitoramento e detecção de eventos;
- backup corporativo, restauração e proteção de dados institucionais;
- suporte 24x7 e resposta coordenada a incidentes;
- previsibilidade de custos e redução da necessidade de aporte imediato em ativos físicos;
- apoio à migração, aos testes, à operação assistida e à entrada em produção do Novo Sistema de Gestão de Processos Seletivos;
- mitigação de riscos à continuidade do serviço público e à lisura dos certames.

17. Providências a serem Adotadas

Antes da formalização da contratação, recomenda-se a adoção das seguintes providências:

- concluir a revisão do Termo de Referência para alinhamento integral entre ETP, proposta de referência e modelo de execução contratual;
- consolidar a pesquisa de preços e a memória de cálculo da vantajosidade econômica da solução;
- validar, pela área técnica, a topologia da solução, o plano de implantação, a estratégia de backup e o fluxo de suporte/NOC;
- definir os responsáveis pela fiscalização técnica, requisitante e administrativa do contrato;
- preparar o plano de transição, migração inicial e critérios de aceite para ativação do ambiente.

18. Declaração de Viabilidade

Esta equipe de planejamento declara **viável com restrições** esta contratação com base neste Estudo Técnico Preliminar.

18.1. Justificativa da Viabilidade com Restrições

Esta equipe de planejamento declara **viável com restrições** esta contratação com base neste Estudo Técnico Preliminar.

19. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

MARIA ELIANE SOBRINHO

Equipe de apoio

Emitido em 16/10/2026

ESTUDO TÉCNICO PRELIMINAR Nº 40/2026 - DICTI (11.12.35)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 16/10/2026 11:39)
MARIA ELIANE SOBRINHO
CHEFE DE DIVISAO
2933725

(Assinado digitalmente em 16/10/2026 11:28)
ZENAIDE CARVALHO DA SILVA
DIRETOR
1506929

(Assinado digitalmente em 16/10/2026 11:34)
JAIRO BELCHIOR FREITAS OLIVEIRA
DIRETOR
2317301

(Assinado digitalmente em 20/10/2026 09:45)
JEFERSON FERREIRA DA SILVA
ANALISTA DE TEC DA INFORMACAO
1122700

Para verificar a autenticidade deste documento entre em https://sipac.unifesspa.edu.br/documentos/ informando seu número: **40**, ano: **2026**, tipo: **ESTUDO TÉCNICO PRELIMINAR**, data de emissão: **16/10/2026** e o código de verificação: **bb7669e5fb**