Conselho Regional de Educação Física da 2ª Região

ESTUDO TÉCNICO PRELIMINAR

Processo Administrativo: PAC 2026/048

Departamento Requisitante: Departamento de Informática

Equipe de Planejamento da Contratação: Marcelo da Silva, matrícula nº 20, e Marcelo Ignácio Texeira, matrícula nº 21, conforme Portaria DLIC CREF2/RS nº 164, de 8 de julho de 2026.

Categoria do objeto: Serviços - solução continuada de segurança de rede gerenciada, com disponibilização de equipamentos em comodato.

1 DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO (art. 18, § 1º, I)

1.1 Descrição do problema a ser resolvido

A infraestrutura de segurança de borda do CREF2/RS precisa assegurar conectividade segura, disponibilidade dos links de internet, comunicação por VPN, acesso aos serviços institucionais e aplicação uniforme de políticas de segurança na Sede Porto Alegre e nos Postos de Atendimento de Caxias do Sul e Pelotas. Nas unidades do interior, os firewalls também exercem função de servidor DHCP, de modo que falhas ou substituições mal coordenadas podem provocar indisponibilidade imediata da rede local.

O tema vem sendo tratado pelo Departamento de Informática desde 2025, quando foi incluído no planejamento e na previsão orçamentária para 2026. Em 28/05/2026 foi formalizado o DFD 2026/047, que originou o PAC 2026/042, aberto em 11/06/2026, inicialmente destinado à aquisição de dois appliances próprios para Caxias do Sul e Pelotas. Em 07/07/2026 foi formalizado o DFD 2026/048, que originou o PAC 2026/048, aberto em 08/07/2026, para contratação dos serviços de implantação, configuração, suporte e monitoramento.

Durante o aprofundamento do planejamento, verificou-se que a divisão entre aquisição de hardware e contratação separada de serviços reproduziria parte do problema atualmente vivenciado: responsabilidades distribuídas entre fornecedores, maior complexidade para diagnóstico de falhas que envolvem VPN, DNS, Active Directory, roteamento ou failover e necessidade de coordenar garantia, licenças e suporte por instrumentos distintos. A Diretoria do CREF2/RS, por meio da Decisão nº 2026/000430, deliberada na Reunião nº 033/2026 em 17/09/2026, decidiu por unanimidade que a contratação dos firewalls deverá ocorrer por meio de comodato. Em consequência, o PAC 2026/042, destinado à aquisição dos equipamentos, será encerrado, e o projeto prosseguirá no PAC 2026/048 como contratação única de solução gerenciada, com os equipamentos fornecidos em comodato.

A transição possui dois marcos objetivos. Os appliances de Caxias do Sul e Pelotas deverão estar implantados, testados e em produção antes de 02/01/2027, data de encerramento do contrato vigente que atende os Postos do Interior. O appliance da Sede Porto Alegre deverá entrar em operação antes de 15/05/2027, data de encerramento do contrato vigente que atende a Sede. O faturamento deverá acompanhar a entrada efetiva em produção de cada etapa, evitando sobreposição indevida de despesas.

Durante o intervalo entre a entrada em produção dos equipamentos do Interior e a substituição do firewall da Sede, os novos appliances de Caxias do Sul e Pelotas deverão manter VPNs IPsec interoperáveis com o firewall Hillstone A1000 atualmente instalado em Porto Alegre. Posteriormente,

as conexões deverão ser reconfiguradas para o novo appliance da Sede, sem interrupção indevida dos serviços.

A implantação não deverá consistir na migração automática das regras atualmente existentes. A futura contratada deverá construir e implementar novas políticas e regras de segurança a partir das necessidades técnicas do CREF2/RS e das diretrizes e manifestação do Encarregado pelo Tratamento de Dados Pessoais (DPO), submetendo as configurações à validação do Departamento de Informática.

1.2 Abrangência e beneficiários

A solução abrangerá as três unidades operacionais contempladas nesta fase: Sede Porto Alegre, Posto de Atendimento de Caxias do Sul e Posto de Atendimento de Pelotas. Serão beneficiados diretamente os servidores e colaboradores que utilizam os recursos de rede, os usuários remotos autorizados, o Departamento de Informática e, indiretamente, os registrados e demais cidadãos atendidos pelo CREF2/RS.

Os postos do interior possuem perfil de pequeno porte, com aproximadamente dois usuários fixos e até três visitantes esporádicos por unidade, dois links de internet de até 600 Mbps e necessidade de rede administrativa, rede de visitantes e futura segregação de voz. A Sede concentra maior volume de usuários e serviços, além de atuar como ponto de integração das VPNs e dos serviços institucionais. A solução deverá, portanto, permitir dimensionamento distinto por unidade, inclusive com modelos diferentes entre Caxias do Sul, Pelotas e Porto Alegre, desde que todos sejam do mesmo fabricante, integrem o mesmo ecossistema de gestão e atendam aos requisitos mínimos aplicáveis a cada unidade.

1.3 Resultados a serem alcançados

a) assegurar continuidade operacional das três unidades nos marcos de transição dos contratos vigentes;

b) concentrar em uma única contratada a responsabilidade pelos appliances, licenças, implantação, suporte, monitoramento, atualizações, reposição e integração da solução;

c) padronizar os três appliances em um mesmo fabricante/ecossistema, sem indicação prévia de marca, permitindo gerenciamento centralizado e políticas uniformes;

d) assegurar SD-WAN, failover e balanceamento entre os dois links dos postos, reduzindo indisponibilidades por falha de enlace;

e) manter VPNs IPsec seguras e interoperáveis com equipamentos de terceiros durante a transição e com a infraestrutura institucional em nuvem;

f) preservar o acesso aos serviços de Active Directory, DNS e demais recursos institucionais através das VPNs;

g) permitir segregação da rede administrativa e da rede de visitantes, inclusive por interfaces físicas enquanto os switches locais não forem gerenciáveis, mantendo suporte a VLAN IEEE 802.1Q para evolução futura;

h) disponibilizar monitoramento, logs, alertas, relatórios e integração com Zabbix e GLPI, apoiando a gestão e a fiscalização contratual;

i) manter proteção de segurança atualizada durante toda a vigência, com IPS, controle de aplicações, filtragem web/URL e antimalware/antivírus ou funções equivalentes;

j) capacitar a equipe do Departamento de Informática para administração, fiscalização técnica e troubleshooting inicial da solução;

k) eliminar cobrança das unidades antes de sua efetiva entrada em produção e reduzir sobreposição de despesas na transição.

2 PREVISÃO NO PLANO DE CONTRATAÇÕES ANUAL (art. 18, § 1º, IX)

2.1 Alinhamento com o PCA

A necessidade integra o planejamento de contratações do exercício de 2026 e encontra-se formalizada no PAC 2026/048. O planejamento foi iniciado em 2025 e desdobrado, em 2026, nos DFDs 2026/047 e 2026/048. A consolidação do objeto no PAC 2026/048 representa refinamento da estratégia de contratação, e não criação de necessidade superveniente. O identificador específico da demanda no PCA, se distinto do número do processo administrativo, deverá ser confirmado pelo DLIC antes da versão final do Termo de Referência.

3 DESCRIÇÃO DOS REQUISITOS DA CONTRATAÇÃO (art. 18, § 1º, II)

3.1 Requisitos da solução

A contratação deverá ser especificada por requisitos funcionais e de desempenho, sem indicação de marca ou modelo. Os três appliances deverão ser fornecidos em comodato, pertencer ao mesmo fabricante e integrar um único ecossistema de gestão. Poderão ser utilizados modelos diferentes em cada unidade, dimensionados conforme o porte e a carga de Caxias do Sul, Pelotas e Porto Alegre, desde que atendam integralmente aos requisitos mínimos aplicáveis. A exigência de homogeneidade decorre da necessidade de uma única plataforma de administração, políticas consistentes, suporte coordenado e redução da complexidade operacional; não constitui preferência por fabricante determinado.

Requisitos mínimos dos appliances:

- appliance físico dedicado do tipo Next Generation Firewall (NGFW), novo, de primeiro uso na entrada em operação do contrato, pertencente à linha atual de produção do fabricante e sem classificação ou anúncio oficial de End of Sale (EOS), End of Life (EOL), End of Support/End of Service Life (EOSL) ou condição equivalente;
- throughput nominal de firewall igual ou superior a 3 Gbps;
- throughput de prevenção de intrusão (IPS) igual ou superior a 700 Mbps;
- throughput de VPN IPsec igual ou superior a 1 Gbps;
- no mínimo 5 interfaces Ethernet RJ45 de 1 GbE ou superiores, admitidas interfaces adicionais e velocidades superiores;
- operação simultânea com pelo menos 2 links WAN independentes de até 600 Mbps cada, sem redução das funcionalidades exigidas;

- SD-WAN com monitoramento da qualidade dos enlaces, failover automático e balanceamento/distribuição de tráfego;
- suporte a VLAN IEEE 802.1Q, com capacidade para pelo menos 3 VLANs, sem prejuízo da segregação por interfaces físicas atualmente necessária nos postos em razão do uso de switches não gerenciáveis;
- firewall stateful, NAT/PAT, políticas por origem, destino, serviço e interface, e serviço DHCP para as redes locais;
- VPN site-to-site IPsec com IKEv2 ou versão superior/equivalente, capacidade para pelo menos 4 túneis simultaneamente ativos por equipamento e suporte a VPN baseada em rota por interface virtual de túnel ou tecnologia equivalente;
- interoperabilidade IPsec com equipamentos e gateways de terceiros, inclusive o Hillstone A1000 da Sede durante a transição e gateways de infraestrutura institucional em nuvem, sem dependência de mesma marca nas duas extremidades;
- rotas estáticas e políticas de encaminhamento independentes para redes alcançadas por diferentes túneis, permitindo comunicação simultânea com Sede e nuvem;
- acesso remoto seguro para pelo menos 25 usuários por IPsec Dialup VPN ou SSL VPN;
- integração com Microsoft Active Directory por LDAP, RADIUS ou protocolo equivalente e possibilidade de utilização de usuários/grupos nas políticas;
- encaminhamento, pelas VPNs, do tráfego necessário a Active Directory, DNS e demais serviços de domínio, inclusive serviços hospedados em nuvem;
- subscrições de segurança oficiais contendo, no mínimo, IPS, controle de aplicações, filtragem web/URL e antimalware/antivírus ou funções equivalentes, além de atualizações de firmware, assinaturas e correções de segurança durante toda a vigência. Não será exigido pacote comercial premium específico, devendo a contratada fornecer apenas o nível de licenciamento necessário ao atendimento integral das funções e níveis de serviço definidos;
- administração segura por HTTPS e/ou SSH, perfis de privilégio, trilha de auditoria das alterações e backup/restauração de configuração;
- gerenciamento centralizado dos três appliances por plataforma fornecida pela contratada, acessível remotamente pelo Departamento de Informática, com autenticação multifator para contas administrativas quando suportada e perfis individualizados. Não será obrigatória licença ou pacote premium de gerenciamento, desde que todas as funcionalidades exigidas sejam atendidas;
- capacidade de integração com Zabbix utilizando recursos nativos do próprio appliance, sem dependência de agente proprietário adicional, por meio de SNMPv3, MIBs/OIDs documentados, SNMP Trap, Syslog e/ou API documentada. A integração deverá permitir ao CREF2/RS monitorar, no mínimo, disponibilidade do equipamento, utilização de CPU e memória, estado e tráfego das interfaces, estado dos links WAN e situação dos túneis VPN;
- fontes de alimentação, cabos e acessórios necessários à operação, compatíveis com a rede elétrica institucional;
- suporte oficial do fabricante e possibilidade de reposição por modelo igual ou superior durante toda a vigência. Caso o modelo deixe de possuir suporte oficial durante o contrato, a contratada deverá promover a substituição necessária sem custo adicional e sem redução de capacidade.

Requisitos mínimos dos serviços:

- planejamento do projeto, com reunião de kickoff, levantamento técnico, definição da arquitetura lógica, plano de implementação, responsáveis, cronograma e critérios de validação;
- implantação lógica e configuração inicial dos appliances, incluindo conectividade, roteamento, SD-WAN, VPNs, DHCP, segmentação, administração e monitoramento;
- elaboração de novas políticas e regras de segurança a partir das necessidades do CREF2/RS e da manifestação do Encarregado/DPO, vedada a simples migração automática das regras atuais;
- configuração e validação das VPNs IPsec de Caxias do Sul e Pelotas com o Hillstone A1000 enquanto ele permanecer na Sede e posterior reconfiguração das VPNs para o novo appliance de Porto Alegre;
- implantação e manutenção da plataforma de gerenciamento centralizado, com dashboards, métricas, alertas e no mínimo 5 relatórios automatizados;
- disponibilização de mecanismos para consulta e exportação dos logs em formato compatível com a infraestrutura do CREF2/RS. Não será exigida retenção mínima de 12 meses em nuvem da contratada; o CREF2/RS estabelecerá rotina interna, preferencialmente mensal, para coleta e armazenamento dos logs em sua própria estrutura. A contratada deverá apoiar a configuração, validação e manutenção do mecanismo de exportação/coleta necessário;
- configuração e validação da integração dos appliances com o Zabbix, utilizando os recursos nativos e protocolos abertos definidos neste ETP, quando o ambiente estiver disponibilizado pelo CREF2/RS, incluindo as métricas mínimas previstas, alertas e demais mecanismos de monitoramento suportados; integração com GLPI para registro e acompanhamento de chamados;
- sistema eletrônico de chamados próprio ou integrado, com protocolo único, individual e imutável, registro de data/hora de abertura, andamento e encerramento, histórico de interações e dados necessários à medição de SLA;
- suporte técnico especializado com cobertura 24x7 exclusivamente para incidentes críticos, tais como indisponibilidade total de unidade, interrupção das VPNs institucionais, falha grave de SD-WAN/failover ou evento de segurança de alta criticidade. Os demais chamados, ajustes e atividades evolutivas poderão ser atendidos em horário comercial, conforme SLA definido no Termo de Referência;
- banco de horas técnicas compartilhado entre as três unidades para atividades consultivas e evolutivas que não estejam incluídas nas obrigações ordinárias de operação, correção, atualização, incidente, garantia ou substituição de hardware. O banco deverá ser dimensionado de forma reduzida, considerando que uma implantação corretamente executada tende a demandar poucas intervenções evolutivas recorrentes; o quantitativo definitivo será estabelecido no Termo de Referência com base na pesquisa de preços;
- monitoramento ativo e proativo da disponibilidade dos appliances, interfaces, links WAN, VPNs, CPU, memória e eventos relevantes, com emissão de alertas e relatórios mensais;
- gestão de atualizações de firmware e assinaturas, executadas de forma planejada e com comunicação prévia de janelas de manutenção;
- reposição de appliance defeituoso por equipamento equivalente ou superior, mantendo licenças e configurações necessárias e observando SLA a ser definido no Termo de Referência;

- treinamento técnico de no mínimo 8 horas para pelo menos 2 integrantes do Departamento de Informática, em português, ao vivo (presencial ou remoto), com abordagem prática da solução implantada, cobrindo administração, políticas, VPN, SD-WAN, monitoramento, logs, relatórios, backup/restauração, atualizações e troubleshooting;
- reunião de encerramento de cada etapa de implantação, apresentação das configurações, validação final, documentação técnica atualizada, diagramas/topologia, inventário, backups de configuração e termo de aceite;
- apoio à reversibilidade ao término do contrato, com entrega de documentação atualizada, exportação dos dados e configurações disponíveis, apoio técnico à transição para solução sucessora e retirada segura dos equipamentos em comodato.

Requisitos de qualificação e segurança da prestação:

- a contratada deverá comprovar condição de parceira oficial, integradora autorizada ou canal habilitado do fabricante ofertado, em nível compatível com o fornecimento de licenças, suporte e acionamento de RMA;
- deverá manter equipe técnica com certificação vigente ou compatível com a solução ofertada, em quantitativo suficiente para cobertura do serviço e sem dependência de um único profissional;
- os acessos administrativos deverão utilizar contas individualizadas, princípio do menor privilégio, autenticação multifator quando disponível e registros de auditoria;
- credenciais, configurações, diagramas, endereçamentos, logs e demais informações de segurança deverão receber tratamento restrito, observando a Lei nº 13.709/2018 (LGPD), políticas internas e orientações do Encarregado/DPO;
- alterações relevantes de configuração deverão ser documentadas e executadas mediante processo de mudança aprovado pelo CREF2/RS, ressalvadas ações emergenciais necessárias à contenção de incidentes, que deverão ser registradas posteriormente.

Sustentabilidade e ciclo de vida:

- os equipamentos deverão observar, quando aplicável, restrições ao uso de substâncias perigosas em equipamentos eletroeletrônicos, como RoHS ou norma equivalente;
- embalagens deverão priorizar materiais recicláveis e dimensionamento compatível com a proteção do produto;
- por se tratar de comodato, a contratada permanecerá responsável pela retirada dos appliances ao término da vigência e pela destinação ambientalmente adequada ao final de sua vida útil, após eliminação segura das configurações e dados remanescentes.

4 LEVANTAMENTO E ANÁLISE DE MERCADO (art. 18, § 1º, III)

4.1 Prospecção de soluções

O levantamento considerou os estudos produzidos no PAC 2026/042, o escopo originalmente desenvolvido no PAC 2026/048, os contratos atualmente vigentes do CREF2/RS, consultas comerciais realizadas durante o planejamento, catálogos e documentação técnica de fabricantes, além de referências de contratações públicas divulgadas no Portal Nacional de Contratações Públicas (PNCP).

Como referências de modelagem, foram identificadas no PNCP contratações que demonstram disponibilidade de soluções integradas no mercado: o Edital nº 0005/2026 da Câmara Municipal de Canoas/RS, para solução integrada de firewall gerenciado com instalação, configuração, suporte, monitoramento e SLA; o Contrato nº 00011/2025 da Secretaria da Fazenda e Planejamento de São Paulo, estruturado como Firewall as a Service (FWaaS), com equipamentos, licenciamentos e serviços; e o Edital nº 40/2026 da Autoridade Nacional de Proteção de Dados (ANPD), para solução NGFW integrada com equipamentos, instalação, configuração, transferência de conhecimento e suporte. Essas referências são utilizadas apenas para validar modelos de contratação existentes no mercado, e não como parâmetro direto de preço ou indicação de fabricante.

Foram consideradas quatro alternativas principais: manutenção dos contratos separados atualmente existentes; aquisição de appliances próprios com serviços em contratação distinta; solução integrada gerenciada com appliances em comodato; e solução exclusivamente virtual/em nuvem sem firewall físico local.

4.2 Análise comparativa das soluções

Alternativa	Vantagens	Desvantagens / riscos	Avaliação
Manter contratos separados atuais	Menor esforço imediato de transição; preserva uma solução já conhecida e atualmente funcional.	Mantém a fragmentação de responsabilidades entre contratos e não incorpora, de forma uniforme nas três unidades, os novos patamares de desempenho, monitoramento institucional independente, gestão centralizada e integração com as ferramentas de fiscalização pretendidos para a próxima contratação. Os contratos possuem datas de término próximas.	Não recomendada.
Aquisição própria + serviços separados	Patrimônio próprio; maior independência do hardware; possibilidade de renovar serviços separadamente.	Exige dois ciclos de contratação e fiscalização; separa responsabilidade entre hardware/licenças e operação; necessidade de gerenciar garantia, RMA e renovação; risco de conflito entre fornecedores.	Tecnicamente viável, porém deixou de ser a estratégia preferida.
Solução gerenciada com comodato	Responsabilidade única; hardware, licenças, suporte, reposição, monitoramento e gestão integrados; atualização tecnológica durante a vigência; faturamento pode acompanhar a entrada em operação; reduz risco operacional da fragmentação.	Maior dependência da contratada durante a vigência e necessidade de planejar reversibilidade ao final do contrato.	Recomendada.

Alternativa	Vantagens	Desvantagens / riscos	Avaliação
Firewall exclusivamente virtual/em nuvem	Escalabilidade e redução de hardware local em alguns cenários.	Não substitui integralmente as funções locais de DHCP, segmentação, SD-WAN e controle dos dois links dos postos; dependência do acesso à internet para funções de borda.	Não recomendada como solução exclusiva.

A comparação com a estrutura atualmente instalada deve ser entendida como evolução de requisitos, e não como desqualificação da solução existente. Os equipamentos atuais foram dimensionados para as necessidades e condições definidas nas contratações anteriores e permanecem relevantes durante a transição. Nos Postos do Interior, a especificação contratual vigente registra, entre outros parâmetros, desempenho NGFW de 400 Mbps, IPS de 610 Mbps e Threat Protection de 200 Mbps. A nova contratação estabelece margem de capacidade superior e requisitos uniformes para o próximo ciclo, incluindo firewall de no mínimo 3 Gbps, IPS de no mínimo 700 Mbps, VPN IPsec de no mínimo 1 Gbps, gerenciamento centralizado, monitoramento institucional por Zabbix e integração das três unidades em uma única plataforma. Na Sede, o equipamento atual continuará sendo utilizado durante a etapa de transição e deverá interoperar por VPN IPsec com os novos appliances do Interior até sua substituição planejada. Assim, o ganho pretendido decorre principalmente da atualização de capacidade, da padronização operacional, da centralização da gestão e da ampliação dos mecanismos de monitoramento e fiscalização.

4.3 Justificativa da solução escolhida

A solução gerenciada com appliances em comodato foi selecionada porque reúne, em um único vínculo contratual, a responsabilidade pela camada física, licenciamento, atualizações, implantação, políticas, VPNs, monitoramento, suporte e reposição dos equipamentos. Essa característica reduz o principal risco operacional identificado no ambiente atual: a dificuldade de atuação coordenada entre empresas distintas quando um incidente envolve mais de uma unidade ou mais de um componente da infraestrutura. A escolha também formaliza a deliberação da Diretoria constante da Decisão nº 2026/000430, de 17/09/2026, que definiu o comodato como modelo para a contratação dos firewalls do CREF2/RS.

O comodato também transfere à contratada o risco de obsolescência e defeito do hardware durante a vigência, desde que o Termo de Referência exija equipamentos atuais, suporte oficial e substituição sem ônus. A Administração deixa de imobilizar recursos em equipamentos que exigiriam contratação adicional de manutenção e renovações de subscrição, passando a remunerar a solução efetivamente em operação.

A homogeneidade dos três appliances em um mesmo fabricante é tecnicamente justificada pela necessidade de gerenciamento centralizado, uniformidade das políticas e atualizações, simplificação do troubleshooting e responsabilidade integral da futura contratada. Essa homogeneidade também permite que o treinamento e a capacitação continuada do Departamento de Informática do CREF2/RS sejam realizados sobre uma única plataforma de administração e monitoramento, reduzindo a curva de aprendizado, a duplicidade de procedimentos e o risco operacional. Não será exigida marca específica, e modelos diferentes poderão ser utilizados para adequação ao porte de cada unidade.

A solução escolhida deverá preservar a interoperabilidade multivendor nas conexões IPsec, pois, durante a transição, os appliances do Interior precisarão operar com o Hillstone A1000 atualmente instalado na Sede e, posteriormente, com a infraestrutura institucional em nuvem.

5 DESCRIÇÃO DA SOLUÇÃO COMO UM TODO (art. 18, § 1º, IV)

5.1 Detalhamento do objeto

O objeto consiste na contratação de empresa especializada para prestação continuada de solução de segurança de rede gerenciada, pelo período de 36 meses, com fornecimento em comodato de 3 appliances físicos NGFW/SD-WAN do mesmo fabricante, sendo 2 destinados aos Postos de Caxias do Sul e Pelotas e 1 destinado à Sede Porto Alegre. Os modelos poderão ser distintos por unidade, desde que dimensionados adequadamente, integrem a mesma plataforma de gestão e permitam ao Departamento de Informática operar e administrar toda a solução a partir de uma única plataforma, objeto do treinamento previsto na contratação. A solução incluirá todas as licenças/subscrições necessárias às funções requeridas, suporte do fabricante, gerenciamento centralizado, implantação, configuração, novas políticas de segurança, VPNs, monitoramento, relatórios, integrações, treinamento, suporte técnico e reposição de hardware necessários ao funcionamento durante toda a vigência.

A implantação será executada em duas etapas operacionais:

Etapa	Unidades	Marco máximo	Condição de faturamento	Atividades principais
1 - Interior	Caxias do Sul e Pelotas	Entrada em operação antes de 02/01/2027	Somente após o aceite e a efetiva entrada em produção dos 2 appliances e dos respectivos serviços.	Implantação, novas políticas, SD-WAN, DHCP, segmentação, VPN IPsec com Hillstone A1000, gerenciamento, monitoramento e suporte.
2 - Sede	Porto Alegre	Entrada em operação antes de 15/05/2027	Somente após o aceite e a efetiva entrada em produção do appliance e dos serviços da Sede.	Implantação do appliance da Sede, novas políticas, reconfiguração das VPNs dos Postos, integração com nuvem e consolidação da gestão centralizada.

O faturamento escalonado é requisito da solução e deverá impedir cobrança do terceiro appliance e dos serviços correspondentes à Sede antes da sua efetiva entrada em produção. Também deverá ser evitada sobreposição indevida com os contratos vigentes.

Não haverá migração automática das regras dos firewalls atuais. A contratada deverá elaborar nova matriz de políticas e regras, submetê-la ao CREF2/RS e implementar as configurações aprovadas, observando as diretrizes do Encarregado/DPO.

5.2 Regime de execução

A contratação terá natureza de serviço continuado com disponibilização de equipamentos em comodato. A vigência inicial será de 36 meses, prazo considerado suficiente para amortização e estabilização da solução sem criar dependência contratual excessivamente longa. Não se recomenda, nesta fase, vigência inicial superior, pois prazo maior poderia dificultar a substituição do fornecedor caso o desempenho do serviço se mostre insatisfatório. Eventual prorrogação futura dependerá de avaliação expressa da qualidade dos serviços, vantajosidade e interesse da Administração. A execução será por etapas, com implantação inicial do Interior e posterior ativação

da Sede. Os appliances permanecerão de propriedade da contratada durante a vigência, que responderá por manutenção, licenciamento, suporte do fabricante e substituição.

Para fins de formação de preços e medição, o Termo de Referência deverá permitir identificar separadamente, quando conveniente, os valores de implantação das etapas e as parcelas mensais correspondentes ao Interior e à Sede, sem parcelar tecnicamente a solução entre fornecedores distintos. Licenças, subscrições, gerenciamento, suporte e demais componentes indispensáveis deverão estar incorporados aos preços contratados, evitando cobranças acessórias imprevisíveis.

Nos Postos de Atendimento de Caxias do Sul e Pelotas, a instalação física dos appliances poderá ser realizada pelo Departamento de Informática do CREF2/RS, em data previamente agendada, com apoio técnico remoto da contratada. Para esse fim, a instalação física compreende a acomodação ou fixação do equipamento no rack existente, a conexão à alimentação elétrica e a interligação ao cabeamento de rede previamente identificado. Essa opção decorre da capacidade técnica da equipe interna para execução dessas atividades básicas de infraestrutura e tem por objetivo evitar custos desnecessários de deslocamento de profissionais da contratada exclusivamente para instalação física. Permanecerão sob responsabilidade da contratada a orientação técnica, a validação das conexões, a configuração lógica detalhada, a criação e aplicação das políticas de segurança, SD-WAN, VPNs, roteamento, integrações, monitoramento, testes, comissionamento e entrada em produção. A execução da instalação física pela equipe do CREF2/RS não reduzirá nem transferirá as responsabilidades da contratada quanto ao correto funcionamento da solução. Na Sede Porto Alegre, a forma de execução da instalação física será definida no plano de implantação, podendo ser realizada pela contratada ou, quando conveniente, pelo Departamento de Informática, sem prejuízo das responsabilidades técnicas da contratada. Não serão exigidas visitas presenciais periódicas; a presença da contratada será necessária apenas quando indispensável à resolução de incidente ou ao cumprimento do SLA e quando a solução não puder ser restabelecida de forma remota ou com apoio da equipe interna, sem cobrança adicional de deslocamento quando a responsabilidade for contratual.

5.3 Modelo de gestão e fiscalização do contrato

A gestão e a fiscalização serão exercidas por servidores formalmente designados, observando a Lei nº 14.133/2021 e as rotinas internas do CREF2/RS. O recebimento de cada etapa deverá depender da validação técnica do appliance, licenças, conectividade, políticas, VPNs, gerenciamento, monitoramento, documentação e testes de failover definidos no Termo de Referência.

A medição mensal deverá considerar apenas as unidades efetivamente em produção e deverá ser acompanhada, no mínimo, de relatório contendo disponibilidade dos equipamentos e links, incidentes, chamados, cumprimento de SLA, alterações realizadas, estado das VPNs, atualizações executadas, eventos relevantes de segurança, utilização de recursos e pendências. O sistema de chamados deverá fornecer protocolo único e imutável e permitir comprovação objetiva dos tempos de atendimento.

Alterações de configuração deverão possuir registro de solicitação, responsável, data/hora, descrição, aprovação e resultado. Mudanças emergenciais deverão ser justificadas e documentadas. A fiscalização poderá consultar a plataforma de gerenciamento, logs, relatórios, Zabbix e GLPI para confrontar as informações apresentadas pela contratada. A integração dos appliances com o Zabbix, por meio de recursos nativos do próprio equipamento e protocolos abertos documentados, deverá apoiar o modelo de gestão baseada em evidências previsto no Manual de Gestão e Fiscalização de Contratos do CREF2/RS, permitindo obtenção independente de indicadores de disponibilidade e desempenho, acompanhamento objetivo dos níveis de serviço, produção de relatórios e

rastreabilidade das evidências utilizadas na fiscalização. Os equipamentos atualmente utilizados dispõem de recursos próprios de monitoramento e geração de logs; contudo, no ambiente hoje operado pelo CREF2/RS não está disponibilizada à fiscalização uma integração operacional com o Zabbix sob controle institucional. A nova contratação transforma essa integração em requisito expresso, verificável e disponível ao CREF2/RS desde a implantação da solução, representando ganho de governança e capacidade de fiscalização, sem juízo depreciativo sobre a tecnologia atualmente instalada.

6 ESTIMATIVAS (Quantidades e Valor)

6.1 Estimativa das Quantidades (art. 18, § 1º, V):

Componente	Quantidade / unidade	Destinação / observação
Appliance NGFW/SD-WAN em comodato	3 unidades	2 para Caxias do Sul/Pelotas e 1 para Porto Alegre; mesmo fabricante, admitidos modelos distintos conforme dimensionamento.
Implantação e comissionamento - Interior	1 etapa	Abrange 2 postos e deverá estar concluída antes de 02/01/2027.
Implantação e comissionamento - Sede	1 etapa	Entrada em operação antes de 15/05/2027.
Serviço gerenciado, monitoramento e suporte	36 meses de vigência	Interior faturado após etapa 1; Sede faturada somente após etapa 2. Suporte 24x7 restrito a incidentes críticos; demais demandas conforme horário e SLA definidos no TR.
Gerenciamento centralizado e exportação de logs	Durante toda a vigência	Gestão dos 3 appliances; consulta e exportação de logs para rotina interna de coleta e armazenamento do CREF2/RS, sem retenção mínima obrigatória em nuvem da contratada.
Treinamento técnico	Mínimo 8 horas / pelo menos 2 participantes	Departamento de Informática; conteúdo prático da solução implantada.
Relatórios automatizados	Mínimo 5 modelos	Relatórios e dashboards configurados para gestão técnica e fiscalização.
Banco de horas técnicas consultivas/evolutivas	Banco compartilhado entre as 3 unidades	Quantitativo reduzido a ser definido no Termo de Referência após a pesquisa de preços; não limita obrigações ordinárias de suporte, incidentes, correções, garantia ou substituição.

As quantidades decorrem da existência de três unidades com firewall de borda e dos marcos contratuais de substituição. O quantitativo de 3 appliances permite unificar o ambiente sob um mesmo contrato e fabricante, mantendo dois equipamentos de menor porte para os Postos e permitindo modelo de maior capacidade para a Sede, se necessário, sem alterar a arquitetura funcional.

6.2 Estimativa do Valor da Contratação (art. 18, § 1º, VI):

A referência global de R$ 216.715,55, apurada na fase anterior do planejamento, é mantida apenas como registro histórico de ordem de grandeza e não deverá ser utilizada como estimativa definitiva do novo modelo. Aquele valor foi composto em cenário distinto, com fornecimento definitivo de equipamentos e premissas de serviço que foram posteriormente revistas.

A nova pesquisa de preços deverá refletir especificamente o modelo de comodato por 36 meses e o escopo ora racionalizado, incluindo: suporte 24x7 apenas para incidentes críticos; banco reduzido de horas técnicas compartilhado entre as três unidades; ausência de obrigação de retenção de logs por 12 meses em nuvem, com coleta e armazenamento pelo próprio CREF2/RS; ausência de visitas presenciais periódicas; possibilidade de instalação física dos appliances do Interior pelo Departamento de Informática, com apoio remoto da contratada, evitando deslocamentos destinados apenas à montagem em rack, ligação de energia e conexão ao cabeamento; dimensionamento distinto dos appliances por unidade; e licenciamento restrito às funções de segurança efetivamente necessárias, sem exigência de pacote premium. A estimativa definitiva deverá observar o art. 23 da Lei nº 14.133/2021, a IN SEGES/ME nº 65/2021, contratações comparáveis no PNCP, pesquisas com fornecedores e demais fontes admitidas.

O enquadramento orçamentário deverá ser definido pelo DLIC em conjunto com a área contábil, considerando a natureza integrada da solução, avaliando-se os elementos 6.2.2.1.1.01.04.04.004 - SERVIÇOS DE INFORMÁTICA e 6.2.2.1.1.01.04.04.016 - LOCAÇÃO DE BENS MÓVEIS, MÁQ. E EQUIPAMENTOS. A parcela do Interior deverá ser apropriada ao Centro de Custo 01.04 - ADMINISTRAÇÃO INTERIOR e a parcela da Sede ao Centro de Custo 01.03 - ADMINISTRAÇÃO CENTRAL.

7 JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DO OBJETO (art. 18, § 1º, VII)

Não se recomenda o parcelamento técnico do objeto entre fornecedores distintos. Hardware em comodato, licenças/subscrições, plataforma de gerenciamento, configuração, políticas, VPNs, monitoramento, suporte e reposição constituem componentes interdependentes de uma mesma solução. A separação recriaria o risco de transferência de responsabilidade que motivou a revisão do modelo de contratação.

A exigência de que os três appliances sejam do mesmo fabricante reforça a necessidade de contratação integrada: o objetivo é manter uma única camada de gerenciamento e política, não restringir a competição a uma marca específica. O mercado possui múltiplos fabricantes com famílias de equipamentos de portes distintos e recursos equivalentes, permitindo competição entre soluções completas.

O faturamento e a implantação poderão ser divididos em etapas e parcelas para fins de medição e adequação orçamentária, sem que isso caracterize parcelamento do objeto entre contratadas diferentes. A Sede somente passará a gerar cobrança após sua entrada em produção.

8 CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES (art. 18, § 1º, VIII)

A contratação possui relação direta com os contratos atualmente responsáveis pela segurança de borda das unidades. O contrato que atende os Postos de Caxias do Sul e Pelotas encerra-se em 02/01/2027, e o contrato que atende a Sede Porto Alegre encerra-se em 15/05/2027. O cronograma deverá garantir transição antes dessas datas, sem necessidade de identificar os atuais fornecedores como requisito da nova contratação.

Também são correlatos os serviços de acesso à internet das três unidades, pois a solução dependerá dos dois enlaces existentes nos Postos e dos links da Sede; o projeto institucional de Controlador de Domínio em nuvem, com o qual deverão existir rotas e VPNs interoperáveis; e o projeto de implantação do Zabbix previsto para 2027. Os appliances contratados deverão possuir capacidade nativa de integração com o Zabbix pelos mecanismos definidos neste ETP, de forma a permitir monitoramento institucional independente e geração de evidências para a gestão e fiscalização do contrato.

O ambiente GLPI do CREF2/RS é correlato à gestão de chamados e deverá ser integrado, quando tecnicamente aplicável, ao fluxo de suporte. A futura implantação de telefonia IP/VoIP também é considerada na capacidade de VLAN, QoS e priorização de tráfego, embora não integre diretamente o objeto desta contratação.

9 PROVIDÊNCIAS PARA ADEQUAÇÃO DO AMBIENTE DO ÓRGÃO (art. 18, § 1º, XI)

- confirmar e documentar os locais de instalação, registrando que as três unidades já dispõem de racks em padrão U adequados aos equipamentos de rede, além de alimentação elétrica, pontos de rede e cabeamento necessários;
- não será exigido o fornecimento específico de parafusos ou elementos comuns de fixação em rack, ficando a forma de acomodação e fixação do appliance a critério da contratada, conforme as características do equipamento ofertado; caso o modelo necessite de suporte, bandeja, orelha, trilho ou kit proprietário específico para instalação segura, esse componente deverá integrar a solução sem custo adicional;
- mapear os links de internet, IPs públicos/fixos, endereçamento interno, redes locais, impressoras, access points e demais dispositivos relevantes;
- documentar a topologia atual e os parâmetros necessários à VPN IPsec com o Hillstone A1000 durante a transição;
- definir, com participação do Departamento de Informática e do Encarregado/DPO, a nova matriz de políticas e regras de segurança, sem migração automática das regras atuais;
- definir a segregação da rede administrativa e da rede de visitantes; nos Postos, enquanto os switches permanecerem não gerenciáveis, prever segregação física por interfaces do firewall, mantendo planejamento para VLANs futuras;
- disponibilizar informações de integração com Active Directory/DNS e com a infraestrutura institucional em nuvem;
- preparar ou disponibilizar o ambiente Zabbix para integração SNMPv3 quando o projeto estiver implantado e definir o fluxo de integração com GLPI;
- definir responsáveis, janelas de mudança, plano de testes e plano de retorno para cada etapa de implantação;

- agendar as janelas de instalação e disponibilizar integrante do Departamento de Informática para execução e/ou acompanhamento das atividades físicas; nos Postos de Caxias do Sul e Pelotas, a instalação física poderá ser executada pela equipe interna, com apoio remoto da contratada, que deverá orientar a atividade, validar as conexões e conduzir a configuração lógica, os testes, o comissionamento e a entrada em produção;
- designar participantes do treinamento e reservar janela de pelo menos 8 horas para capacitação prática;
- definir os indicadores e níveis de serviço no Termo de Referência, incluindo criticidade de chamados, tempos de resposta/solução, disponibilidade e reposição de equipamento;
- planejar a reversibilidade ao término da contratação, assegurando posse institucional de documentação, inventário, backups e exportações necessárias à transição futura.

10 DECLARAÇÃO DE VIABILIDADE (art. 18, § 1º, XIII)

Os requisitos e características definidos neste Estudo Técnico Preliminar correspondem ao cenário técnico considerado adequado pelo Departamento de Informática para atendimento das necessidades atuais e previstas do CREF2/RS, considerando segurança, disponibilidade, desempenho, interoperabilidade, capacidade de monitoramento, continuidade operacional, gestão contratual e possibilidade de evolução da infraestrutura durante a vigência pretendida. As especificações propostas foram estabelecidas a partir das condições atualmente existentes, das limitações identificadas no ambiente em operação e dos resultados pretendidos com a nova contratação. Eventuais alterações posteriores desses requisitos deverão ser formalmente justificadas no processo e avaliadas quanto aos impactos técnicos, aos riscos assumidos e aos resultados esperados.

Com base na necessidade identificada, na experiência operacional dos contratos vigentes, nos estudos produzidos nos PACs 2026/042 e 2026/048, nas consultas de mercado e nas referências de contratações públicas, a Equipe de Planejamento conclui que a contratação de solução gerenciada de firewall NGFW/SD-WAN com três appliances em comodato é tecnicamente viável e adequada ao interesse público.

O modelo integrado reduz a fragmentação de responsabilidades, assegura atualização e reposição de hardware durante a vigência, permite gestão centralizada e atende aos marcos de transição do Interior e da Sede. A contratação deverá observar a neutralidade de marca, mantendo requisitos mínimos funcionais e de desempenho e garantindo competição entre fabricantes capazes de fornecer uma solução completa.

A viabilidade econômica definitiva dependerá da pesquisa de preços específica para o modelo de comodato e serviço gerenciado, com faturamento escalonado e com as medidas de racionalização de custos definidas neste ETP. A referência histórica existente é suficiente apenas para demonstrar a evolução do planejamento e deverá ser substituída pela nova estimativa antes da definição do valor da contratação no Termo de Referência.

11 RESPONSÁVEIS

Equipe de Planejamento da Contratação designada pela Portaria DLIC CREF2/RS nº 164, de 8 de julho de 2026:

cref2/RS
Conselho Regional de Educação Física
da 2ª Região

- Marcelo da Silva - Departamento de Informática - matrícula nº 20 - Coordenador da Equipe de Planejamento da Contratação.
- Marcelo Ignácio Texeira - Departamento de Informática - matrícula nº 21 - Integrante da Equipe de Planejamento da Contratação.

Porto Alegre/RS, 13/10/2026.

MARCELO DA SILVA
Coordenador da Equipe de Planejamento da Contratação

MARCELO IGNÁCIO TEXEIRA
Integrante da Equipe de Planejamento da Contratação

SIS DOC NET ASSINATURA ELETRÔNICA
Documento assinado eletronicamente por **MARCELO DA SILVA, ASSESSOR DE INFORMÁTICA, INFORMÁTICA, IP de acesso 177.69.28.250,** em 13/10/2026, às 16:16:19, conforme horário oficial de Brasília. Com fundamento na Lei nº 14.063, de 23 de setembro de 2020.

SIS DOC NET ASSINATURA ELETRÔNICA
Documento assinado eletronicamente por **MARCELO IGNACIO TEXEIRA, SUPERVISOR DE PROSPECÇÃO EM TECNOLOGIA, INFORMÁTICA, IP de acesso 177.69.28.250,** em 11/11/2026, às 09:48:15, conforme horário oficial de Brasília. Com fundamento na Lei nº 14.063, de 23 de setembro de 2020.

cref2/RS
Conselho Regional de Educação Física
da 2ª Região

ATUALIZAÇÃO DO ESTUDO TÉCNICO PRELIMINAR

Solução continuada de segurança de rede gerenciada – firewall NGFW/SD-WAN em comodato

Processo Administrativo: PAC 2026/048

Departamento Requisitante: Departamento de Informática

Equipe de Planejamento da Contratação: Marcelo da Silva, matrícula nº 20, e Marcelo Ignácio Texeira, matrícula nº 21, conforme Portaria DLIC CREF2/RS nº 164, de 8 de julho de 2026.

Documento atualizado: Estudo Técnico Preliminar, versão 5, de 13/10/2026.

1 FINALIDADE

1.1 Este documento registra as alterações do planejamento da contratação ocorridas após a assinatura do Estudo Técnico Preliminar, versão 5, em 13/10/2026 (ETP v5), decorrentes da pesquisa de preços, do refinamento dos requisitos técnicos e da adequação da solução ao orçamento disponível, com a motivação de cada alteração.

1.2 O ETP v5 permanece válido em tudo o que não for alterado por este documento, que o integra e, com ele, servirá de base à elaboração do Termo de Referência.

2 HISTÓRICO DO PLANEJAMENTO

2.1 A contratação percorreu as seguintes etapas de planejamento, conforme documentos constantes do PAC 2026/048:

Marco	Registro	Efeito no planejamento
2025	Inclusão da necessidade no planejamento e na previsão orçamentária de 2026.	Origem da demanda institucional.
DFD 2026/047, de 28/05/2026, e PAC 2026/042, de 11/06/2026	Aquisição de dois appliances próprios para os Postos de Caxias do Sul e Pelotas.	Estratégia inicial de aquisição de equipamentos.
DFD 2026/048, de 07/07/2026, e PAC 2026/048, de 08/07/2026	Contratação dos serviços de implantação, configuração, suporte e monitoramento.	Serviços planejados separadamente da aquisição.
Decisão da Diretoria nº 2026/000430, de 17/09/2026	Decisão unânime, na Reunião nº 033/2026, de que a contratação dos firewalls será realizada por meio de comodato.	Encerramento do PAC 2026/042 e prosseguimento no PAC 2026/048 como solução gerenciada única.
ETP v5, de 13/10/2026	Comodato de três appliances do mesmo fabricante, implantação escalonada e requisitos mínimos gerais.	Base do planejamento ora atualizado.
Pesquisa de preços, de 30/10/2026	Estimativa específica para o modelo de comodato com serviço gerenciado.	Valor global estimado de R$ 177.200,00 e adequação do escopo ao orçamento.
Refinamento dos requisitos, de outubro e novembro de 2026	Diferenciação dos appliances por unidade, níveis de serviço, instrumento de medição e estrutura dos itens.	Alterações registradas neste documento.

2.2 A necessidade institucional permanece a mesma desde a origem. As etapas posteriores alteraram a forma de atendê-la, e não a necessidade que a motivou.

3 JUSTIFICATIVA DA ALTERAÇÃO DE ESCOPO

3.1 O DFD 2026/048 foi estruturado para a contratação de serviços, enquanto a aquisição dos dois equipamentos do Interior foi registrada separadamente no DFD 2026/047 e no PAC 2026/042. Essa divisão entre equipamentos e serviços manteria fragmentadas as responsabilidades: falhas envolvendo VPN, DNS, Active Directory, roteamento ou failover exigiriam coordenação entre fornecedores e instrumentos distintos, além de separar garantia, licenciamento e suporte.

3.2 A Decisão da Diretoria nº 2026/000430, de 17/09/2026, deliberada por unanimidade na Reunião nº 033/2026, determinou que a contratação dos firewalls seja realizada por meio de comodato. Em consequência, o PAC 2026/042 foi encerrado e o PAC 2026/048 passou a abranger solução gerenciada integrada, que reúne equipamentos e serviços da Sede Porto Alegre e dos Postos de Caxias do Sul e Pelotas sob responsabilidade contratual única.

3.3 A alteração não cria necessidade nova. Reorganiza a forma de atendimento, com ganhos de continuidade operacional, gestão centralizada, responsabilização única por equipamentos, licenças, implantação, suporte e reposição, e sincronização com o encerramento dos contratos vigentes, em 02/01/2027 para os Postos e em 15/05/2027 para a Sede.

4 ALTERAÇÕES EM RELAÇÃO AO ETP V5

4.1 As alterações do planejamento em relação ao ETP v5 e as respectivas motivações são as seguintes:

Tema	ETP v5	Definição atualizada	Motivação
Banco de horas técnicas	Banco compartilhado e reduzido para atividades consultivas e evolutivas, com quantitativo a definir após a pesquisa.	Não haverá banco de horas pré-contratado. Demandas que extrapolem o escopo ordinário dependerão de solicitação formal e instrumento administrativo próprio.	Adequação ao orçamento disponível. A exclusão alcança apenas horas evolutivas avulsas; suporte, correções, atualizações, substituição de hardware e níveis de serviço permanecem incluídos no preço mensal.
Treinamento	Treinamento técnico de, no mínimo, 8 horas para pelo menos 2 integrantes do Departamento de Informática.	Transferência de conhecimento operacional durante a implantação, sem carga horária mínima, suficiente para que pelo menos 2 integrantes do Departamento de Informática administrem a plataforma.	Adequação ao orçamento disponível. A capacitação é preservada pela transferência de conhecimento, com documentação e comprovação perante a fiscalização.
Tipos de appliance	Requisitos mínimos gerais, aplicáveis a todos os equipamentos.	Dois tipos do mesmo fabricante e da mesma plataforma: Tipo I para a Sede e Tipo II para os Postos, admitidos modelos distintos.	Dimensionamento de cada equipamento à carga e à função da unidade, sem exigir equipamento de porte de Sede nos Postos (seção 5).
Desempenho do Tipo I (Sede)	Firewall ≥ 3 Gbps, IPS ≥ 700 Mbps, VPN IPsec ≥ 1 Gbps e 5 interfaces.	Firewall ≥ 5 Gbps, IPS ≥ 1,5 Gbps, VPN IPsec ≥ 2 Gbps e 8 interfaces.	Concentração, na Sede, dos usuários, dos serviços institucionais e dos túneis VPN dos Postos.
VPN IPsec do Tipo II (Postos)	VPN IPsec ≥ 1 Gbps.	VPN IPsec ≥ 600 Mbps por appliance.	Compatibilidade com os links de até 600 Mbps de cada Posto, com redução de custo e ampliação da competitividade.

Tema	ETP v5	Definição atualizada	Motivação
Equipe técnica	Equipe com certificação vigente, em quantitativo suficiente e sem dependência de um único profissional.	No mínimo 1 profissional certificado, com substituição por qualificação equivalente, verificação a qualquer tempo pela fiscalização e prazo de 30 dias para regularização.	Proporcionalidade ao porte da solução e ampliação da competitividade. A continuidade é assegurada pelos níveis de serviço, exigíveis inclusive durante eventual regularização.
Níveis de serviço e medição	Detalhamento remetido ao Termo de Referência a ser elaborado.	Níveis de serviço por severidade e Instrumento de Medição de Resultado pelo Índice de Atendimento no Prazo (IAP): meta de 90%, com descontos de 10%, 20% e 30% na fatura mensal conforme a faixa apurada.	Medição objetiva da qualidade do serviço, com ajuste do pagamento proporcional ao desempenho.
Estrutura dos itens e regime de execução	Solução única, sem parcelamento entre fornecedores.	Grupo único com dois itens: item 1, Appliance Tipo I (até 32 meses); item 2, Appliance Tipo II (72 appliances/mês). Menor preço global do grupo e empreitada por preço unitário.	Mantida a adjudicação a um só fornecedor, exigida pelo mesmo fabricante e plataforma. O preço por appliance permite medir e pagar apenas as unidades em produção e ajustar quantitativos nos limites do art. 125 da Lei nº 14.133, de 2021.
Estimativa da contratação	R$ 216.715,55, mantido como referência da fase anterior, pendente de pesquisa específica.	R$ 177.200,00 para 36 meses, conforme disposto na pesquisa de preços, de 30/10/2026 (seção 6).	Pesquisa específica para o modelo de comodato com serviço gerenciado, com exclusão do banco de horas e do treinamento com carga horária mínima.
Classificação contábil	Avaliação entre os elementos SERVIÇOS DE INFORMÁTICA e LOCAÇÃO DE BENS MÓVEIS, MÁQ. E EQUIPAMENTOS.	Elemento 6.2.2.1.1.01.04.04.016 – LOCAÇÃO DE BENS MÓVEIS, MÁQ. E EQUIPAMENTOS, com os Centros de Custo 01.03 (Sede) e 01.04 (Interior).	Definição administrativa e contábil da natureza da despesa, considerando a disponibilização mensal dos equipamentos com os serviços agregados.
Nova unidade no Interior	Não previsto.	Possibilidade de inclusão, durante a vigência e suas prorrogações, de nova unidade no Interior, atendida por Appliance Tipo II, mediante acréscimo quantitativo do item 2 ao preço unitário contratado.	Planejamento institucional de nova unidade no Interior no decorrer da contratação, sem data definida. A medição por appliance/mês permite o acréscimo nos limites do art. 125 da Lei nº 14.133, de 2021.

4.2 Permanecem sem alteração de mérito em relação ao ETP v5, devendo ser detalhados no Termo de Referência a ser elaborado:

4.2.1 o atendimento técnico 24x7 restrito aos incidentes críticos, com os demais chamados atendidos em dias úteis, conforme os níveis de serviço;

4.2.2 a elaboração de novas políticas de segurança conforme as necessidades do CREF2/RS e as diretrizes do Encarregado pelo Tratamento de Dados Pessoais (DPO), sem migração automática das regras atuais;

4.2.3 a integração com GLPI ou fluxo equivalente, condicionada à disponibilidade técnica do ambiente institucional;

4.2.4 a instalação física nos Postos pela equipe do Departamento de Informática, permanecendo com a contratada a pré-configuração, a configuração lógica, os ajustes, os testes, o comissionamento e a entrada em produção;

4.2.5 a dispensa de retenção de logs em nuvem da contratada, com coleta e armazenamento em estrutura própria do CREF2/RS;

4.2.6 os requisitos de sustentabilidade e a logística reversa dos equipamentos substituídos ou retirados, após eliminação segura de dados e configurações;

4.2.7 o faturamento de cada unidade somente após o aceite e a entrada em produção, sem sobreposição com os contratos vigentes; e

4.2.8 a vigência de 36 (trinta e seis) meses.

5 FUNDAMENTAÇÃO DO DIMENSIONAMENTO

5.1 A adoção de dois tipos de appliance decorre do dimensionamento da mesma solução para ambientes distintos, mantidos o mesmo fabricante e a mesma plataforma de gerenciamento para políticas, atualizações, suporte e operação uniformes.

5.2 Os Postos de Caxias do Sul e Pelotas são ambientes de pequeno porte, com aproximadamente 2 usuários fixos e até 3 visitantes simultâneos por unidade, cerca de 20 dispositivos conectados, 2 links de até 600 Mbps, redes administrativa e de visitantes e eventual segregação futura de voz. O firewall também exerce a função de servidor DHCP e precisa acomodar a topologia existente, com switches não gerenciáveis, o que justifica o mínimo de 5 interfaces físicas.

5.3 A Sede Porto Alegre concentra cerca de 80 usuários de domínio, de 150 a 200 dispositivos conectados, os servidores e os serviços de Active Directory e DNS, as VPNs dos Postos, o acesso remoto e as integrações com a infraestrutura em nuvem. A indisponibilidade ou a insuficiência do appliance da Sede repercute nas três unidades, o que justifica maior capacidade de processamento, IPS e VPN.

5.4 A eventual inclusão de nova unidade no Interior, de porte equivalente ao dos Postos atuais, será atendida por Appliance Tipo II, nas mesmas condições técnicas.

5.5 São adotados os seguintes parâmetros mínimos:

5.5.1 Appliance Tipo I (Sede): firewall igual ou superior a 5 Gbps; IPS igual ou superior a 1,5 Gbps; VPN IPsec igual ou superior a 2 Gbps; 8 interfaces RJ45 de 1 GbE ou superiores; 10 túneis VPN site-to-site simultâneos; e acesso remoto para 25 usuários simultâneos;

5.5.2 Appliance Tipo II (Postos): firewall igual ou superior a 3 Gbps; IPS igual ou superior a 700 Mbps; VPN IPsec igual ou superior a 600 Mbps; 5 interfaces RJ45 de 1 GbE ou superiores; operação simultânea com 2 links de até 600 Mbps; e 4 túneis VPN site-to-site simultâneos.

5.6 Os parâmetros mínimos foram verificados em modelos de dois fabricantes, utilizados exclusivamente como referência de mercado, sem indicação ou preferência de marca. As combinações de referência foram: Fortinet FortiGate 70G (Sede) e FortiGate 50G (Postos); Fortinet FortiGate 90G (Sede) e FortiGate 50G (Postos); e Sophos XGS 118 Gen.2 (Sede) e XGS 108 Gen.2 (Postos).

5.7 Conforme as folhas de dados dos fabricantes, todos os modelos de referência atendem ou superam os parâmetros mínimos do respectivo tipo, o que demonstra a existência de mais de um fabricante apto a fornecer a solução e preserva a competitividade:

Tipo	Fabricante / modelo	Firewall	IPS	VPN IPsec	Interfaces RJ45
Tipo I – Sede	**Mínimo exigido**	**≥ 5 Gbps**	**≥ 1,5 Gbps**	**≥ 2 Gbps**	**8**
Tipo I – Sede	Fortinet FortiGate 70G	10 Gbps	2,5 Gbps	7,1 Gbps	10
Tipo I – Sede	Fortinet FortiGate 90G	28 Gbps	4,5 Gbps	25 Gbps	8 + 2 compartilhadas
Tipo I – Sede	Sophos XGS 118 Gen.2	15,5 Gbps	3,5 Gbps	13 Gbps	9 (2,5 GbE)
Tipo II – Postos	**Mínimo exigido**	**≥ 3 Gbps**	**≥ 700 Mbps**	**≥ 600 Mbps**	**5**

cref2/RS
Conselho Regional de Educação Física
da 2ª Região

Tipo	Fabricante / modelo	Firewall	IPS	VPN IPsec	Interfaces RJ45
Tipo II – Postos	Fortinet FortiGate 50G	5 Gbps	2,25 Gbps	4,5 Gbps	5
Tipo II – Postos	Sophos XGS 108 Gen.2	12,5 Gbps	2,5 Gbps	8,25 Gbps	6 (2,5 GbE)

Valores máximos informados nas folhas de dados dos fabricantes. Todos os modelos de referência comportam os túneis VPN site-to-site e os usuários de acesso remoto exigidos.

6 ESTIMATIVA DO VALOR E ADEQUAÇÃO ORÇAMENTÁRIA

6.1 O valor global estimado da contratação é de R$ 177.200,00 (cento e setenta e sete mil e duzentos reais) para 36 (trinta e seis) meses, conforme disposto na pesquisa de preços, de 30/10/2026, que substitui a referência de R$ 216.715,55 mantida no ETP v5.

6.2 A estimativa é composta por:

6.2.1 item 1 – Appliance Tipo I (Sede): R$ 2.500,00 por mês, totalizando R$ 80.000,00 na projeção de 32 mensalidades, a partir de maio de 2027;

6.2.2 item 2 – Appliances Tipo II (Postos): R$ 1.350,00 por appliance/mês, totalizando R$ 2.700,00 por mês para 2 (dois) appliances e R$ 97.200,00 em 36 meses.

6.3 A projeção por exercício é de R$ 52.400,00 em 2027, R$ 62.400,00 em 2028 e R$ 62.400,00 em 2029. Os valores não incluem reajustes futuros pelo Índice de Custos de Tecnologia da Informação – ICTI, e o faturamento efetivo da Sede dependerá da data de aceite e entrada em produção.

6.4 A despesa será classificada no elemento 6.2.2.1.1.01.04.04.016 – LOCAÇÃO DE BENS MÓVEIS, MÁQ. E EQUIPAMENTOS, com os valores do item 1 (Sede) vinculados ao Centro de Custo 01.03 – ADMINISTRAÇÃO CENTRAL e os do item 2 (Postos) vinculados ao Centro de Custo 01.04 – ADMINISTRAÇÃO INTERIOR.

7 REGISTROS COMPLEMENTARES

7.1 A demanda não possui identificador específico no Plano de Contratações Anual de 2026, encontra-se formalizada no PAC 2026/048 e está incluída no Plano de Contratações Anual de 2027, exercício de início da execução contratual.

8 CONCLUSÃO

8.1 As alterações registradas preservam a necessidade, a solução e o modelo de comodato definidos no ETP v5 e na Decisão da Diretoria nº 2026/000430, de 17/09/2026, e adequam requisitos, quantitativos e estimativa ao porte de cada unidade e ao orçamento disponível. A equipe de planejamento mantém a conclusão pela viabilidade da contratação.

Porto Alegre/RS, 11 de novembro de 2026.

MARCELO DA SILVA
Coordenador da Equipe de Planejamento da Contratação

MARCELO IGNÁCIO TEXEIRA
Integrante da Equipe de Planejamento da Contratação

SIS DOC NET ASSINATURA ELETRÔNICA
Documento assinado eletronicamente por **MARCELO DA SILVA, ASSESSOR DE INFORMÁTICA, INFORMÁTICA, IP de acesso 189.6208.184**, em 11/11/2026, às 09:37:15, conforme horário oficial de Brasília. Com fundamento na Lei nº 14.063, de 23 de setembro de 2020.

SIS DOC NET ASSINATURA ELETRÔNICA
Documento assinado eletronicamente por **MARCELO IGNACIO TEXEIRA, SUPERVISOR DE PROSPECÇÃO EM TECNOLOGIA, INFORMÁTICA, IP de acesso 177.69.28.250,** em 11/11/2026, às 09:47:46, conforme horário oficial de Brasília. Com fundamento na Lei nº 14.063, de 23 de setembro de 2020.