

INST.FED.DE EDUC.,CIENC.E TEC.DE SÃO PAULO

Estudo Técnico Preliminar 210/2026

1. Informações Básicas

Número do processo: 23305.011838.2026-47

2. Descrição da necessidade

A presente contratação tem por finalidade atender à necessidade institucional da Direção-Geral do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – IFSP, Campus Diadema, visando promover as condições técnicas indispensáveis à implantação, estruturação e pleno funcionamento da unidade, no contexto do processo de expansão da Rede Federal de Educação Profissional, Científica e Tecnológica, em consonância com as diretrizes estratégicas institucionais e com as ações previstas no Novo Programa de Aceleração do Crescimento (Novo PAC) do Governo Federal.

No âmbito desse processo de expansão, destaca-se a implantação e estruturação do IFSP – Campus Diadema, localizado na Avenida Sete de Setembro, nº 1670, Centro, Município de Diadema/SP, CEP 09912-010, unidade que demandará a disponibilização de infraestrutura tecnológica robusta, segura, padronizada e compatível com os padrões corporativos de Tecnologia da Informação e Comunicação adotados pelo IFSP.

Considerando tratar-se de unidade em fase de implantação e adequação de suas instalações físicas, faz-se necessária a execução integrada das soluções de conectividade, infraestrutura de telecomunicações e segurança eletrônica, de modo a evitar retrabalhos, incompatibilidades técnicas, intervenções posteriores nas edificações e custos adicionais decorrentes da execução fragmentada das soluções.

A expansão das unidades exige a implementação de infraestrutura tecnológica integrada, composta por rede lógica estruturada, backbone óptico em fibra monomodo, sistemas ativos de rede e sistemas de segurança eletrônica, incluindo circuito fechado de televisão (CFTV) e controle de acesso, assegurando uniformidade tecnológica, escalabilidade e aderência aos requisitos institucionais de desempenho e segurança.

A infraestrutura de rede deverá contemplar, entre outros elementos:

I – Cabeamento estruturado metálico categoria 6 (Cat6), destinado ao atendimento horizontal de ambientes administrativos, acadêmicos, laboratórios, salas de aula e demais áreas institucionais;

II – Backbone óptico em fibra monomodo (SM), destinado à interligação entre racks, edificações ou pontos estratégicos da unidade, garantindo elevada capacidade de transmissão, baixa latência, imunidade a interferências eletromagnéticas e possibilidade de expansão futura;

III – Fornecimento e instalação de Distribuidores Internos Ópticos (DIO), execução de emendas ópticas por fusão certificadas e realização de testes de atenuação e continuidade mediante utilização de equipamentos específicos, tais como OTDR e power meter, com emissão dos respectivos relatórios técnicos;

IV – Implantação da infraestrutura física de telecomunicações, compreendendo eletrocalhas, eletrodutos, canaletas, caixas de passagem, suportes, pontos de telecomunicações e demais elementos necessários à adequada acomodação, proteção e organização do cabeamento estruturado, observando-se as normas técnicas aplicáveis e possibilitando futuras expansões e manutenções;

V – Fornecimento, instalação e configuração de equipamentos ativos de rede, incluindo switches gerenciáveis, pontos de acesso sem fio e solução de segurança perimetral, indispensáveis à operacionalização dos serviços de conectividade, segmentação lógica, gerenciamento centralizado e proteção dos ativos institucionais.

A adoção de infraestrutura híbrida, composta por cabeamento metálico e backbone óptico, mostra-se tecnicamente necessária para assegurar desempenho adequado às aplicações institucionais, tais como sistemas acadêmicos e administrativos corporativos, plataformas de ensino, serviços de autenticação, sistemas de videomonitoramento IP e soluções de controle de acesso em tempo real, garantindo, ainda, escalabilidade, interoperabilidade e sustentabilidade tecnológica no médio e longo prazo.

A disponibilização de cobertura sem fio corporativa constitui requisito essencial para atendimento das atividades acadêmicas e administrativas, permitindo mobilidade, suporte a múltiplos usuários simultâneos e integração segura aos serviços institucionais, especialmente em ambientes de ensino, laboratórios e áreas de convivência.

Da mesma forma, a implantação de solução de segurança perimetral de rede (firewall corporativo) é indispensável para o monitoramento e controle do tráfego de dados, prevenção contra ameaças cibernéticas, aplicação de políticas de segurança, estabelecimento de conexões seguras e proteção das informações institucionais, em conformidade com as diretrizes de segurança da informação adotadas pelo IFSP.

A solução contempla, ainda, a implantação de sistema de circuito fechado de televisão (CFTV) destinado ao monitoramento contínuo das áreas internas e externas da unidade, com gravação em alta resolução, armazenamento seguro e integração à infraestrutura de rede lógica estruturada. A adoção dessa solução contribuirá para a proteção do patrimônio público, preservação dos bens institucionais e fortalecimento da segurança da comunidade acadêmica.

A solução de videomonitoramento deverá abranger áreas estratégicas da unidade, permitindo acompanhamento em tempo real, recuperação de eventos gravados, geração de evidências para apuração de ocorrências e integração com os demais sistemas de segurança implantados.

Poderão ser adotadas, ainda, medidas complementares de proteção perimetral, destinadas à mitigação de riscos relacionados a invasões, vandalismo e danos ao patrimônio público, reforçando a segurança física das instalações institucionais.

O sistema de controle de acesso deverá abranger mecanismos destinados ao gerenciamento automatizado do fluxo de pedestres, assegurando o registro e a rastreabilidade de eventos, a geração de relatórios gerenciais e a integração com os sistemas de segurança eletrônica.

A solução deverá contemplar o controle de acesso nas entradas principais da unidade, bem como em ambientes que demandem restrição específica, tais como áreas administrativas, laboratórios, salas técnicas e demais dependências definidas pela Administração, mediante utilização de catracas eletrônicas, controladores faciais, fechaduras eletromagnéticas e dispositivos complementares.

A utilização de tecnologias biométricas deverá observar os princípios da necessidade, adequação e finalidade previstos na Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), restringindo o tratamento de dados pessoais ao estritamente necessário para fins de segurança institucional.

Os quantitativos previstos para a presente contratação foram definidos a partir de levantamento técnico preliminar realizado para a unidade, considerando a distribuição física dos ambientes, a quantidade estimada de usuários, os requisitos de segurança institucional, a necessidade de expansão futura e a compatibilidade com os padrões corporativos estabelecidos pelo IFSP.

As estimativas contemplam infraestrutura de rede lógica, conectividade sem fio, backbone óptico, videomonitoramento, controle de acesso e demais componentes necessários ao pleno funcionamento da unidade, garantindo capacidade operacional compatível com as necessidades atuais e futuras do Campus Diadema.

Considera-se fundamental que a implantação dessa infraestrutura ocorra de forma integrada às etapas de adequação e estruturação física do Campus Diadema, evitando retrabalhos, incompatibilidades técnicas e intervenções posteriores nas edificações. A execução coordenada da infraestrutura física de telecomunicações, da rede lógica estruturada, do backbone óptico, dos equipamentos ativos de rede e dos sistemas de segurança eletrônica favorece a padronização tecnológica compatível com os padrões institucionais adotados pelo IFSP, possibilita maior eficiência na gestão contratual, promove uniformidade arquitetônica e reduz custos decorrentes de futuras adaptações.

A solução encontra-se estruturada em três grupos tecnicamente integrados, compreendendo: **(i) infraestrutura de rede de dados; (ii) sistema de CFTV; e (iii) sistema de controle de acesso**, incluindo o fornecimento de materiais, equipamentos e serviços técnicos especializados necessários à implantação integral da solução.

Diante do exposto, a contratação mostra-se necessária e estratégica para viabilizar a implantação, estruturação e o início das atividades acadêmicas e administrativas do IFSP – Campus Diadema, garantindo conectividade institucional, segurança física e lógica, governança tecnológica e continuidade dos serviços públicos educacionais, em conformidade com os princípios da eficiência, economicidade, planejamento e interesse público previstos na Lei nº 14.133, de 1º de abril de 2021, além de alinhar-se às políticas públicas de expansão da educação profissional e tecnológica no âmbito do Novo Programa de Aceleração do Crescimento (Novo PAC).

3. Área requisitante

Área Requisitante	Responsável
Direção Geral	176.133.588-01

4. Necessidades de Negócio

A presente contratação visa atender às necessidades institucionais da Direção-Geral do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – IFSP, Campus Diadema, no âmbito das ações de implantação, estruturação e início das atividades acadêmicas e administrativas da unidade, assegurando a disponibilidade de infraestrutura tecnológica e de segurança compatível com os padrões corporativos adotados pelo IFSP.

A expansão da Rede Federal de Educação Profissional, Científica e Tecnológica, impulsionada pelas diretrizes do Novo Programa de Aceleração do Crescimento (Novo PAC), impõe à Administração Pública o dever de garantir que as novas unidades sejam implantadas com infraestrutura de Tecnologia da Informação e Comunicação (TIC) adequada, padronizada, segura e integrada à arquitetura tecnológica institucional existente.

Nesse contexto, torna-se imprescindível a implantação de infraestrutura completa de conectividade, compreendendo rede lógica estruturada, backbone óptico, infraestrutura física de telecomunicações, equipamentos ativos de rede, conectividade sem fio corporativa e mecanismos de segurança perimetral, possibilitando comunicação segura e estável entre os ambientes administrativos e acadêmicos e assegurando a integração com os sistemas corporativos institucionais, tais como plataformas acadêmicas, sistemas administrativos, serviços de autenticação, ambientes colaborativos e demais soluções de gestão utilizadas pelo IFSP.

A implantação da infraestrutura proposta constitui requisito essencial para o adequado funcionamento das atividades finalísticas da instituição, permitindo o desenvolvimento das ações de ensino, pesquisa, extensão e gestão administrativa, além de proporcionar escalabilidade tecnológica e suporte ao crescimento futuro da unidade.

Paralelamente, a implementação dos sistemas de Circuito Fechado de Televisão (CFTV) e de controle de acesso, abrangendo o gerenciamento do fluxo de pedestres e veículos, o controle de áreas restritas e a utilização de tecnologias de reconhecimento facial, atende à necessidade institucional de proteção do patrimônio público, segurança da comunidade acadêmica, rastreabilidade de eventos e mitigação de riscos operacionais.

A utilização de recursos biométricos deverá observar rigorosamente os princípios estabelecidos pela Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), limitando o tratamento de dados pessoais ao estritamente necessário para o atendimento das finalidades relacionadas à segurança institucional.

Sob a perspectiva do negócio institucional, a contratação apresenta caráter estratégico, uma vez que viabiliza a implantação estruturada e padronizada do Campus diadema, assegurando governança tecnológica, interoperabilidade entre sistemas, conformidade com as diretrizes institucionais de segurança da informação e aderência aos princípios do planejamento, da eficiência e da economicidade previstos na Lei nº 14.133, de 1º de abril de 2021.

Dessa forma, a solução proposta não se limita à disponibilização de infraestrutura física de rede e segurança, constituindo elemento estruturante para a operacionalização das atividades acadêmicas e administrativas do IFSP – Campus Diadema, contribuindo para a sustentabilidade tecnológica, a integridade institucional e a consolidação da política pública de expansão da educação profissional, científica e tecnológica no âmbito da Rede Federal.

5. Necessidades Tecnológicas

A contratação deverá atender às necessidades tecnológicas relacionadas à implantação, estruturação e início das atividades acadêmicas e administrativas do **Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – IFSP, Campus Diadema**, assegurando a disponibilidade de infraestrutura de Tecnologia da Informação e Comunicação (TIC) e de segurança compatível com os padrões corporativos adotados pelo IFSP.

A solução deverá assegurar infraestrutura segura, padronizada, escalável e de alto desempenho, permitindo a interligação de ambientes administrativos, acadêmicos e operacionais da unidade, garantindo integração plena com os sistemas institucionais corporativos e com a arquitetura tecnológica adotada pelo IFSP.

A solução tecnológica deverá contemplar os seguintes componentes estruturantes:

a) Infraestrutura de Cabeamento Estruturado Metálico (Horizontal)

A rede lógica interna deverá ser implantada por meio de cabeamento estruturado categoria 6 (Cat6), em conformidade com as normas técnicas aplicáveis (ABNT NBR 14565, ANSI/TIA-568 e ISO/IEC 11801), assegurando:

- suporte a aplicações de dados, voz e imagem em padrão Gigabit Ethernet;
- baixa latência e adequada largura de banda;
- organização padronizada em racks, patch panels e identificação de pontos;
- facilidade de manutenção e expansão futura;
- compatibilidade com alimentação PoE para dispositivos como câmeras IP, access points e demais equipamentos de rede.

Todos os pontos de rede deverão ser certificados, com emissão de relatório técnico que comprove o atendimento aos parâmetros de desempenho exigidos para a categoria especificada.

b) Infraestrutura Física de Telecomunicações

A solução deverá contemplar a implantação da infraestrutura física necessária ao suporte dos sistemas tecnológicos, incluindo eletrocalhas, eletrodutos, canaletas, caixas de passagem, suportes e demais elementos destinados à acomodação, proteção e organização do cabeamento estruturado, observando-se as normas técnicas aplicáveis e possibilitando futuras expansões e manutenções.

c) Backbone Óptico em Fibra Monomodo

Considerando a necessidade de interligação entre racks, edificações ou setores estratégicos da unidade, a solução deverá contemplar backbone óptico em fibra monomodo (SM), garantindo:

- alta capacidade de transmissão de dados;
- imunidade a interferências eletromagnéticas;
- maior estabilidade de enlace;
- baixa atenuação em médias distâncias;
- preparação para futuras ampliações da infraestrutura.

O backbone óptico deverá incluir:

- fornecimento e lançamento de cabo óptico autossustentado (CFOA-AS), quando aplicável em estrutura aérea;
- instalação de Distribuidores Internos Ópticos (DIO);
- execução de emendas por fusão com baixa perda óptica;
- organização adequada das fibras, respeitando o raio mínimo de curvatura;
- testes de continuidade e certificação por meio de OTDR ou equipamento equivalente, com emissão de relatório técnico.

Os enlaces ópticos deverão ser compatíveis com equipamentos ativos dotados de portas SFP, assegurando interoperabilidade entre backbone e switches de rede.

d) Equipamentos Ativos de Rede

A solução deverá incluir switches gerenciáveis, pontos de acesso Wi-Fi corporativos e firewall institucional, capazes de:

- operar em padrão Gigabit Ethernet;
- suportar VLANs (802.1Q), QoS e agregação de links (LACP);
- permitir segmentação lógica da rede;
- garantir segurança por meio de autenticação 802.1X, ACLs e mecanismos de proteção contra ataques de rede;
- integrar-se ao backbone óptico por meio de uplinks SFP compatíveis com fibra monomodo.

O firewall deverá prover inspeção profunda de pacotes (DPI), prevenção de intrusões (IPS), VPN e controle de aplicações, assegurando proteção perimetral e segmentação adequada da rede institucional.

e) Sistema de CFTV IP

O sistema de videomonitoramento deverá ser integralmente baseado em tecnologia IP, integrando-se à infraestrutura lógica implantada, contemplando:

- câmeras IP Full HD ou superior;
- gravação contínua ou por evento;
- armazenamento em NVR com disco rígido projetado para operação 24 horas por dia, 7 dias por semana;
- compatibilidade com protocolo ONVIF;
- acesso remoto autorizado;
- integração com o sistema de controle de acesso.

O tráfego de vídeo deverá ser adequadamente segmentado e priorizado na rede, garantindo estabilidade, desempenho e qualidade de gravação.

A solução poderá contemplar medidas complementares de proteção perimetral destinadas à mitigação de riscos relacionados a invasões, vandalismo e danos ao patrimônio público.

f) Sistema de Controle de Acesso

O sistema de controle de acesso deverá operar em rede TCP/IP, integrado à infraestrutura lógica e ao sistema de CFTV, permitindo:

- reconhecimento facial;
- cadastro e gerenciamento centralizado de usuários;
- definição de perfis e níveis hierárquicos;
- registro e auditoria de eventos;
- aplicação de políticas como anti-passback;
- integração com APIs para sistemas institucionais.

A solução deverá contemplar o controle de acesso de pedestres e veículos, incluindo catracas eletrônicas, cancelas automáticas, controladores faciais, fechaduras eletromagnéticas e demais dispositivos necessários ao gerenciamento seguro dos acessos à unidade.

O sistema deverá operar em plataforma web, com armazenamento seguro e disponibilidade contínua, assegurando rastreabilidade e governança sobre os acessos às instalações.

g) Segurança da Informação e Conformidade

A infraestrutura tecnológica deverá atender aos princípios de:

- confidencialidade;
- integridade;
- disponibilidade;
- autenticidade;
- rastreabilidade.

Deverá estar alinhada às diretrizes da Política de Segurança da Informação do IFSP, à Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e às boas práticas previstas na ABNT NBR ISO/IEC 27001, garantindo proteção de dados institucionais e pessoais.

h) Escalabilidade e Sustentabilidade Tecnológica

A arquitetura da solução deverá ser modular e escalável, permitindo:

- ampliação futura de pontos de rede;
- inclusão de novas câmeras e dispositivos;
- expansão do backbone óptico;
- expansão dos sistemas de controle de acesso;
- atualização de equipamentos ativos sem necessidade de reestruturação integral da infraestrutura.

A solução deverá priorizar padronização tecnológica institucional, facilidade de manutenção, racionalização de custos operacionais e compatibilidade com a arquitetura de TIC adotada pelo IFSP.

Síntese

As necessidades tecnológicas identificadas demandam a implantação de infraestrutura convergente, integrada e padronizada, composta por infraestrutura física de telecomunicações, cabeamento estruturado metálico, backbone óptico, equipamentos ativos de rede, sistema de CFTV IP e controle de acesso, assegurando desempenho adequado, segurança física e lógica, interoperabilidade, governança tecnológica e sustentabilidade da infraestrutura de TIC necessária ao pleno funcionamento do IFSP – Campus Diadema.

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

A solução a ser escolhida fundamenta-se na necessidade institucional de prover infraestrutura tecnológica moderna, integrada, segura e padronizada, destinada à implantação, estruturação e início das atividades acadêmicas e administrativas do **Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – IFSP**, Campus Diadema, localizado na Avenida Sete de Setembro, nº 1670, Centro, Município de Diadema/SP, CEP 09912-010 em conformidade com os padrões corporativos de Tecnologia da Informação e Comunicação adotados institucionalmente pelo IFSP.

Entre os requisitos observados para a definição da solução de TIC estão:

Compatibilidade com a infraestrutura lógica e de rede utilizada pelo IFSP, garantindo interoperabilidade e integração com os sistemas corporativos institucionais;

Observância às normas técnicas aplicáveis de cabeamento estruturado, especialmente ABNT NBR 14565, ANSI/TIA-568, ISO/IEC 11801 e correlatas, bem como às normas de segurança elétrica, trabalho em altura, telecomunicações e demais regulamentos técnicos aplicáveis;

Utilização de materiais, componentes e equipamentos certificados, com garantia de desempenho, rastreabilidade, procedência e conformidade com os padrões de qualidade exigidos pelo IFSP;

Solução escalável e modular, que permita futuras ampliações, adequações e substituições parciais sem necessidade de reestruturação completa da infraestrutura implantada;

Implantação de infraestrutura física de telecomunicações, composta por eletrocalhas, eletrodutos, canaletas, caixas de passagem, suportes, fixações e demais elementos necessários à acomodação, proteção e organização dos sistemas tecnológicos;

Implantação de cabeamento estruturado metálico categoria 6, destinado ao atendimento horizontal dos ambientes administrativos, acadêmicos, laboratórios, salas técnicas, áreas de convivência e demais espaços institucionais;

Implantação de backbone óptico em fibra monomodo, incluindo fornecimento e lançamento de cabo óptico, instalação de Distribuidores Internos Ópticos — DIO, execução de emendas por fusão, organização das fibras, testes de continuidade, atenuação e certificação óptica;

Fornecimento, instalação, configuração e validação de equipamentos ativos de rede, incluindo switches gerenciáveis, pontos de acesso sem fio corporativos e solução de segurança perimetral, compatíveis com os padrões tecnológicos adotados pelo IFSP;

Integração dos sistemas de CFTV, controle de acesso, catracas eletrônicas, controladores faciais, fechaduras eletromagnéticas e cancelas automáticas à rede lógica do campus, com acesso controlado, autenticação de usuários e comunicação baseada em protocolo TCP/IP;

Atendimento aos requisitos de segurança da informação, confidencialidade, disponibilidade, integridade, autenticidade e rastreabilidade dos dados trafegados e armazenados nos sistemas;

Elaboração de projeto técnico executivo detalhado, contemplando topologia da rede, distribuição dos pontos de telecomunicações, infraestrutura física, backbone óptico, localização de racks, switches, access points, câmeras, catracas, controladores faciais, cancelas, fechaduras eletromagnéticas, pontos de energia e demais componentes da solução;

Realização de testes, certificações, validações e homologação técnica da solução implantada, com entrega de relatório técnico validando a conformidade da instalação, o desempenho da rede, a conectividade dos equipamentos, o funcionamento dos sistemas de CFTV e controle de acesso e a integração entre os subsistemas.

Requisitos de Qualificação Técnica

Considerando a natureza e a criticidade do objeto, que envolve a implantação de infraestrutura de rede, backbone óptico, CFTV, controle de acesso, segurança perimetral e integração de sistemas, são estabelecidos requisitos complementares de qualificação técnica, devidamente descritos e justificados a seguir:

a) Certificações Técnicas e Conformidade Normativa

Descrição:

Comprovar que a solução tecnológica, os equipamentos, os softwares e, quando aplicável, os ambientes de hospedagem utilizados pelo sistema atendem a padrões de qualidade, segurança, desempenho, disponibilidade e conformidade técnica reconhecidos nacional e internacionalmente.

A solução deverá observar as normas técnicas aplicáveis ao objeto, especialmente aquelas relacionadas a cabeamento estruturado, telecomunicações, infraestrutura óptica, segurança elétrica, trabalho em altura, sistemas IP, segurança da informação e proteção de dados.

Quando a solução de software de controle de acesso, CFTV ou gerenciamento centralizado for ofertada em ambiente de nuvem ou Datacenter externo, deverá ser comprovado que a infraestrutura de hospedagem atende aos requisitos mínimos de disponibilidade, continuidade operacional e segurança, mediante a apresentação de uma das seguintes alternativas:

I – Certificação Tier III (ou superior), conforme a norma ANSI/TIA-942, aplicável ao Datacenter onde a solução estiver hospedada;

OU

II – Documento emitido pelo organismo certificador ou pelo operador do Datacenter que comprove que o ambiente de hospedagem da solução ofertada possui certificações válidas ISO 22301, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 e SOC 2.

Deverão ser apresentados, quando aplicável:

- Certificados de conformidade técnica dos equipamentos ofertados;
- Comprovação de atendimento às normas técnicas aplicáveis de cabeamento estruturado, telecomunicações e segurança elétrica;
- Documentação comprobatória referente à infraestrutura de hospedagem da solução, observando uma das alternativas previstas neste item;
- Documentos técnicos dos fabricantes que demonstrem compatibilidade, desempenho, recursos de segurança, protocolos suportados e requisitos de operação.

Justificativa:

A exigência assegura que a solução ofertada possua qualidade técnica, desempenho, segurança, confiabilidade e disponibilidade compatíveis com a criticidade do ambiente institucional do IFSP – Campus Carapicuíba. A implantação de um campus exige infraestrutura tecnológica estável desde o início de suas atividades, evitando interrupções operacionais, falhas de conectividade, indisponibilidade de serviços acadêmicos e administrativos e riscos à segurança física e lógica da unidade.

No caso de sistemas hospedados externamente, a comprovação de infraestrutura adequada de Datacenter reduz riscos de falhas, perdas de dados, interrupções operacionais e incidentes de segurança, garantindo continuidade dos serviços de controle de acesso, videomonitoramento e gestão centralizada dos dispositivos.

Considerando que atualmente existem diferentes modelos de certificação internacionalmente reconhecidos capazes de demonstrar elevados níveis de disponibilidade, continuidade operacional e segurança da informação, a Administração optou por admitir formas alternativas de comprovação da infraestrutura de hospedagem da solução SaaS. A medida amplia a competitividade do certame sem comprometer a segurança da contratação, preservando a exigência de padrões técnicos compatíveis com a criticidade da solução tecnológica pretendida.

Fundamentos normativos:

- Lei nº 14.133/2021, especialmente quanto à exigência de comprovações técnicas compatíveis com a complexidade do objeto;
- Normas técnicas ABNT NBR 14565, ANSI/TIA-568, ISO/IEC 11801 e ANSI/TIA-942, quando aplicáveis;
- ISO 22301 – Sistema de Gestão de Continuidade de Negócios;
- ISO/IEC 27001 – Sistema de Gestão da Segurança da Informação;
- ISO/IEC 27017 – Controles de Segurança para Serviços em Nuvem;
- ISO/IEC 27018 – Proteção de Dados Pessoais em Serviços de Computação em Nuvem;
- SOC 2 – Service Organization Control 2;
- Normas Regulamentadoras NR-10 e NR-35, quando aplicáveis;
- Diretrizes institucionais de TIC, segurança da informação e governança tecnológica do IFSP.

b) Declaração de Revenda Autorizada ou Representação Comercial

Descrição

Assegurar que a empresa proponente seja revendedora oficialmente autorizada, representante comercial legítima ou parceira reconhecida do fabricante ou detentor dos direitos de comercialização dos equipamentos, softwares, licenças, appliances, controladores, câmeras, catracas, dispositivos biométricos, sistemas de gerenciamento e demais componentes críticos ofertados, quando aplicável.

Deverão ser apresentados:

- Declaração de revenda autorizada, representação comercial ou autorização de fornecimento válida, emitida pelo fabricante, distribuidor oficial ou detentor dos direitos de comercialização da solução;
- A declaração deverá ter sido emitida há, no mínimo, 6 (seis) meses antes da data da sessão pública da licitação, permanecendo válida na data de apresentação da proposta;
- A declaração deverá ser emitida em documento oficial do fabricante, distribuidor oficial ou representante legalmente autorizado, contendo elementos que permitam a verificação de sua autenticidade, tais como assinatura eletrônica verificável, assinatura digital, assinatura física acompanhada da identificação do emitente, código de validação, endereço eletrônico institucional ou outro meio idôneo de confirmação;
- Documentação técnica ou comercial que comprove a origem regular dos produtos, licenças e softwares ofertados;
- Quando aplicável, comprovação de que a licitante possui acesso ao suporte técnico oficial, atualizações de software, garantias e canais formais de atendimento disponibilizados pelo fabricante.

Justificativa

Considerando que o objeto da contratação compreende o fornecimento de equipamentos, softwares e serviços cuja garantia, atualização tecnológica, suporte técnico especializado, fornecimento de peças, componentes originais e manutenção da solução dependem do relacionamento formal entre o fabricante e a empresa fornecedora, justifica-se a exigência de apresentação de Declaração de Revenda Autorizada emitida pelo fabricante, distribuidor oficial ou representante legalmente autorizado.

A exigência de que a declaração tenha sido emitida há, no mínimo, 6 (seis) meses antes da data da sessão pública busca evidenciar que o relacionamento comercial entre a licitante e o fabricante não foi constituído exclusivamente para participação no certame, reduzindo o risco de apresentação de autorizações eventuais, precárias ou emitidas apenas para atender à presente licitação, sem demonstrar efetiva capacidade de manter suporte técnico continuado durante toda a execução contratual.

A manutenção de relacionamento comercial previamente estabelecido proporciona maior segurança à Administração quanto ao fornecimento regular dos equipamentos e softwares, ao acesso aos canais oficiais de suporte técnico, ao fornecimento de atualizações, ao cumprimento das garantias do fabricante e à disponibilidade de peças e componentes originais durante toda a vigência do contrato, reduzindo riscos de descontinuidade dos serviços, indisponibilidade da solução tecnológica e prejuízos ao interesse público.

A possibilidade de verificação da autenticidade da declaração por diferentes meios, não se restringindo exclusivamente à assinatura digital, visa preservar a ampla competitividade do certame sem comprometer a segurança documental, permitindo à Administração realizar diligências para confirmação da autenticidade do documento sempre que entender necessário.

Dessa forma, a exigência mostra-se compatível com a complexidade da contratação e constitui medida preventiva de gestão de riscos destinada a assegurar maior segurança na execução contratual, observando os princípios do planejamento, da eficiência, da segurança da contratação, da continuidade do serviço público e da seleção da proposta mais vantajosa previstos na Lei nº 14.133/2021.

Fundamentos normativos

- Lei nº 14.133/2021, especialmente quanto à qualificação técnica, gestão de riscos, planejamento da contratação e seleção da proposta mais vantajosa;
- Lei nº 9.609/1998, quando envolver programas de computador;

- Lei nº 9.610/1998, quando aplicável aos direitos autorais;
- Diretrizes institucionais de governança de TIC, segurança da informação e gestão de riscos do IFSP.

c) Teste de Penetração (Pentest)

Descrição

Comprovar que a solução de software ofertada foi submetida à avaliação especializada de segurança cibernética, mediante a realização de Teste de Penetração (Penetration Test – Pentest), com o objetivo de identificar vulnerabilidades, avaliar a efetividade dos controles de segurança implementados e demonstrar a adoção de boas práticas de proteção da informação.

Deverão ser apresentados

- Relatório técnico ou declaração emitida pela empresa responsável pela execução do Teste de Penetração (Pentest), comprovando que a solução ofertada foi submetida à avaliação de segurança cibernética;
- O teste deverá ter sido realizado há, no máximo, 12 (doze) meses em relação à data da sessão pública da licitação;
- O documento deverá identificar a solução avaliada, a data de realização do teste e a empresa responsável por sua execução.

Justificativa

O Teste de Penetração (Pentest) constitui prática reconhecida internacionalmente para avaliação da segurança de aplicações, sistemas computacionais e ambientes tecnológicos, permitindo a identificação de vulnerabilidades, falhas de configuração e potenciais riscos de exploração por agentes maliciosos, bem como a verificação da efetividade dos controles de segurança implementados.

A exigência de comprovação da realização de Teste de Penetração emitido há, no máximo, 12 (doze) meses antes da data da sessão pública da licitação visa assegurar que a plataforma ofertada tenha sido submetida recentemente à avaliação especializada de segurança cibernética, refletindo condições compatíveis com o cenário atual de ameaças e vulnerabilidades.

Considerando que a solução objeto da contratação compreende sistema de gerenciamento de controle de acesso, videomonitoramento e demais componentes tecnológicos que poderão processar dados pessoais, registros de acesso, imagens e informações sensíveis relacionadas à segurança patrimonial e institucional do IFSP, mostra-se imprescindível que a plataforma demonstre adequado nível de segurança da informação, reduzindo riscos de acessos não autorizados, indisponibilidade dos serviços, comprometimento da integridade dos dados e incidentes de segurança.

A adoção do prazo máximo de 12 (doze) meses observa os princípios da razoabilidade e da proporcionalidade, considerando a constante evolução das ameaças cibernéticas, a necessidade de atualização contínua dos sistemas e a importância de que a avaliação reflita condições atuais da solução ofertada, sem impor restrição desproporcional à competitividade do certame.

A exigência encontra fundamento nas boas práticas de governança de Tecnologia da Informação, na gestão de riscos, nas diretrizes de segurança da informação e na proteção de dados pessoais previstas na Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD), bem como nos princípios do planejamento, da eficiência, da segurança da contratação e da seleção da proposta mais vantajosa estabelecidos pela Lei nº 14.133/2021.

Fundamentos normativos

- Lei nº 14.133/2021;
- Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD);
- Boas práticas de Segurança da Informação e Segurança Cibernética aplicáveis à Administração Pública;
- Diretrizes institucionais de governança e gestão de riscos em TIC.

d) Comprovação de Profissionais Capacitados em NR-10 e NR-35

Descrição:

Garantir que as atividades que envolvam instalações elétricas, lançamento de cabeamento estruturado, montagem de racks, instalação de equipamentos de rede, câmeras, dispositivos de controle de acesso e demais serviços executados em altura ou com risco elétrico sejam realizadas por profissionais devidamente capacitados, em conformidade com as Normas Regulamentadoras expedidas pelo Ministério do Trabalho e Emprego.

Deverão ser apresentados:

- Comprovação de que a licitante dispõe de profissional(is) com certificado de capacitação válido em NR-10 – Segurança em Instalações e Serviços em Eletricidade, para execução das atividades que envolvam instalações elétricas ou risco elétrico;
- Comprovação de que a licitante dispõe de profissional(is) com certificado de capacitação válido em NR-35 – Trabalho em Altura, para execução das atividades realizadas em altura, quando aplicáveis;
- As capacitações em NR-10 e NR-35 poderão ser comprovadas por profissionais distintos, desde que a licitante demonstre possuir equipe apta a executar todas as atividades previstas na contratação.
- Os certificados poderão ser apresentados com ocultação (tarja) dos dados pessoais não essenciais, preservando-se as informações necessárias para verificação da autenticidade, validade da capacitação e identificação da norma regulamentadora correspondente, em observância à Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

Justificativa:

A presente contratação contempla serviços especializados que envolvem instalações elétricas, lançamento de cabeamento estruturado, instalação de equipamentos de telecomunicações, montagem de racks, instalação de câmeras, dispositivos de controle de acesso, infraestrutura de rede e demais atividades que, por sua natureza, demandam a observância obrigatória das Normas Regulamentadoras NR-10 e NR-35, visando à proteção da integridade física dos trabalhadores, da comunidade acadêmica e do patrimônio público.

Diante da complexidade técnica da solução e da necessidade de início imediato da execução contratual após a emissão da ordem de serviço, mostra-se necessário que a comprovação da existência de profissionais devidamente capacitados ocorra na fase de habilitação, evidenciando que a licitante já dispõe de capacidade operacional compatível com a execução do objeto.

A exigência não possui a finalidade de restringir a competitividade ou vincular nominalmente os profissionais à futura execução contratual, mas de assegurar que a empresa participante já possua estrutura técnica mínima apta a iniciar os serviços de forma segura, eficiente e em conformidade com a legislação de segurança do trabalho, reduzindo os riscos inerentes à contratação.

Caso a verificação da capacitação fosse postergada para momento posterior à assinatura do contrato e a empresa contratada não dispusesse de profissionais habilitados para execução das atividades sujeitas às Normas Regulamentadoras aplicáveis, a Administração seria obrigada a promover notificações, conceder prazo para regularização, instaurar procedimentos administrativos sancionatórios e, eventualmente, rescindir o contrato, ocasionando atrasos na implantação da infraestrutura tecnológica do campus, comprometimento do cronograma institucional, aumento dos custos administrativos e necessidade de realização de nova contratação.

Assim, a comprovação da disponibilidade de profissionais capacitados na fase de habilitação constitui medida preventiva de gestão de riscos, proporcional à natureza e à complexidade do objeto, destinada a assegurar que a futura contratada possua condições técnicas imediatas para executar os serviços contratados com segurança, qualidade e observância da legislação aplicável.

A comprovação da qualificação dos profissionais na fase de habilitação não impede sua substituição durante a execução contratual, desde que os profissionais substitutos possuam capacitação equivalente e atendam integralmente às exigências das Normas Regulamentadoras aplicáveis, preservando-se, durante toda a execução do contrato, o nível de qualificação técnica exigido pela Administração.

Fundamentos normativos:

- Lei nº 14.133/2021, especialmente art. 67, relativo à qualificação técnica compatível com a complexidade do objeto;
- Norma Regulamentadora nº 10 – Segurança em Instalações e Serviços em Eletricidade;
- Norma Regulamentadora nº 35 – Trabalho em Altura;
- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);
- Demais normas de segurança do trabalho aplicáveis.

e) Registro de Programa de Computador / Propriedade Intelectual

Descrição

Assegurar que a solução de software ofertada seja regularmente comercializada no território nacional, possua origem identificável, legitimidade para sua comercialização e esteja protegida quanto aos direitos de propriedade intelectual e industrial, proporcionando maior segurança jurídica à Administração durante toda a execução contratual.

Deverão ser apresentados

- Certificado de registro da marca expedido pelo Instituto Nacional da Propriedade Industrial (INPI); ou
- Comprovante de depósito do respectivo pedido de registro perante o INPI; ou
- Documento emitido pelo titular da marca autorizando sua utilização e comercialização pela licitante.

Quando aplicável, a Administração poderá promover diligências para confirmação da autenticidade e da validade da documentação apresentada.

Justificativa

Considerando que a presente contratação contempla o fornecimento de solução de software destinada ao gerenciamento centralizado dos sistemas de controle de acesso, videomonitoramento e demais componentes tecnológicos da infraestrutura de Tecnologia da Informação e Comunicação (TIC), justifica-se a exigência de comprovação da regularidade da marca vinculada ao software ofertado, mediante apresentação do certificado de registro perante o Instituto Nacional da Propriedade Industrial (INPI), do comprovante de depósito do respectivo pedido de registro ou de documento emitido pelo titular autorizando sua utilização e comercialização.

A medida visa conferir maior segurança jurídica à Administração quanto à origem, legitimidade e regularidade da solução de software ofertada, reduzindo riscos relacionados à violação de direitos de propriedade intelectual e industrial, à utilização indevida de marcas, à ocorrência de litígios entre desenvolvedores, fabricantes, representantes ou distribuidores e à eventual descontinuidade do suporte técnico, das atualizações, da manutenção corretiva, evolutiva ou do licenciamento do software durante toda a execução contratual.

A exigência busca assegurar que a Administração Pública contrate solução regularmente identificada no mercado nacional, cuja titularidade da marca ou autorização para sua utilização e comercialização possa ser objetivamente demonstrada, proporcionando maior confiabilidade quanto à continuidade do fornecimento, da evolução tecnológica, do suporte especializado e da manutenção da solução durante toda a vigência contratual.

A exigência não possui caráter restritivo à competitividade, uma vez que poderá ser atendida mediante a apresentação do certificado de registro da marca expedido pelo INPI, do comprovante de depósito do respectivo pedido de registro ou de documento emitido pelo titular autorizando a utilização e comercialização da marca

vinculada ao software ofertado. Dessa forma, preservam-se os princípios da isonomia, da ampla competitividade, da proporcionalidade, da segurança da contratação e da seleção da proposta mais vantajosa, previstos na Lei nº 14.133/2021.

O registro da marca perante o INPI constitui importante instrumento de segurança jurídica nas relações comerciais envolvendo soluções de software, conferindo publicidade à titularidade do sinal distintivo e reduzindo riscos de conflitos relacionados à identidade comercial da solução ofertada. A exigência complementa os mecanismos de proteção à propriedade intelectual e industrial aplicáveis ao software, contribuindo para que a Administração contrate solução regularmente disponibilizada no mercado, com origem identificável, suporte oficial e continuidade de evolução tecnológica.

Fundamentos normativos

- Lei nº 14.133/2021;
- Lei nº 9.279, de 14 de maio de 1996 (Lei da Propriedade Industrial);
- Lei nº 9.609, de 19 de fevereiro de 1998 (Lei do Software);
- Lei nº 9.610, de 19 de fevereiro de 1998 (Lei de Direitos Autorais);
- Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

f) Prova de Conceito da Solução — PoC

Dada a natureza tecnológica e a complexidade da solução pretendida — que envolve a integração entre sistemas de controle de acesso, CFTV, catracas eletrônicas, controladores faciais, cancelas automáticas, infraestrutura de rede lógica, equipamentos ativos e gestão centralizada dos dispositivos — faz-se necessária a realização de uma Prova de Conceito — PoC, Proof of Concept, antes da implantação definitiva da solução.

A Prova de Conceito consiste na demonstração técnica prática das funcionalidades e capacidades da solução ofertada pela licitante, em ambiente controlado, simulando as condições reais de operação e integração com os sistemas institucionais do IFSP.

Esse procedimento tem por objetivo validar previamente se a solução proposta atende aos requisitos funcionais, técnicos, operacionais, de segurança e de desempenho estabelecidos neste Estudo Técnico Preliminar e que serão detalhados no Termo de Referência.

A realização da PoC permite verificar, de forma empírica, aspectos cruciais como:

Interoperabilidade e compatibilidade da solução com a infraestrutura tecnológica do IFSP;

Estabilidade, desempenho e tempo de resposta dos equipamentos e sistemas;

Integração entre os módulos de CFTV, controle de acesso e rede lógica;

Funcionamento das catracas eletrônicas, controladores faciais, mecanismos de autenticação e dispositivos de gerenciamento de acesso;

Compatibilidade com protocolos abertos, tais como TCP/IP, ONVIF, RTSP, HTTPS, APIs de integração e demais protocolos aplicáveis;

Atendimento aos requisitos de segurança da informação, incluindo autenticação, criptografia, segregação de perfis de acesso, controle de privilégios, registro de logs e rastreabilidade de eventos;

Aderência às normas técnicas e aos padrões institucionais de TIC;

Usabilidade, ergonomia e facilidade de operação da interface administrativa do sistema;

Geração de relatórios gerenciais, trilhas de auditoria, registros de acesso e eventos operacionais;

Capacidade de integração entre controle de acesso, videomonitoramento e gestão centralizada dos dispositivos;

Capacidade de expansão futura e parametrização de novos usuários, dispositivos, perfis e ambientes.

A PoC restringir-se-á à demonstração dos componentes lógicos, softwares, equipamentos ativos e funcionalidades de integração da solução, não sendo exigida a reprodução integral da infraestrutura física prevista na contratação, tais como cabeamento estruturado, backbone óptico, lançamento de fibra, eletrocalhas, eletrodutos, canaletas, caixas de passagem ou demais serviços de instalação civil, elétrica e eletromecânica.

Além de ser um instrumento de comprovação técnica, a PoC atua como mecanismo preventivo de mitigação de riscos contratuais, evitando a contratação de soluções que, embora formalmente conformes na fase de habilitação, não demonstrem, na prática, a capacidade de atender aos requisitos do IFSP.

A experiência acumulada em contratações públicas de TIC demonstra que muitos riscos de incompatibilidade tecnológica, instabilidade, limitações funcionais, falhas de integração e insuficiência de desempenho somente são identificados durante testes práticos prévios, razão pela qual a Prova de Conceito se justifica como etapa indispensável no planejamento da contratação.

A exigência da PoC é proporcional e adequada à complexidade técnica da contratação, não restringindo a competitividade, mas garantindo que apenas soluções efetivamente compatíveis e validadas tecnicamente sejam implantadas.

Tal procedimento também assegura transparência, isonomia e objetividade na avaliação técnica, pois as condições de teste deverão ser previamente definidas no Termo de Referência e acompanhadas por servidores designados pela Administração.

O resultado da PoC servirá como comprovação de atendimento aos requisitos funcionais e técnicos mínimos e integrará o processo decisório da fase de julgamento da proposta, conforme modelo a ser detalhado no Termo de Referência.

A não demonstração de conformidade técnica durante a PoC implicará reprovação técnica da solução ofertada, observadas as regras previstas no edital, no Termo de Referência, na legislação vigente e nos princípios do contraditório, da ampla defesa, da isonomia e do julgamento objetivo.

Essa exigência encontra respaldo legal e normativo nos seguintes dispositivos:

Lei nº 14.133/2021, especialmente quanto à possibilidade de exigência de demonstrações práticas, comprovações técnicas e aferição de compatibilidade da solução com as necessidades da Administração;

Dispositivos da Lei nº 14.133/2021 relativos ao planejamento da contratação, à qualificação técnica, à seleção da proposta mais vantajosa e à mitigação de riscos;

Normativos federais aplicáveis às contratações de TIC, quando cabíveis;

PDTIC do IFSP, especialmente quanto aos objetivos relacionados à padronização tecnológica, segurança da informação, interoperabilidade, gestão de riscos e governança de TIC;

Estudo Técnico Preliminar, que prevê a necessidade de validação técnica, mitigação de riscos e garantia de interoperabilidade.

Dessa forma, a Prova de Conceito é instrumento técnico de avaliação e mitigação de riscos plenamente justificado, garantindo que a solução a ser contratada esteja em conformidade com os padrões institucionais de TIC, atenda aos requisitos de segurança e integração e seja tecnicamente viável para operação no ambiente do IFSP — Campus Diadema.

Esses requisitos asseguram que a solução escolhida seja tecnicamente adequada, suficiente para atender às demandas do campus e compatível com os padrões corporativos e de governança de TIC do IFSP, garantindo eficiência, segurança e sustentabilidade da infraestrutura implantada.

g) Justificativa para a Não Adoção do Sistema de Registro de Preços — SRP

Considerando as características do objeto e a necessidade de implantação integrada das soluções de infraestrutura de rede, backbone óptico, equipamentos ativos, CFTV e controle de acesso no IFSP — Campus Diadema, não se aplica a utilização do Sistema de Registro de Preços — SRP.

A adoção do SRP pressupõe fornecimento parcelado, padronizado, recorrente ou demanda futura incerta, condições que não se verificam neste caso, uma vez que a execução deverá ocorrer de forma planejada, específica, coordenada e vinculada ao cronograma de implantação, estruturação e início das atividades acadêmicas e administrativas do Campus Diadema.

A contratação pretendida possui escopo previamente definido e quantitativos determinados a partir de levantamento técnico específico da unidade, considerando a distribuição física dos ambientes, a quantidade estimada de pontos de rede, câmeras, controladores, catracas, cancelas, racks, equipamentos ativos, enlaces ópticos, infraestrutura física e demais componentes necessários à operacionalização da unidade.

Não se trata, portanto, de aquisição destinada à formação de estoque, atendimento de demandas futuras indeterminadas, fornecimento eventual a múltiplas unidades ou contratação de bens comuns de consumo recorrente. Trata-se de solução específica de implantação de infraestrutura tecnológica e de segurança para uma unidade determinada, com escopo certo, prazo definido e necessidade vinculada à ativação institucional do campus.

Ademais, a natureza do objeto envolve instalação física, configuração lógica, integração entre subsistemas, testes, certificações, validação técnica e comissionamento conjunto da solução. Esses elementos demandam planejamento executivo, compatibilidade técnica e responsabilidade coordenada sobre a implantação, circunstâncias que não se harmonizam com a lógica típica do Sistema de Registro de Preços.

A adoção do SRP poderia gerar riscos de descontinuidade da execução, fragmentação da responsabilidade técnica, incompatibilidade entre etapas de fornecimento e instalação, dificuldade de compatibilização com o cronograma de implantação do campus e aumento dos riscos operacionais relacionados à integração entre rede, CFTV e controle de acesso.

Assim, a contratação específica mostra-se a forma mais eficiente, adequada e vantajosa para a Administração, por permitir a execução planejada e integral da solução, com controle sobre prazos, responsabilidades, garantias, testes, certificações e homologação.

Dessa forma, fica justificada a não adoção do Sistema de Registro de Preços, uma vez que a contratação específica revela-se mais adequada sob os aspectos técnico, operacional, econômico e institucional, em consonância com os princípios do planejamento, da eficiência, da economicidade, da segurança jurídica e da seleção da proposta mais vantajosa previstos na Lei nº 14.133/2021.

h) Princípios da Padronização e do Parcelamento

Em atendimento aos princípios da padronização, do planejamento, da eficiência, da economicidade, da competitividade e da obtenção da proposta mais vantajosa, foram avaliados os aspectos relacionados à padronização e ao parcelamento do objeto no contexto desta contratação.

Quanto à padronização, verificou-se que a solução proposta deve manter compatibilidade técnica, lógica e operacional com a infraestrutura e os sistemas institucionais de TIC do IFSP, em observância às diretrizes de interoperabilidade, segurança da informação, gestão de riscos e governança tecnológica.

A adoção de padrões corporativos garante uniformidade de arquitetura, facilidade de manutenção, integração com sistemas legados e sistemas institucionais, racionalização de custos futuros, maior eficiência no suporte técnico, redução de riscos de incompatibilidade e preservação da continuidade dos serviços.

A padronização é especialmente relevante no presente caso, pois a solução envolve múltiplos subsistemas interdependentes, incluindo rede lógica, backbone óptico, equipamentos ativos, firewall, Wi-Fi corporativo, CFTV,

controle de acesso, catracas, controladores faciais, cancelas automáticas e software de gerenciamento. A compatibilidade entre esses elementos é condição essencial para o funcionamento adequado, seguro e sustentável da infraestrutura tecnológica do campus.

Em relação ao parcelamento, avaliou-se que o objeto possui componentes distintos, mas fortemente integrados do ponto de vista técnico e operacional. Embora seja possível identificar subsistemas como rede de dados, CFTV e controle de acesso, a execução da solução depende da compatibilidade entre infraestrutura física, rede lógica, equipamentos ativos, endereçamento, segmentação, autenticação, energia, conectividade, armazenamento, videomonitoramento e controle de eventos.

O fracionamento inadequado da contratação poderia acarretar riscos de incompatibilidade entre equipamentos e softwares, perda de desempenho, dificuldades de integração, sobreposição de garantias, indefinição de responsabilidades técnicas, atrasos na implantação, necessidade de retrabalho, aumento de custos indiretos e prejuízos à interoperabilidade da solução.

A implantação coordenada da infraestrutura permite melhor controle técnico, responsabilidade integrada sobre a entrega, uniformidade na documentação, padronização dos testes, compatibilidade entre os subsistemas e maior segurança na homologação final da solução.

Dessa forma, a estratégia de contratação deverá observar a solução que melhor atenda ao interesse público, podendo a Administração estruturar o objeto de modo a preservar a competitividade sem comprometer a integração técnica, a segurança operacional, a gestão das garantias, a eficiência da fiscalização e a sustentabilidade tecnológica da solução.

Caso se opte pela contratação em lote único, a justificativa técnica repousará na necessidade de preservar a interoperabilidade, a responsabilidade técnica unificada, a compatibilidade entre os subsistemas e a coordenação simultânea da implantação.

Caso a Administração opte por dividir o objeto em grupos ou lotes, a modelagem deverá assegurar que os lotes mantenham coerência técnica, evitando fragmentação excessiva, sobreposição de responsabilidades, incompatibilidades e prejuízos à integração final da solução.

Assim, a decisão quanto ao parcelamento deverá observar, no Termo de Referência, a vantajosidade concreta para a Administração, a preservação da competitividade, a economicidade, a viabilidade técnica e a segurança da implantação, em conformidade com a Lei nº 14.133/2021.

Dessa forma, os requisitos listados acima asseguram que a solução escolhida seja tecnicamente adequada, suficiente para atender às demandas do IFSP — Campus Diadema e compatível com os padrões corporativos e de governança de TIC do IFSP, garantindo eficiência, segurança, interoperabilidade, sustentabilidade tecnológica, proteção patrimonial e suporte adequado ao início das atividades acadêmicas e administrativas da unidade.

7. Estimativa da demanda - quantidade de bens e serviços

A presente contratação tem por objetivo atender às necessidades institucionais do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – IFSP, **Campus Diadema**, no contexto da implantação e estruturação da unidade, visando viabilizar o início das atividades acadêmicas e administrativas. A solução contempla a implantação da infraestrutura de Tecnologia da Informação e Comunicação (TIC), incluindo rede lógica, cabeamento estruturado, backbone óptico, equipamentos ativos de rede, conectividade sem fio, firewall, sistema de videomonitoramento (CFTV), sistema de controle de acesso, bem como os serviços técnicos especializados de instalação, configuração, integração, testes, validação e homologação.

A estimativa da demanda foi elaborada com base em levantamento técnico preliminar realizado para o **Campus Diadema**, considerando a configuração física da unidade, os ambientes administrativos e acadêmicos, laboratórios, salas de aula, áreas técnicas, áreas de circulação, acessos de pedestres e veículos, pontos estratégicos de monitoramento e demais espaços necessários ao pleno funcionamento institucional.

Os quantitativos foram dimensionados de forma a garantir o atendimento das necessidades atuais do campus, assegurando a integração entre a infraestrutura de rede e os sistemas de segurança eletrônica. O

dimensionamento considerou a interoperabilidade entre os subsistemas de conectividade, videomonitoramento, controle de acesso e segurança perimetral, observando ainda critérios de padronização tecnológica, escalabilidade da solução, facilidade de gerenciamento e compatibilidade com a arquitetura corporativa de TIC adotada pelo IFSP.

A solução compreende o fornecimento de materiais, equipamentos e serviços necessários à implantação integral da infraestrutura tecnológica da unidade, abrangendo cabeamento estruturado metálico categoria 6, backbone óptico em fibra monomodo, racks, patch panels, organizadores, switches, pontos de acesso Wi-Fi corporativo, firewall, sistema de CFTV com câmeras IP, gravador de vídeo em rede (NVR) e armazenamento dedicado, sistema de controle de acesso com catracas, controladores faciais, cancelas automáticas, fechaduras eletromagnéticas, software de gerenciamento, infraestrutura complementar e todos os serviços de instalação, configuração, integração, testes, validação e homologação.

As quantidades estimadas encontram-se consolidadas nos **Grupos 1, 2 e 3**, conforme demonstrado a seguir.

Grupo 01 – Rede e Infraestrutura de TI

O Grupo 01 contempla os equipamentos, materiais e serviços necessários à implantação da infraestrutura de Tecnologia da Informação e Comunicação (TIC) do Campus Diadema, compreendendo cabeamento estruturado categoria 6, backbone óptico em fibra monomodo, racks, patch panels, conectores, patch cords, equipamentos ativos de rede, pontos de acesso Wi-Fi corporativo, firewall, projetores multimídia e todos os serviços técnicos necessários à instalação, configuração, certificação, validação e homologação da solução.

Grupo 01 - REDE E INFRAESTRUTURA TI			
Item	Especificação	Qtde	Unid. Medida
1	Conector RJ-45 Fêmea CAT.6	400	Unid.
2	Ponto de Acesso Interno AP WiFi	30	Unid.
3	Patch Cord 2,5m CAT.6	200	Unid.
4	Patch Cord 1,5m CAT.6	200	Unid.
5	Switch 48 portas POE	6	Unid.
6	Switch 24 portas POE	5	Unid.
7	Patch Panel 24 portas CAT.6	4	Unid.
8	Patch Panel 48 portas CAT.6	6	Unid.
9	Painel acabamento 19"x1U	7	Unid.
10	Organizador de cabos	14	Unid.

11	Bandeja fixa	14	Unid.
12	Conector RJ45 macho CAT.6	500	Unid.
13	Cabo de Rede CAT.6	7500	Metro
14	Firewall	1	Unid.
15	Régua alimentação rack	10	Unid.
16	Etiquetas para cabos	600	Unid.
17	Projetor	8	Unid.
18	Suporte projetor	8	Unid.
19	Extender HDMI	8	Unid.
20	Rack piso 40U	1	Unid.
21	Rack parede 12U	8	Unid.
22	Lançamento cabo óptico	300	Metro
23	DIO fibra óptica	1	Serviço
24	Emenda por fusão	6	Serviço
25	Infraestrutura de rede	1	Serviço
26	Instalação/Validação/Homologação	1	Serviço

Justificativa do dimensionamento do Grupo 01

Os quantitativos foram dimensionados a partir do levantamento técnico dos ambientes administrativos, acadêmicos, laboratórios, salas de aula, setores de apoio, áreas técnicas e demais dependências previstas para o funcionamento do campus. O número de pontos de rede considera tanto as necessidades atuais de conectividade quanto a reserva técnica para futuras ampliações, assegurando flexibilidade operacional e redução de intervenções na infraestrutura.

Os equipamentos ativos foram especificados para suportar a quantidade estimada de usuários, dispositivos de rede e equipamentos IP integrados à solução, garantindo capacidade de processamento, disponibilidade dos serviços, alimentação PoE para dispositivos compatíveis e gerenciamento centralizado da infraestrutura. O backbone óptico em fibra monomodo foi previsto para assegurar comunicação de alta capacidade entre os racks

e setores estratégicos da unidade, proporcionando elevada largura de banda, baixa atenuação, imunidade a interferências eletromagnéticas e possibilidade de expansão tecnológica.

Os projetores multimídia foram dimensionados conforme a quantidade de ambientes acadêmicos destinados às atividades de ensino, apresentações e treinamentos, contribuindo para a adequada estruturação dos espaços pedagógicos desde o início das atividades do campus.

Os serviços técnicos especializados compreendem todas as etapas necessárias à implantação da infraestrutura, incluindo instalação física, organização dos racks, certificação do cabeamento, configuração lógica dos equipamentos, integração entre os sistemas, testes operacionais, validação funcional e apoio ao processo de recebimento definitivo, garantindo a entrega da solução plenamente operacional.

Grupo 02 – Rede CFTV

O Grupo 02 contempla os equipamentos, materiais e serviços necessários à implantação do sistema de videomonitoramento IP do Campus Diadema, abrangendo câmeras internas e externas, gravador de vídeo em rede (NVR), armazenamento dedicado, switches PoE, racks, infraestrutura de cabeamento, postes metálicos, suportes, TV para monitoramento, grades de proteção, concertina e serviços de instalação, configuração, integração e testes do sistema.

GRUPO 02 - REDE CFTV			
Item	Especificação	Qtde	Unid. Medida
27	Gravador NVR 32 canais	1	Unid.
28	Disco Rígido HD 10TB	1	Unid.
29	Câmera IP Bullet para videomonitoramento	14	Unid.
30	Câmera IP Dome para videomonitoramento	18	Unid.
31	Suporte câmera	10	Unid.
32	Switch PoE 16P	2	Unid.
33	Mini Rack	2	Unid.
34	Patch Panel 16P	2	Unid.
35	Caixa proteção	16	Unid.
36	Bandeja fixa	2	Unid.
37	Concertina	200	Metro

38	Painel acabamento	2	Unid.
39	Organizador de cabos	2	Unid.
40	Distribuidor energia	2	Unid.
41	Cabo de rede Cat 6e	2100	Metro
42	Poste CFTV	4	Unid.
43	Smart TV 50	1	Unid.
44	Suporte TV	1	Unid.
45	Grade proteção	22	Unid.
46	Infraestrutura CFTV	1	Serviço
47	Instalação CFTV	32	Serviço

Justificativa do dimensionamento do Grupo 02

O sistema de videomonitoramento foi dimensionado considerando o levantamento dos acessos principais, áreas de circulação, estacionamentos, perímetro externo, ambientes internos, corredores, entradas de edifícios e demais pontos estratégicos definidos pela Administração, de forma a proporcionar cobertura adequada das áreas de interesse para segurança institucional.

A quantidade de câmeras contempla diferentes tipos de ambientes, empregando modelos apropriados para uso interno e externo, permitindo monitoramento contínuo e maior eficiência na identificação de ocorrências. A capacidade de armazenamento foi definida para suportar a gravação ininterrupta das imagens, assegurando disponibilidade para consultas posteriores, em conformidade com as necessidades operacionais da instituição.

Os elementos complementares, como postes, suportes, mini racks, infraestrutura de rede, grades de proteção, caixas de proteção e dispositivos de reforço perimetral, foram previstos para garantir a correta instalação dos equipamentos, proteção física dos ativos e durabilidade da solução. Os serviços especializados abrangem a instalação, configuração, integração, testes operacionais e validação do sistema de CFTV, assegurando seu pleno funcionamento e integração com a infraestrutura de rede do campus.

Grupo 03 – Controle de Acesso

O Grupo 03 contempla os equipamentos, materiais e serviços destinados à implantação do sistema eletrônico de controle de acesso do Campus Diadema, compreendendo catracas com reconhecimento facial, catraca acessível (PCD), cancelas automáticas, controladores faciais, kits de fechaduras eletromagnéticas, portão auxiliar, fechamento físico complementar, software de gerenciamento, infraestrutura de instalação e serviços técnicos de implantação, configuração, integração, testes e validação

GRUPO 03 - CONTROLE DE ACESSO

Item	Especificação	Qtde	Unid. Medida
48	Catraca Facial	2	Unid.
49	Catraca PNE	1	Unid.
50	Cancela Automática	2	Unid.
51	Controlador de Acesso com Reconhecimento Facial	10	Unid.
52	Kit Fecho	10	Unid.
53	Portão auxiliar	1	Unid.
54	Fechamento inox	2	Metro
55	Software gerenciamento	1	Unid.
56	Automatização portão	2	Serviço
57	Instalação e validação	23	Serviço
58	Infraestrutura acesso	1	Serviço

Justificativa do dimensionamento do Grupo 03

Os quantitativos foram definidos com base na análise dos acessos de pedestres e veículos previstos para o campus, considerando o fluxo estimado de estudantes, servidores, colaboradores, visitantes e prestadores de serviço. A solução foi projetada para garantir controle automatizado dos acessos, rastreabilidade dos eventos, aumento da segurança patrimonial e adequada gestão da circulação de pessoas nas dependências institucionais.

A previsão de catracas com reconhecimento facial, incluindo equipamento acessível para pessoas com deficiência ou mobilidade reduzida, atende aos princípios de acessibilidade, segurança e controle institucional. Os controladores faciais e kits de fechaduras eletromagnéticas foram dimensionados para proteger ambientes administrativos, laboratórios, salas técnicas, CPD e demais áreas de acesso restrito, permitindo gerenciamento centralizado e registro de todas as movimentações.

As cancelas automáticas, o portão auxiliar e os elementos de fechamento físico complementam o controle dos acessos veiculares e perimetrais, enquanto o software de gerenciamento possibilita administração unificada dos dispositivos, emissão de relatórios, cadastramento de usuários e integração com os demais sistemas de segurança eletrônica do campus. Os serviços técnicos previstos abrangem toda a implantação da solução,

desde a infraestrutura física até a configuração, integração, testes e validação final, garantindo pleno funcionamento e compatibilidade com os demais sistemas institucionais.

Escopo complementar de serviços e entregas técnicas

Além do fornecimento dos materiais e equipamentos mencionados, a Contratada deverá fornecer e executar os serviços e produtos técnicos complementares necessários à implantação integral dos sistemas de rede lógica, CFTV, controle de acesso e apoio tecnológico do Campus Diadema, conforme descrito a seguir.

a) Planejamento e projeto técnico

A contratada deverá realizar levantamento técnico detalhado das áreas de intervenção, validando os pontos de rede, rotas de cabeamento, localização de racks, posicionamento de câmeras, catracas, controladores faciais, cancelas, projetores, pontos de energia, barreiras físicas e demais componentes da solução.

Deverá ser apresentado projeto executivo contendo, no mínimo:

- topologia física e lógica da rede;
- localização dos pontos de telecomunicações;
- rotas de eletrocalhas, eletrodutos, canaletas e caixas de passagem;
- localização dos racks e equipamentos ativos;
- backbone óptico e identificação dos enlaces;
- posicionamento das câmeras e respectivos campos de cobertura;
- localização das catracas, cancelas, controladores faciais e dispositivos de abertura;
- identificação dos ambientes atendidos;
- especificação dos materiais e equipamentos a serem instalados;
- plano de testes, validação e homologação.

b) Instalação de barreiras físicas e controle de acesso

A contratada deverá executar a instalação de catracas eletrônicas, catraca acessível, cancelas automáticas, controladores faciais, fechaduras eletromagnéticas, botoeiras, fontes, acionadores de emergência, portões auxiliares, fechamento tubular e demais dispositivos de controle de acesso.

A instalação deverá observar as condições de acessibilidade, fluxo de usuários, segurança de evacuação, integração com o software de gerenciamento e compatibilidade com o sistema de CFTV.

Deverão ser realizados testes de abertura, bloqueio, autenticação, registro de eventos, funcionamento em contingência, comunicação TCP/IP, integração com o sistema de gerenciamento e emissão de relatórios.

c) Infraestrutura física, cabeamento e fibra óptica

A contratada deverá executar a infraestrutura física necessária à implantação da rede lógica, CFTV e controle de acesso, incluindo eletrocalhas, conduítes, canaletas, caixas de passagem, suportes, fixações e demais componentes de acomodação e proteção dos cabos.

Deverá ser executado cabeamento estruturado categoria 6, em conformidade com as normas técnicas aplicáveis, com identificação dos cabos, pontos, patch panels e racks.

O backbone óptico deverá ser implantado com cabo óptico monomodo, DIO, fusões, organização das fibras e testes de certificação. Os enlaces deverão ser entregues com relatórios técnicos de continuidade e atenuação.

d) Instalação de equipamentos ativos e acessórios

A contratada deverá instalar, organizar e configurar switches, access points, firewall, racks, patch panels, organizadores, régua de energia, bandejas, câmeras, NVR, TV de monitoramento, projetores, suportes, extensores HDMI e demais acessórios previstos na solução.

A configuração deverá observar as diretrizes fornecidas pela Administração, especialmente quanto à segmentação lógica da rede, identificação dos equipamentos, conectividade, parâmetros de segurança, VLANs, SSIDs, endereçamento, integração dos sistemas e testes de operação.

e) Testes, certificações e homologação

A contratada deverá realizar todos os testes necessários à validação da solução implantada, incluindo:

- testes de continuidade e certificação dos pontos de rede;
- testes de atenuação e continuidade dos enlaces ópticos;
- testes de conectividade dos switches, access points e firewall;
- testes de cobertura e operação da rede sem fio;
- testes de visualização, gravação e recuperação de imagens do CFTV;
- testes de autenticação facial e controle de acesso;
- testes de abertura e bloqueio de catracas, portas e cancelas;
- testes de emissão de relatórios e rastreabilidade de eventos;
- testes de integração entre CFTV, controle de acesso e rede lógica;
- apoio à homologação pela fiscalização do contrato.

f) Entregas técnicas

Ao final da execução, a contratada deverá entregar, no mínimo:

- projeto executivo atualizado;
- relatório de certificação dos pontos de rede;
- relatório de testes dos enlaces ópticos;
- relatório de instalação e configuração dos equipamentos ativos;
- relatório de instalação e validação do sistema de CFTV;
- relatório de instalação e validação do controle de acesso;
- relação dos equipamentos instalados, com número de série quando aplicável;
- diagramas físicos e lógicos atualizados;
- manuais técnicos e operacionais;
- orientações básicas de operação aos servidores indicados;
- apoio à Comissão de Recebimento na realização dos testes de aceitação.

Descrição técnica complementar

A descrição complementar tem por finalidade apresentar informações técnicas adicionais sobre determinados itens que, em razão de sua complexidade funcional ou relevância tecnológica, demandam detalhamento específico para melhor compreensão de suas características de desempenho, operação e integração.

As especificações detalhadas dos materiais, equipamentos, sistemas e serviços deverão constar em apêndice próprio ou no Termo de Referência, contendo descrição resumida, descrição completa, requisitos mínimos de desempenho, normas aplicáveis, condições de instalação, garantia, suporte e critérios de aceitação.

Síntese

Os quantitativos e serviços acima refletem o dimensionamento necessário à implantação completa, integrada e funcional da infraestrutura tecnológica, pedagógica e de segurança eletrônica do **IFSP – Campus Diadema**.

As estimativas consideram a implantação de rede lógica estruturada, backbone óptico, equipamentos ativos, cobertura Wi-Fi, firewall, sistema de CFTV, controle de acesso de pedestres e veículos, controle de ambientes restritos, proteção perimetral, apoio audiovisual às atividades acadêmicas e serviços técnicos especializados.

A solução proposta assegura conectividade institucional, segurança física e lógica, rastreabilidade de eventos, interoperabilidade entre sistemas, padronização tecnológica, escalabilidade, sustentabilidade operacional e compatibilidade com as diretrizes corporativas de Tecnologia da Informação e Comunicação adotadas pelo IFSP.

Metodologia para Estimativa dos Quantitativos

A estimativa dos quantitativos da presente contratação foi elaborada a partir de levantamento técnico realizado pela equipe de planejamento, considerando as necessidades do IFSP – Campus Diadema e as características da solução de Tecnologia da Informação e Comunicação (TIC) necessária ao atendimento das atividades administrativas, acadêmicas e de apoio.

O dimensionamento da solução considerou a distribuição física dos ambientes da unidade, a quantidade de salas de aula, laboratórios, setores administrativos, biblioteca, auditório, áreas comuns e demais espaços que demandam infraestrutura tecnológica, bem como a arquitetura de rede adotada institucionalmente pelo IFSP.

Para definição dos quantitativos foram observados, entre outros, os seguintes critérios técnicos:

- quantidade de ambientes a serem atendidos pela infraestrutura de rede lógica;
- necessidade de interligação entre os pontos de telecomunicações por meio de backbone óptico e cabeamento estruturado;
- dimensionamento dos equipamentos ativos de rede em função do número de pontos de rede, equipamentos PoE, dispositivos conectados e possibilidade de expansão futura;
- cobertura adequada da rede sem fio corporativa, considerando área de abrangência e capacidade estimada de usuários;
- posicionamento dos equipamentos do sistema de videomonitoramento (CFTV) e do controle de acesso, conforme as necessidades de segurança patrimonial e controle de circulação de pessoas;
- dimensionamento dos recursos audiovisuais destinados aos ambientes de ensino; e
- serviços especializados necessários para instalação, configuração, integração, certificação, testes, treinamento e homologação da solução.

Os quantitativos dos materiais auxiliares e componentes complementares foram definidos de forma proporcional aos equipamentos principais e à infraestrutura projetada, observando as normas técnicas aplicáveis, as recomendações dos fabricantes e as boas práticas de implantação de soluções de TIC.

A definição dos quantitativos teve como objetivo assegurar a implantação integral da solução, contemplando todos os componentes necessários ao seu pleno funcionamento, bem como margem técnica compatível para ajustes decorrentes da execução e para futuras expansões da infraestrutura tecnológica da unidade.

Os quantitativos constantes deste Estudo Técnico Preliminar serviram de base para a elaboração do Termo de Referência e estão fundamentados nos levantamentos técnicos realizados pela equipe de planejamento da contratação, nas características físicas e funcionais da unidade e nas especificações técnicas da solução pretendida.

8. Levantamento de soluções

Para a definição da solução mais adequada às necessidades institucionais do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – IFSP, Campus Diadema, no contexto da implantação e estruturação da unidade para início de suas atividades acadêmicas e administrativas, foram consideradas diferentes alternativas tecnológicas e operacionais disponíveis no mercado.

A análise contemplou aspectos relacionados à viabilidade técnica, operacional e econômica das soluções, bem como sua capacidade de atendimento às necessidades identificadas pela Administração, considerando requisitos de conectividade institucional, segurança patrimonial, controle de acesso, disponibilidade dos serviços, interoperabilidade entre sistemas, escalabilidade, sustentabilidade tecnológica e aderência aos padrões corporativos de Tecnologia da Informação e Comunicação adotados pelo IFSP.

As soluções avaliadas encontram-se descritas a seguir:

Solução	Descrição Técnica Resumida	Composição / Elementos Principais	Objetivo Atendido
Solução 1 – Implantação integrada da infraestrutura	Implantação completa e integrada da infraestrutura de TIC do Campus Diadema, contemplando rede lógica estruturada, backbone óptico, equipamentos ativos, Wi-Fi corporativo, segurança perimetral, CFTV IP, controle de	Cabeamento estruturado Cat.6; infraestrutura física; backbone óptico em fibra monomodo; DIO; fusões ópticas; switches gerenciáveis; firewall corporativo; access points Wi-Fi; racks; patch panels; câmeras IP; NVR; armazenamento 24x7; catracas com	Atender integralmente às necessidades de conectividade, segurança física e lógica, controle de acesso, suporte às

tecnológica e de segurança eletrônica	acesso por reconhecimento facial, controle de acesso veicular e serviços especializados de instalação, configuração, certificação e homologação.	reconhecimento facial; controladores faciais; cancelas automáticas; softwares integrados; projetores multimídia; serviços técnicos especializados.	atividades acadêmicas e administrativas e implantação estruturada do Campus Diadema.
Solução 2 – Sistema convencional com CFTV analógico e controle de acesso simplificado	Implantação de sistema de vigilância baseado em tecnologia analógica, associado a mecanismos básicos de controle de acesso sem integração com sistemas institucionais e sem infraestrutura estruturada de TIC.	Câmeras analógicas; DVR; cabeamento coaxial; catracas com cartão RFID; infraestrutura elétrica simplificada; rede local sem gerenciamento; ausência de backbone óptico; ausência de Wi-Fi corporativo; inexistência de integração entre sistemas.	Proporcionar recursos básicos de monitoramento e controle de acesso, sem integração tecnológica, escalabilidade ou aderência aos padrões institucionais.
Solução 3 – Prestação de serviços em regime de terceirização integral (outsourcing)	Contratação de empresa especializada para fornecimento dos equipamentos, infraestrutura, softwares, operação e manutenção dos sistemas, mediante locação ou comodato.	Equipamentos pertencentes à contratada; software proprietário; infraestrutura fornecida pela contratada; equipe externa responsável pela operação e manutenção contínua dos sistemas.	Transferir integralmente à contratada a responsabilidade pela disponibilização e operação dos serviços de monitoramento e controle de acesso.
Solução 4 – Implantação parcial e gradual da infraestrutura tecnológica	Implantação fragmentada da solução, executada em etapas sucessivas, condicionada à disponibilidade orçamentária, postergando a integração plena dos sistemas e a conclusão da infraestrutura.	Quantidade reduzida de câmeras; implantação parcial do cabeamento estruturado; backbone óptico incompleto; switches sem integração plena; número reduzido de access points; implantação parcial das catracas e controladores faciais; ausência inicial de integração entre os subsistemas.	Atender parcialmente às necessidades imediatas do campus, distribuindo os investimentos ao longo do tempo.

Análise comparativa das soluções

A **Solução 1** apresenta elevado grau de aderência às necessidades institucionais do Campus Diadema, permitindo a implantação completa da infraestrutura tecnológica necessária ao funcionamento da unidade desde o início de suas atividades. A solução contempla integração entre os sistemas de rede, videomonitoramento e controle de acesso, favorecendo a interoperabilidade, a padronização tecnológica, a racionalização dos custos operacionais e a mitigação de riscos relacionados à segurança patrimonial e à indisponibilidade dos serviços.

A **Solução 2**, embora apresente menor investimento inicial, utiliza tecnologias consideradas obsoletas ou insuficientes para o contexto institucional do IFSP, não oferecendo mecanismos adequados de integração, escalabilidade, gerenciamento centralizado ou aderência aos padrões corporativos de TIC adotados pela instituição. Além disso, a utilização de infraestrutura analógica implica limitações técnicas significativas, especialmente quanto à qualidade das imagens, expansão futura e interoperabilidade com outros sistemas.

A **Solução 3** possibilita a transferência da responsabilidade operacional à contratada, porém implica dependência tecnológica contínua, custos recorrentes elevados e menor autonomia administrativa sobre a gestão dos sistemas implantados. Adicionalmente, a utilização de equipamentos pertencentes à contratada pode dificultar futuras expansões, substituições tecnológicas ou integração com soluções corporativas adotadas pelo IFSP.

A **Solução 4** apresenta a vantagem de diluição do investimento ao longo do tempo; entretanto, a implantação fragmentada compromete a integração entre os subsistemas, gera retrabalhos, eleva os custos globais de implantação e posterga a disponibilização integral dos recursos tecnológicos necessários ao adequado funcionamento do campus. A execução em etapas independentes também aumenta os riscos de incompatibilidade tecnológica, sobreposição de responsabilidades e dificuldades na gestão das garantias.

Solução escolhida

Após análise das alternativas disponíveis, verificou-se que a **Solução 1 – Implantação integrada da infraestrutura tecnológica e de segurança eletrônica** é a que melhor atende às necessidades do IFSP – Campus Diadema, por apresentar maior aderência aos requisitos funcionais, técnicos, operacionais e institucionais identificados durante a fase de planejamento da contratação.

A adoção dessa solução permitirá a disponibilização de ambiente tecnológico seguro, padronizado, escalável e alinhado às diretrizes corporativas de TIC do IFSP, assegurando condições adequadas para o desenvolvimento das

atividades acadêmicas e administrativas da unidade, bem como promovendo maior eficiência na gestão dos recursos públicos investidos.

Dessa forma, conclui-se que a implantação integrada da infraestrutura de rede lógica, backbone óptico, equipamentos ativos, conectividade sem fio, sistema de CFTV IP, controle de acesso e serviços técnicos especializados constitui a alternativa mais vantajosa para a Administração, sob os aspectos técnico, operacional e econômico.

9. Análise comparativa de soluções

Para a definição da solução mais adequada às necessidades institucionais do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – IFSP, Campus Diadema, no contexto da implantação e estruturação da unidade para início de suas atividades acadêmicas e administrativas, foram consideradas diferentes alternativas tecnológicas e operacionais disponíveis no mercado.

As alternativas foram avaliadas sob os critérios de aderência às necessidades institucionais, eficiência técnica, viabilidade econômica, facilidade de manutenção, nível de integração entre sistemas, governança tecnológica, segurança da informação, escalabilidade e sustentabilidade operacional de longo prazo.

As soluções analisadas encontram-se descritas no quadro comparativo a seguir:

Alternativa	Descrição Resumida	Vantagens	Desvantagens / Limitações	Conclusão
Solução 1 – Sistema Integrado de Infraestrutura Tecnológica e Segurança Eletrônica	Implantação completa da infraestrutura tecnológica do Campus Diadema, contemplando cabeamento estruturado categoria 6, backbone óptico em fibra monomodo, infraestrutura física, equipamentos ativos de rede, Wi-Fi corporativo, firewall, sistema de CFTV IP, controle de acesso por reconhecimento facial, controle de acesso veicular, recursos audiovisuais e serviços especializados de instalação, configuração, testes e homologação.	Integração plena entre os subsistemas; gestão centralizada; maior nível de segurança física e lógica; elevada escalabilidade; padronização tecnológica; melhor desempenho da rede; redução de retrabalhos; facilidade de manutenção; maior vida útil da infraestrutura; compatibilidade com os padrões corporativos do IFSP.	Maior investimento inicial em razão da abrangência da solução e da aquisição de equipamentos com características corporativas.	Viável e recomendada. Atende integralmente às necessidades institucionais do Campus Diadema
Solução 2 – Sistema convencional com equipamentos analógicos e controle de acesso simplificado	Implantação de sistema baseado em câmeras analógicas com DVR e controle de acesso por cartão RFID ou registros manuais, sem integração com infraestrutura lógica estruturada e sem gerenciamento centralizado.	Menor investimento inicial; simplicidade de instalação em ambientes reduzidos.	Baixa qualidade de imagem; ausência de integração entre sistemas; limitações de expansão; maior vulnerabilidade operacional; inexistência de gerenciamento centralizado; custos elevados de manutenção corretiva e substituição futura; incompatibilidade com os padrões institucionais do IFSP.	Inviável tecnicamente. Não atende aos requisitos institucionais de integração, segurança e escalabilidade.
Solução 3 – Terceirização integral dos sistemas de monitoramento e controle	Contratação de empresa especializada para fornecimento da infraestrutura, equipamentos, softwares, operação e manutenção, mediante regime de locação ou comodato.	Redução do investimento inicial; transferência da responsabilidade operacional à contratada; atualização tecnológica potencialmente mais frequente.	Custos recorrentes elevados; dependência tecnológica e operacional da contratada; ausência de domínio institucional sobre dados e infraestrutura; riscos associados à descontinuidade contratual; menor autonomia administrativa.	Inadequada sob os aspectos econômico e operacional. Não garante autonomia institucional nem preservação do investimento público.
Solução 4 – Implantação parcial e gradual da	Implantação fragmentada da infraestrutura de rede, CFTV e controle de acesso,	Possibilidade de distribuição do investimento ao longo do tempo.	Posterga a disponibilização integral dos serviços; gera retrabalhos; aumenta os custos globais da implantação; dificulta a integração entre subsistemas; eleva o risco de	Desaconselhada. Compromete a eficiência da implantação e aumenta os

Conclusão da análise comparativa

Após a avaliação das alternativas disponíveis, concluiu-se que a **Solução 1 – Sistema Integrado de Infraestrutura Tecnológica e Segurança Eletrônica** representa a opção mais vantajosa para a Administração Pública, tanto sob o ponto de vista técnico quanto econômico.

Embora demande maior investimento inicial, a solução integrada proporciona redução dos custos operacionais ao longo do ciclo de vida da infraestrutura, menor incidência de retrabalhos, simplificação das atividades de manutenção, maior interoperabilidade entre os sistemas e ampliação da capacidade de expansão futura do campus.

Além disso, a solução permite que o IFSP – Campus Diadema inicie suas atividades acadêmicas e administrativas dispondo de infraestrutura tecnológica compatível com os padrões institucionais adotados pela instituição, garantindo níveis adequados de conectividade, segurança patrimonial, rastreabilidade de eventos, controle de fluxo de pessoas e proteção das informações institucionais.

A adoção da solução integrada assegura, ainda:

- cobertura adequada das áreas estratégicas para fins de monitoramento e controle de acesso;
- integração entre infraestrutura lógica, videomonitoramento e sistemas de autenticação;
- disponibilidade de conectividade estruturada para ambientes acadêmicos e administrativos;
- suporte à expansão futura da unidade sem necessidade de reestruturação integral da infraestrutura implantada;
- padronização tecnológica e compatibilidade com a arquitetura corporativa de TIC do IFSP;
- redução do custo total de propriedade da solução ao longo do tempo, decorrente da diminuição de custos de manutenção corretiva, substituição prematura de equipamentos e retrabalhos de implantação;
- observância às normas técnicas aplicáveis, incluindo ABNT NBR 14565, ISO/IEC 11801, ANSI/TIA-568, NR-10 e demais regulamentos pertinentes.

Dessa forma, conclui-se que a **Solução 1** demonstra superioridade técnica, econômica e operacional em relação às demais alternativas avaliadas, atendendo plenamente às necessidades identificadas para o IFSP – Campus Diadema e alinhando-se aos princípios do planejamento, da eficiência, da economicidade e da obtenção da proposta mais vantajosa previstos na **Lei nº 14.133/2021**.

A escolha da solução integrada mostra-se, portanto, adequada e compatível com os objetivos institucionais relacionados à implantação estruturada do campus, garantindo condições apropriadas para o desenvolvimento das atividades de ensino, pesquisa, extensão e gestão administrativa.

10. Registro de soluções consideradas inviáveis

Durante o levantamento das alternativas disponíveis no mercado, verificou-se que as soluções classificadas como Solução 2 – Sistema Convencional com Equipamentos Analógicos e Controle de Acesso Simplificado, Solução 3 – Terceirização Integral dos Sistemas de Monitoramento e Controle e Solução 4 – Implantação Parcial e Gradual da Infraestrutura Tecnológica apresentaram limitações técnicas, operacionais e econômicas incompatíveis com as necessidades institucionais do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – IFSP, Campus Diadema.

Embora tecnicamente exequíveis sob determinadas circunstâncias, tais alternativas não atendem aos requisitos mínimos de desempenho, integração, escalabilidade, segurança e sustentabilidade operacional necessários ao adequado funcionamento da infraestrutura tecnológica e dos sistemas de segurança eletrônica do campus.

A seguir, apresenta-se a análise individual das limitações identificadas para cada alternativa avaliada.

Solução 2 – Sistema Convencional com Equipamentos Analógicos e Controle de Acesso Simplificado

Essa alternativa consiste na utilização de equipamentos analógicos para videomonitoramento, associados a sistemas básicos de controle de acesso, sem integração com a infraestrutura lógica institucional e sem gerenciamento centralizado.

Em geral, contempla a utilização de câmeras analógicas conectadas a gravadores do tipo DVR, cabeamento coaxial e mecanismos simplificados de autenticação, tais como cartões RFID ou registros manuais de entrada e saída.

Principais limitações identificadas:

- baixa qualidade das imagens capturadas, dificultando a identificação precisa de indivíduos e ocorrências em áreas estratégicas do campus;
- limitações relacionadas ao armazenamento e à recuperação de gravações, especialmente em cenários que demandem maior período de retenção das imagens;
- inexistência de integração entre os sistemas de videomonitoramento e os mecanismos de controle de acesso, inviabilizando a correlação automática entre eventos de acesso e registros de vídeo;
- utilização de infraestrutura tecnológica incompatível com os padrões atuais de redes IP corporativas adotados pelo IFSP;
- reduzida capacidade de expansão futura, exigindo substituição integral dos componentes em eventual ampliação da solução;
- dificuldade de manutenção decorrente da progressiva descontinuidade de equipamentos analógicos no mercado;
- ausência de mecanismos modernos de autenticação, tais como reconhecimento facial e integração com bases de dados institucionais;
- impossibilidade de integração eficiente com a infraestrutura lógica estruturada, com os equipamentos ativos de rede e com os sistemas corporativos da instituição.

Conclusão

A solução foi considerada tecnicamente inviável, por não atender aos requisitos mínimos de integração, segurança, desempenho e escalabilidade exigidos para a implantação do IFSP – Campus Diadema.

Além de apresentar limitações operacionais significativas, a adoção dessa alternativa implicaria rápida obsolescência tecnológica e elevação dos custos futuros decorrentes de substituições e adequações da infraestrutura implantada.

Solução 3 – Prestação de Serviços em Regime de Terceirização Integral

Essa alternativa consiste na contratação de empresa especializada responsável pelo fornecimento dos equipamentos, infraestrutura, softwares, manutenção e operação dos sistemas, em regime de locação, comodato ou prestação continuada de serviços.

Principais limitações identificadas:

- perda de autonomia institucional sobre a infraestrutura crítica de segurança e conectividade implantada no campus;
- dependência tecnológica e operacional da contratada para manutenção, expansão, atualização e continuidade dos serviços;
- custos recorrentes elevados ao longo do tempo, resultando em custo total de propriedade superior ao investimento necessário para implantação de solução própria;
- risco de descontinuidade operacional em decorrência do término do contrato, atrasos em procedimentos licitatórios subsequentes ou eventuais inadimplementos contratuais;
- limitação da capacidade institucional de customização e integração da solução com sistemas próprios do IFSP;
- maior complexidade na gestão contratual e fiscalização dos níveis de serviço prestados;
- riscos associados à proteção de dados pessoais e institucionais, especialmente considerando o tratamento de informações biométricas, registros de acesso e imagens capturadas pelos sistemas de videomonitoramento;
- ausência de incorporação definitiva dos ativos tecnológicos ao patrimônio público.

Conclusão

A solução foi considerada economicamente e operacionalmente inadequada, por comprometer a autonomia administrativa, gerar dependência excessiva de terceiros e apresentar custo global potencialmente superior ao da implantação definitiva da infraestrutura.

Adicionalmente, não se mostra alinhada à estratégia institucional de consolidação de infraestrutura tecnológica própria para suporte permanente às atividades acadêmicas e administrativas do Campus Diadema.

Solução 4 – Implantação Parcial e Gradual da Infraestrutura Tecnológica

Essa alternativa pressupõe a implantação fragmentada dos sistemas de rede, videomonitoramento e controle de acesso, condicionando sua conclusão à disponibilidade orçamentária futura.

Na prática, parte da infraestrutura seria instalada inicialmente, permanecendo outros componentes para execução em etapas posteriores.

Principais limitações identificadas:

- comprometimento da integração entre os subsistemas de rede, controle de acesso e videomonitoramento;
- necessidade de retrabalho decorrente da posterior ampliação ou readequação das estruturas inicialmente implantadas;
- aumento dos custos globais da contratação em função da repetição de mobilizações, instalações e configurações;
- risco de incompatibilidade técnica entre equipamentos adquiridos em momentos distintos;
- atraso na disponibilização integral dos recursos tecnológicos necessários ao funcionamento do campus;
- redução da efetividade dos mecanismos de segurança física e lógica durante o período de implantação incompleta;
- ampliação da complexidade de gestão contratual e de fiscalização das diversas etapas de execução;
- prejuízo à padronização tecnológica e à uniformidade da infraestrutura institucional.

Conclusão

A solução foi considerada não recomendada, por gerar ineficiência administrativa, custos adicionais futuros e riscos operacionais decorrentes da ausência de integração plena entre os componentes da solução.

Considerando que o Campus Diadema será implantado para início de suas atividades acadêmicas e administrativas em ambiente plenamente funcional, a adoção de infraestrutura parcial não atende adequadamente às necessidades institucionais identificadas.

Síntese conclusiva

Diante das análises realizadas, concluiu-se que as Soluções 2, 3 e 4 não apresentam condições técnicas, operacionais e econômicas compatíveis com as necessidades do IFSP – Campus Diadema

As limitações identificadas comprometem aspectos essenciais relacionados à conectividade institucional, segurança patrimonial, controle de acesso, interoperabilidade entre sistemas, governança tecnológica, proteção de dados e sustentabilidade operacional da infraestrutura.

Restou evidenciado que apenas a Solução 1 – Implantação Integrada da Infraestrutura Tecnológica e de Segurança Eletrônica é capaz de assegurar o nível de funcionalidade, confiabilidade, disponibilidade e capacidade de expansão exigidos pela Administração Pública.

A solução integrada possibilita a implantação definitiva da infraestrutura necessária ao funcionamento do campus, contemplando rede lógica estruturada, backbone óptico, conectividade sem fio, segurança perimetral, videomonitoramento IP, controle de acesso, recursos tecnológicos de apoio às atividades acadêmicas e serviços especializados de implantação, configuração e homologação.

Dessa forma, conclui-se que a adoção da Solução 1 representa a alternativa mais vantajosa para a Administração, por demonstrar superioridade técnica, econômica e operacional, atendendo aos princípios do planejamento, da

eficiência, da economicidade e da busca da solução mais adequada ao interesse público, previstos na Lei nº 14.133/2021.

11. Análise comparativa de custos (TCO)

A análise comparativa de custos teve por finalidade avaliar os impactos financeiros decorrentes das alternativas tecnológicas consideradas durante o levantamento técnico, visando identificar a solução que apresenta a melhor relação custo-benefício para o Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – IFSP, Campus Diadema, no contexto da implantação de sua infraestrutura tecnológica e de segurança eletrônica.

A avaliação foi realizada considerando não apenas os custos iniciais de implantação, mas também os custos associados à operação, manutenção preventiva e corretiva, atualização tecnológica, substituição de componentes, possibilidade de expansão futura, necessidade de retrabalhos e sustentabilidade operacional ao longo do ciclo de vida da solução.

Nesse contexto, adotou-se como referência o conceito de Custo Total de Propriedade (Total Cost of Ownership – TCO), que considera o custo global da solução durante seu período estimado de utilização, permitindo análise mais aderente ao princípio da economicidade previsto na Lei nº 14.133/2021.

Com base nos levantamentos realizados, as alternativas analisadas apresentaram as seguintes características econômicas estimadas:

Solução	Descrição Resumida	Custo Inicial (Implantação)	Custo de Manutenção / Operação	Custo Total do Ciclo de Vida (5 anos)	Observações
Solução 1 – Sistema Integrado de Infraestrutura Tecnológica e Segurança Eletrônica (Escolhida)	Implantação completa da infraestrutura tecnológica do campus, incluindo rede lógica estruturada, backbone óptico, equipamentos ativos, Wi-Fi corporativo, firewall, CFTV IP, controle de acesso facial, controle de acesso veicular, recursos audiovisuais e serviços especializados de implantação e homologação.	Elevado	Baixo	Mais vantajoso	Permite gestão centralizada, reduz retrabalhos, gera patrimônio permanente para o IFSP e possibilita expansão futura com menor impacto financeiro. Exige substituições prematuras, apresenta baixa capacidade de expansão e demanda elevados custos de manutenção e adequação tecnológica. O custo acumulado tende a
Solução 2 – Sistema Convencional com Equipamentos Analógicos e Controle de Acesso Simplificado	Implantação baseada em equipamentos analógicos e mecanismos básicos de controle de acesso, sem integração plena entre os sistemas.	Baixo	Elevado	Desfavorável	

Solução 3 – Terceirização Integral dos Sistemas	Contratação de empresa especializada para fornecimento dos equipamentos, infraestrutura, software, manutenção e operação em regime de locação ou comodato.	Reduzido	Muito elevado	Desfavorável	superar o investimento em solução própria, não gera patrimônio público e aumenta a dependência tecnológica da contratada.
					Gera retrabalhos, amplia os custos de integração e eleva o custo global da solução em decorrência da fragmentação da implantação.
Solução 4 – Implantação Parcial e Gradual da Infraestrutura	Execução da infraestrutura em etapas sucessivas, condicionadas à disponibilidade orçamentária futura.	Moderado por etapa	Elevado	Desfavorável	

Avaliação econômica das alternativas

A Solução 1, embora demande maior investimento inicial, apresenta o melhor desempenho sob a perspectiva do custo total do ciclo de vida da infraestrutura.

A implantação integrada reduz significativamente a necessidade de intervenções futuras, evita retrabalhos decorrentes da incompatibilidade entre subsistemas e possibilita melhor aproveitamento da infraestrutura instalada, especialmente no que se refere ao cabeamento estruturado, backbone óptico, equipamentos ativos e sistemas de segurança eletrônica.

Além disso, a adoção de solução própria gera incorporação dos ativos ao patrimônio do IFSP, ampliando a autonomia institucional e reduzindo despesas recorrentes associadas à locação de equipamentos ou contratação continuada de serviços especializados.

Por outro lado, a Solução 2, embora apresente menor custo inicial, demanda substituições antecipadas, possui baixa capacidade de expansão e tende a elevar significativamente os custos de manutenção corretiva ao longo do tempo, tornando-se economicamente desvantajosa em médio prazo.

A Solução 3 transfere a responsabilidade operacional à contratada, porém implica pagamentos recorrentes durante toda a vigência contratual, não gerando patrimônio permanente para a Administração Pública. Em cenários de médio e longo prazo, o custo acumulado da terceirização tende a superar o investimento necessário para implantação de infraestrutura própria.

Já a Solução 4, baseada na implantação gradual dos sistemas, acarreta custos adicionais relacionados à mobilização repetida de equipes, adequações da infraestrutura previamente instalada, reconfiguração de equipamentos e integração entre tecnologias adquiridas em momentos distintos, comprometendo a economicidade da contratação.

Conclusão da análise comparativa de custos

A partir da avaliação realizada, conclui-se que a Solução 1 – Sistema Integrado de Infraestrutura Tecnológica e Segurança Eletrônica apresenta a melhor relação custo-benefício para o IFSP – Campus Diadema.

Embora represente maior investimento inicial, a solução integrada proporciona:

- menor custo total de propriedade ao longo do ciclo de vida da infraestrutura;
- redução dos custos de manutenção corretiva e preventiva;
- eliminação de retrabalhos decorrentes de implantações fragmentadas;

- maior vida útil dos componentes instalados;
- possibilidade de expansão futura sem necessidade de substituição integral da infraestrutura;
- geração de patrimônio permanente para o IFSP;
- maior autonomia administrativa e tecnológica;
- padronização dos recursos de TIC e segurança eletrônica;
- melhor aproveitamento dos recursos públicos investidos.

Dessa forma, verifica-se que a adoção da solução integrada atende aos princípios da economicidade, da eficiência, do planejamento, da sustentabilidade operacional e da busca pela proposta mais vantajosa para a Administração Pública, previstos na Lei nº 14.133/2021, demonstrando-se como a alternativa mais adequada sob os aspectos técnico, econômico e institucional para a implantação do IFSP – Campus Diadema.

12. Descrição da solução de TIC a ser contratada

A presente contratação destina-se a viabilizar a implantação da infraestrutura tecnológica e dos sistemas de segurança eletrônica necessários ao funcionamento do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – IFSP, Campus Diadema, assegurando conformidade com os padrões corporativos de Tecnologia da Informação e Comunicação adotados institucionalmente.

Conforme demonstrado nas análises técnicas, econômicas e comparativas realizadas neste Estudo Técnico Preliminar, a **Solução 1 – Implantação Integrada da Infraestrutura Tecnológica e de Segurança Eletrônica**, detalhada no Termo de Referência, foi identificada como a alternativa que melhor atende às necessidades institucionais do Campus Diadema, apresentando maior aderência aos requisitos técnicos estabelecidos, melhor relação custo-benefício ao longo do ciclo de vida da solução, maior nível de integração entre os subsistemas, facilidade de manutenção, padronização tecnológica e capacidade de expansão futura.

Dessa forma, a Solução 1 é indicada como a solução a ser contratada, por atender de maneira mais eficiente, segura, econômica e sustentável às demandas relacionadas à implantação da unidade e ao início de suas atividades acadêmicas e administrativas.

A solução de TIC a ser contratada consiste na implantação de solução integrada de infraestrutura tecnológica, compreendendo rede lógica estruturada, backbone óptico em fibra monomodo, equipamentos ativos de rede, conectividade sem fio, recursos de segurança perimetral, sistema de videomonitoramento IP, controle de acesso de pedestres e veículos, recursos tecnológicos de apoio às atividades acadêmicas e serviços técnicos especializados de implantação, configuração, integração, testes e homologação.

A contratação abrange o fornecimento de materiais, equipamentos, softwares, licenças e serviços técnicos especializados, garantindo a entrega de solução completa, funcional, interoperável e em conformidade com as normas técnicas aplicáveis.

A solução contempla infraestrutura física, lógica e de segurança eletrônica estruturada em arquitetura híbrida, combinando cabeamento metálico e backbone óptico, assegurando desempenho adequado, padronização institucional, interoperabilidade entre sistemas e sustentabilidade tecnológica de longo prazo.

Para fins de detalhamento técnico e melhor compreensão dos componentes que integram a solução a ser contratada, apresentam-se a seguir seus principais elementos estruturantes.

a) Infraestrutura de rede de dados

A solução deverá contemplar a implantação integral da infraestrutura de rede lógica do Campus Diadema, compreendendo:

1. Cabeamento estruturado metálico

- implantação de rede categoria 6 (Cat.6), em conformidade com as normas ABNT NBR 14565, ANSI/TIA-568 e ISO/IEC 11801;
- fornecimento e instalação de cabos, conectores, patch cords, patch panels, racks, organizadores e demais acessórios necessários;

- identificação padronizada de todos os pontos de telecomunicações;
- certificação integral dos pontos de rede, com emissão dos respectivos relatórios técnicos.

2. Backbone óptico em fibra monomodo

- fornecimento e lançamento de cabo óptico monomodo, inclusive em infraestrutura aérea quando aplicável;
- instalação de Distribuidores Internos Ópticos – DIO;
- execução de emendas por fusão;
- organização das fibras ópticas nos distribuidores;
- realização de testes de continuidade e atenuação;
- certificação dos enlaces ópticos por meio de OTDR ou equipamento equivalente;
- integração com equipamentos ativos por meio de interfaces SFP compatíveis.

O backbone óptico constituirá a espinha dorsal da infraestrutura de rede do campus, garantindo alta capacidade de transmissão, estabilidade dos enlaces e suporte à expansão futura da unidade.

b) Equipamentos ativos de rede

A solução deverá incluir equipamentos ativos compatíveis com os padrões tecnológicos adotados pelo IFSP, contemplando:

- switches gerenciáveis com suporte a VLANs, QoS e uplinks ópticos;
- pontos de acesso Wi-Fi corporativos;
- firewall corporativo com funcionalidades de inspeção profunda de pacotes, VPN, filtragem de conteúdo, prevenção de intrusões e demais mecanismos de segurança;
- racks e infraestrutura complementar de telecomunicações.

Os equipamentos ativos deverão operar de forma integrada ao backbone óptico e ao cabeamento estruturado, permitindo segmentação lógica da rede, priorização de tráfego e adequada gestão dos recursos tecnológicos do campus.

c) Sistema de CFTV IP

A solução deverá contemplar sistema de videomonitoramento baseado em tecnologia IP, compreendendo:

- câmeras IP Full HD ou superior, destinadas ao monitoramento de áreas internas e externas;
- gravador NVR compatível com o quantitativo previsto de câmeras;
- unidades de armazenamento específicas para operação contínua 24 horas por dia, 7 dias por semana;
- compatibilidade com protocolo ONVIF;
- acesso controlado às imagens e registros;
- integração com os sistemas de controle de acesso;
- segmentação do tráfego de vídeo na infraestrutura de rede.

O sistema deverá permitir monitoramento contínuo das áreas estratégicas do campus, contribuindo para a proteção do patrimônio público e para a segurança da comunidade acadêmica.

d) Sistema de controle de acesso

A solução deverá contemplar mecanismos automatizados de controle de fluxo de pessoas e veículos, incluindo:

- catracas com reconhecimento facial;
- catraca acessível para pessoas com deficiência ou mobilidade reduzida;
- controladores faciais para ambientes restritos;
- fechaduras eletromagnéticas e acessórios de acionamento;
- cancelas automáticas para controle de acesso veicular;
- software de gerenciamento centralizado, com interface web;
- cadastro e gerenciamento de usuários;
- registro e auditoria de eventos;
- definição de perfis e níveis hierárquicos de acesso;
- funcionalidades de segurança, incluindo anti-passback;

- integração com o sistema de CFTV e com a infraestrutura de rede.

e) Recursos tecnológicos de apoio às atividades acadêmicas

A solução deverá contemplar equipamentos destinados ao suporte das atividades de ensino e administrativas, incluindo:

- projetores multimídia;
- suportes para fixação;
- extensores HDMI e demais acessórios necessários à sua operação.

Esses recursos visam garantir condições adequadas para a realização das atividades acadêmicas, reuniões institucionais, treinamentos e demais ações desenvolvidas pela unidade.

f) Implantação, integração e entrega da solução

A execução deverá ocorrer de forma integrada, contemplando a implantação completa da infraestrutura física e lógica, dos equipamentos ativos, dos sistemas de videomonitoramento e dos mecanismos de controle de acesso.

A contratada deverá:

- elaborar e apresentar projeto executivo para aprovação da Administração;
- executar a instalação física da infraestrutura e dos equipamentos;
- realizar a configuração e integração dos sistemas;
- executar os testes de funcionamento previstos;
- realizar a certificação da rede metálica e dos enlaces ópticos;
- emitir os respectivos relatórios técnicos;
- entregar a documentação técnica atualizada da solução implantada;
- apresentar o conjunto de documentos "as built" ao término da execução.

Após a conclusão da implantação, deverão ser realizados treinamentos técnico-operacionais destinados aos servidores indicados pela Administração, abrangendo:

- utilização do sistema de CFTV;
- operação do sistema de controle de acesso;
- procedimentos básicos relacionados à infraestrutura de rede implantada;
- orientações quanto aos procedimentos de contingência e operação cotidiana dos sistemas.

A homologação da solução ficará condicionada à comprovação do pleno funcionamento integrado dos subsistemas e à conclusão satisfatória dos treinamentos previstos.

g) Integração e arquitetura unificada

Todos os subsistemas deverão operar de forma integrada, assegurando:

- interoperabilidade entre CFTV, controle de acesso e infraestrutura de rede;
- gestão centralizada por meio de interface web;
- segmentação lógica dos serviços;
- aplicação de mecanismos de segurança da informação;
- possibilidade de expansão futura sem necessidade de reestruturação integral da infraestrutura implantada.

h) Resultados esperados

A solução deverá proporcionar:

- infraestrutura de rede robusta e certificada;
- backbone óptico estável e validado;
- conectividade adequada aos ambientes acadêmicos e administrativos;
- cobertura sem fio corporativa;
- monitoramento contínuo das áreas estratégicas do campus;

- controle automatizado de acesso de pessoas e veículos;
- proteção física e lógica integrada;
- suporte adequado às atividades de ensino;
- padronização tecnológica institucional;
- escalabilidade e sustentabilidade operacional da infraestrutura implantada.

i) Conformidade normativa e técnica

A solução deverá observar os princípios, normas e diretrizes aplicáveis, especialmente:

- Lei nº 14.133/2021;
- normas internas e diretrizes de TIC do IFSP;
- ABNT NBR 14565;
- ANSI/TIA-568;
- ISO/IEC 11801;
- normas aplicáveis à certificação de enlaces ópticos;
- ABNT NBR ISO/IEC 27001;
- NR-10;
- NR-35, quando aplicável;
- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais;
- Política de Segurança da Informação do IFSP.

j) Descrição da Solução de TIC a ser contratada:

Declara-se que o objeto desta contratação constitui uma única Solução de Tecnologia da Informação e Comunicação (TIC), composta por componentes tecnicamente integrados e funcionalmente interdependentes, compreendendo infraestrutura de rede, backbone óptico, equipamentos ativos, sistema de videomonitoramento (CFTV), controle de acesso, softwares e serviços especializados de implantação, configuração, integração, testes e homologação. Assim, a contratação não se enquadra nas hipóteses de vedação previstas nos arts. 3º e 4º da Instrução Normativa SGD /MGI nº 94/2022, tratando-se de solução integrada de TIC abrangida pelo art. 2º, inciso I, da referida Instrução Normativa.

Dessa forma, a solução proposta mostra-se adequada para atender às necessidades identificadas para o IFSP – Campus Diadema, assegurando infraestrutura tecnológica integrada, segura, escalável e compatível com os padrões institucionais necessários ao pleno funcionamento da unidade.

K) Justificativa para definição das parcelas de maior relevância técnica e dos quantitativos mínimos para comprovação da capacidade técnico-operacional

Nos termos do art. 67 da Lei nº 14.133/2021, a definição das parcelas de maior relevância técnica foi realizada pela equipe de planejamento da contratação com base em **critérios técnicos**, considerando, de forma conjunta:

- a essencialidade do equipamento ou serviço para o funcionamento da solução integrada;
- a complexidade técnica de fornecimento, instalação, configuração, integração e homologação;
- a necessidade de conhecimentos técnicos especializados para sua execução;
- os riscos operacionais decorrentes de eventual execução inadequada;
- o impacto do componente na disponibilidade, segurança, desempenho e funcionamento da infraestrutura tecnológica do campus.

A seleção das parcelas não decorreu exclusivamente do valor financeiro dos itens ou dos quantitativos previstos, mas da avaliação técnica acerca de sua criticidade para o adequado funcionamento da solução integrada de infraestrutura de rede, segurança eletrônica e controle de acesso.

Com base nesses critérios, foram selecionadas as seguintes parcelas de maior relevância técnica:

Tabela 1- Parcelas de Maior Relevância Técnica para fins de Comprovação da Capacidade Técnico-Operacional

Subsistema	Grupo	Item	Descrição	Quantidade a ser comprovada	Unidade de Medida
Infraestrutura de Rede Lógica	01	25	Infraestrutura de Rede	1	Serviço
Infraestrutura de Rede Lógica	01	13	Cabo CAT6	3.750	Metro
Infraestrutura de Rede Lógica	01	26	Instalação, Validação e Homologação	1	Serviço
Equipamentos Ativos de Rede	01	2	Ponto de Acesso Interno (AP Wi-Fi)	15	Unidade
Equipamentos Ativos de Rede	01	5	Switch 48 Portas PoE	3	Unidade
Equipamentos Ativos de Rede	01	14	Firewall	1	Unidade
Sistema de Videomonitoramento (CFTV)	02	29	Câmera IP Bullet para Videomonitoramento	7	Unidade
Sistema de Videomonitoramento (CFTV)	02	30	Câmera IP Dome para Videomonitoramento	9	Unidade
Sistema de Controle de Acesso	03	51	Controlador de acesso com reconhecimento facial	5	Unidade
Sistema de Controle de Acesso	03	55	Software de Gerenciamento	1	Unidade
Sistema de Controle de Acesso	03	48	Catraca Facial	1	Unidade
Sistema de Controle de Acesso	03	49	Catraca PNE	1	Unidade

Para fins de comprovação da capacidade técnico-operacional, adotou-se, como regra geral, quantitativo correspondente a até 50% das quantidades previstas para contratação, observando o limite estabelecido no art. 67 da Lei nº 14.133/2021. Nos casos em que a parcela considerada de maior relevância possui quantitativo

unitário, a comprovação da execução de uma unidade decorre da impossibilidade material de fracionamento dessa experiência, sendo necessária para demonstrar que a licitante já executou anteriormente aquela parcela específica considerada crítica para o objeto.

L) Justificativa para a não exigência de garantia da contratação

Considerando a natureza do objeto e os riscos identificados no planejamento da contratação, optou-se pela não exigência da garantia da contratação prevista nos arts. 96 e seguintes da Lei nº 14.133/2021. A execução contratual contará com mecanismos suficientes de mitigação de riscos, tais como fiscalização permanente por equipe designada, critérios de recebimento provisório e definitivo, aplicação das sanções administrativas cabíveis, obrigação de garantia dos equipamentos fornecidos, suporte técnico e assistência técnica durante o período contratual. Dessa forma, conclui-se que a exigência de garantia de execução contratual mostra-se desnecessária e desproporcional ao caso concreto, podendo restringir a competitividade e elevar os custos da contratação sem benefício proporcional à Administração.

13. Estimativa de custo total da contratação

Valor (R\$): 1.740.822,52

A estimativa do valor da contratação foi elaborada com base em pesquisa de preços realizada junto a fornecedores especializados nos segmentos de infraestrutura de Tecnologia da Informação e Comunicação (TIC), segurança eletrônica, controle de acesso, equipamentos de rede, videomonitoramento, infraestrutura óptica e recursos tecnológicos de apoio às atividades acadêmicas, considerando o escopo integral da solução definida neste Estudo Técnico Preliminar.

A pesquisa de preços contemplou o fornecimento de materiais, equipamentos, softwares, licenças, infraestrutura física, mão de obra especializada e serviços técnicos necessários à implantação completa da solução integrada destinada ao Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – IFSP, Campus Diadema, incluindo instalação, configuração, integração, certificação, testes, treinamento operacional e homologação dos sistemas.

A formação do preço estimado observou as disposições do art. 23 da Lei nº 14.133, de 1º de abril de 2021, bem como os procedimentos estabelecidos pela Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, especialmente quanto à utilização de parâmetros de mercado idôneos e compatíveis com as especificações técnicas do objeto.

Para composição do orçamento estimativo, foram consideradas cotações obtidas junto a empresas atuantes no mercado especializado, além da análise da compatibilidade entre os preços praticados e as características técnicas dos materiais, equipamentos e serviços previstos na solução escolhida.

Após a consolidação das informações coletadas e a análise crítica dos valores obtidos, chegou-se ao valor estimado global de R\$ R\$ 1.740.822,52 (um milhão, setecentos e quarenta mil, oitocentos e vinte e dois reais e cinquenta e dois centavos.). para a contratação da solução integrada de infraestrutura tecnológica e segurança eletrônica do IFSP – Campus Diadema.

O valor estimado contempla, dentre outros componentes, os custos relacionados a:

- fornecimento de materiais para implantação da infraestrutura de rede lógica estruturada categoria 6;
- fornecimento e instalação de backbone óptico em fibra monomodo;
- odo, incluindo DIO, emendas por fusão, certificações e testes;
- fornecimento e instalação de infraestrutura física de telecomunicações, incluindo eletrocalhas, eletrodutos, canaletas, suportes e demais elementos necessários à acomodação e proteção dos sistemas implantados;
- fornecimento, instalação e configuração de equipamentos ativos de rede, incluindo switches gerenciáveis, pontos de acesso Wi-Fi corporativos, firewall e acessórios;
- fornecimento e implantação do sistema de videomonitoramento IP, incluindo câmeras, gravadores NVR, unidades de armazenamento e infraestrutura complementar;

- fornecimento e implantação do sistema de controle de acesso, incluindo catracas com reconhecimento facial, catracas acessíveis, controladores faciais, fechaduras eletromagnéticas, cancelas automáticas e respectivos acessórios;
- fornecimento de softwares, licenças e recursos necessários à gestão integrada dos sistemas;
- fornecimento de equipamentos tecnológicos de apoio às atividades acadêmicas, incluindo projetores multimídia e acessórios;
- execução dos serviços especializados de instalação, configuração, integração, certificação, validação, testes funcionais e homologação da solução implantada;
- elaboração do projeto executivo e atualização da documentação técnica da infraestrutura implantada;
- realização de treinamento técnico-operacional destinado aos servidores indicados pela Administração;
- fornecimento das garantias contratuais e dos suportes técnicos previstos nas especificações do Termo de Referência.

O valor estimado reflete a complexidade e a abrangência da solução proposta, considerando a necessidade de implantação integrada da infraestrutura tecnológica necessária ao início das atividades acadêmicas e administrativas do Campus Diadema, bem como os padrões institucionais de desempenho, segurança, interoperabilidade e escalabilidade adotados pelo IFSP.

Ressalta-se que a estimativa foi elaborada com base nas condições de mercado vigentes à época da realização da pesquisa de preços, constituindo parâmetro de referência para a avaliação da vantajosidade das propostas a serem apresentadas no certame.

Os documentos que subsidiaram a formação do orçamento estimativo encontram-se devidamente juntados aos autos do processo administrativo, assegurando a transparência, a rastreabilidade dos critérios adotados e a observância aos princípios da legalidade, da economicidade, da eficiência e da seleção da proposta mais vantajosa para a Administração Pública.

Dessa forma, conclui-se que o valor estimado de R\$ 1.740.822,52 (um milhão, setecentos e quarenta mil, oitocentos e vinte e dois reais e cinquenta e dois centavos.) representa a melhor estimativa disponível para a implantação da solução integrada de infraestrutura tecnológica e segurança eletrônica do IFSP – Campus Diadema, sendo compatível com os quantitativos, especificações técnicas e resultados pretendidos pela Administração.

14. Justificativa técnica da escolha da solução

A solução escolhida, consistente na implantação integrada da infraestrutura tecnológica e dos sistemas de segurança eletrônica do **Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – IFSP, Campus Diadema**, foi selecionada por atender plenamente aos requisitos técnicos, funcionais, operacionais e institucionais identificados durante as etapas de levantamento das necessidades, análise comparativa das alternativas disponíveis e avaliação econômica realizadas neste Estudo Técnico Preliminar.

A solução contempla a implantação de infraestrutura de rede lógica estruturada, backbone óptico em fibra monomodo, equipamentos ativos de rede, conectividade sem fio corporativa, recursos de segurança perimetral, sistema de videomonitoramento IP, controle automatizado de acesso de pessoas e veículos, recursos tecnológicos de apoio às atividades acadêmicas e serviços técnicos especializados de instalação, configuração, integração, testes e homologação.

A decisão pela adoção da solução integrada fundamenta-se nos seguintes aspectos técnicos:

a) Integração entre os subsistemas tecnológicos

A solução proposta reúne, em uma única arquitetura tecnológica, os sistemas de rede de dados, backbone óptico, conectividade sem fio, videomonitoramento, controle de acesso e gerenciamento centralizado dos dispositivos implantados.

A integração entre esses subsistemas possibilita interoperabilidade operacional, gestão unificada, compartilhamento de infraestrutura e maior eficiência na administração dos recursos tecnológicos da unidade.

Adicionalmente, a adoção de arquitetura integrada reduz a ocorrência de incompatibilidades técnicas entre equipamentos e softwares, simplifica os procedimentos de manutenção e favorece a rastreabilidade dos eventos relacionados à segurança física e lógica do campus.

b) Adequação às necessidades institucionais do Campus Diadema

A solução foi dimensionada especificamente para atender às necessidades do Campus Diadema, considerando o início de suas atividades acadêmicas e administrativas e a necessidade de disponibilização imediata de infraestrutura tecnológica adequada ao funcionamento da unidade.

Foram considerados aspectos relacionados à quantidade estimada de usuários, distribuição física dos ambientes, necessidade de cobertura das áreas estratégicas para videomonitoramento, controle de acesso de pedestres e veículos, conectividade para ambientes administrativos e acadêmicos, bem como suporte às atividades de ensino desenvolvidas pela instituição.

Dessa forma, a solução selecionada não constitui mera aquisição de equipamentos isolados, mas sim a implantação de infraestrutura tecnológica integrada e funcional, capaz de atender às demandas presentes e futuras da unidade.

c) Aderência às normas técnicas e aos padrões institucionais

A solução foi concebida em conformidade com as normas técnicas aplicáveis à infraestrutura de redes, segurança da informação e instalações de telecomunicações, observando, dentre outras:

- ABNT NBR 14565 – Cabeamento estruturado para edifícios comerciais e data centers;
- ANSI/TIA-568 – Commercial Building Telecommunications Cabling Standard;
- ISO/IEC 11801 – Information technology – Generic cabling for customer premises;
- ABNT NBR ISO/IEC 27001 – Sistemas de Gestão da Segurança da Informação;
- normas aplicáveis à certificação de enlaces ópticos e ensaios de refletometria óptica;
- NR-10 – Segurança em instalações e serviços em eletricidade;
- NR-35 – Trabalho em altura, quando aplicável;
- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais;
- Política de Segurança da Informação e diretrizes de Tecnologia da Informação adotadas pelo IFSP.

A observância dessas normas assegura qualidade técnica, segurança operacional, padronização institucional e conformidade regulatória da infraestrutura implantada.

d) Confiabilidade e disponibilidade operacional

Os equipamentos e componentes previstos na solução apresentam características compatíveis com ambientes corporativos e educacionais de médio porte, priorizando durabilidade, estabilidade operacional, disponibilidade de suporte técnico e ampla oferta de assistência especializada no mercado nacional.

A utilização de equipamentos compatíveis com protocolos amplamente difundidos reduz riscos de obsolescência precoce e amplia as possibilidades de substituição e expansão futura sem comprometimento da infraestrutura existente.

Além disso, a utilização de backbone óptico, equipamentos ativos gerenciáveis e mecanismos adequados de segmentação lógica contribui para a continuidade dos serviços e para a redução da ocorrência de interrupções não planejadas.

e) Escalabilidade e sustentabilidade tecnológica

A solução foi estruturada de forma modular e escalável, permitindo ampliações futuras da infraestrutura sem necessidade de substituição integral dos componentes instalados.

A utilização de cabeamento estruturado categoria 6, backbone óptico em fibra monomodo, switches gerenciáveis, controladores faciais baseados em tecnologia IP e sistemas integrados de gerenciamento favorece a evolução gradual da infraestrutura tecnológica, acompanhando o crescimento da unidade e a incorporação de novas demandas institucionais.

Essa característica contribui para a sustentabilidade tecnológica da solução e para a otimização dos investimentos públicos realizados.

f) Segurança física e lógica integrada

A integração entre os sistemas de controle de acesso e videomonitoramento possibilita maior efetividade na proteção do patrimônio público, na gestão do fluxo de pessoas e na preservação da integridade física da comunidade acadêmica.

Os mecanismos de autenticação facial, controle automatizado de acessos, rastreabilidade de eventos e correlação entre registros de acesso e imagens capturadas pelas câmeras ampliam significativamente a capacidade institucional de prevenção, monitoramento e resposta a ocorrências.

Sob a perspectiva da segurança lógica, a utilização de firewall corporativo, segmentação de tráfego e mecanismos adequados de gerenciamento contribui para a proteção das informações institucionais e dos recursos tecnológicos disponibilizados pela unidade.

g) Racionalização dos custos de implantação e manutenção

Embora a solução integrada demande maior investimento inicial, sua adoção reduz significativamente os custos associados à manutenção corretiva, à substituição prematura de equipamentos e à necessidade de readequações futuras da infraestrutura.

A execução coordenada dos serviços de infraestrutura, instalação, configuração e homologação reduz retrabalhos, otimiza o uso dos recursos disponíveis e favorece a unificação das garantias técnicas associadas aos equipamentos e serviços contratados.

Além disso, a incorporação definitiva dos ativos ao patrimônio do IFSP fortalece a autonomia institucional e reduz a dependência de contratações recorrentes para disponibilização dos recursos tecnológicos essenciais ao funcionamento do campus.

Conclusão

Diante das análises realizadas, conclui-se que a solução integrada selecionada representa a alternativa tecnicamente mais adequada para atender às necessidades do IFSP – Campus Diadema.

A solução demonstra superioridade sob os aspectos de desempenho, confiabilidade, interoperabilidade, segurança, escalabilidade, sustentabilidade tecnológica e racionalização dos custos ao longo do ciclo de vida da infraestrutura.

Adicionalmente, mostra-se plenamente aderente aos princípios do planejamento, da eficiência, da economicidade, da obtenção da proposta mais vantajosa e do atendimento ao interesse público previstos na Lei nº 14.133/2021.

Dessa forma, a escolha da solução integrada encontra-se tecnicamente justificada, constituindo a alternativa que melhor equilibra robustez operacional, inovação tecnológica, segurança institucional e sustentabilidade dos investimentos necessários à implantação e ao funcionamento do IFSP – Campus Diadema.

15. Justificativa econômica da escolha da solução

A escolha da solução integrada para implantação da infraestrutura tecnológica e dos sistemas de segurança eletrônica do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – IFSP, Campus Diadema encontra respaldo não apenas nos aspectos técnicos e operacionais já demonstrados neste Estudo Técnico Preliminar, mas também em critérios objetivos de vantajosidade econômica para a Administração Pública.

A análise econômica foi realizada com base nos resultados obtidos durante o levantamento de soluções disponíveis no mercado e na análise comparativa de custos, considerando o custo total de propriedade da solução (Total Cost of Ownership – TCO) ao longo do seu ciclo de vida estimado, abrangendo os custos de aquisição, implantação, operação, manutenção, atualização tecnológica e expansão futura da infraestrutura.

Os estudos demonstraram que, embora a solução integrada demande investimento inicial superior às demais alternativas avaliadas, ela apresenta o melhor desempenho econômico no médio e longo prazo, revelando-se a opção mais vantajosa para a Administração.

A justificativa econômica da escolha fundamenta-se nos seguintes aspectos:

a) Menor custo total de ciclo de vida

A infraestrutura proposta foi concebida com base em tecnologias amplamente difundidas e compatíveis com ambientes corporativos e educacionais, priorizando equipamentos com maior durabilidade, estabilidade operacional e disponibilidade de suporte técnico no mercado nacional.

A utilização de infraestrutura estruturada, backbone óptico, equipamentos ativos gerenciáveis e sistemas integrados de segurança reduz significativamente a necessidade de substituições prematuras, minimizando os custos associados à manutenção corretiva e à renovação antecipada dos ativos tecnológicos.

Dessa forma, o investimento inicial mais elevado é compensado pela redução dos custos operacionais e pela maior vida útil dos componentes implantados, resultando em menor custo global ao longo do período de utilização da solução.

b) Redução dos custos de manutenção e suporte técnico

Os equipamentos previstos na solução integrada apresentam características compatíveis com utilização contínua em ambientes institucionais, permitindo maior previsibilidade das ações de manutenção preventiva e reduzindo a ocorrência de falhas críticas.

Além disso, a padronização dos componentes tecnológicos simplifica os processos de suporte, reduz o estoque de peças de reposição necessárias e favorece a capacitação das equipes responsáveis pela gestão e fiscalização contratual.

A adoção de soluções integradas também reduz a necessidade de contratação de múltiplos fornecedores especializados para manutenção de tecnologias distintas, contribuindo para a racionalização dos custos administrativos associados à operação da infraestrutura.

c) Eliminação de retrabalhos e duplicidade de investimentos

A implantação completa e integrada da infraestrutura tecnológica do Campus Diadema evita a necessidade de intervenções sucessivas decorrentes de implantações fragmentadas ou provisórias.

A execução coordenada dos serviços de infraestrutura física, cabeamento estruturado, backbone óptico, instalação dos equipamentos ativos, implantação dos sistemas de CFTV e controle de acesso reduz significativamente os custos decorrentes de desmontagens, adaptações, remanejamentos e reconfigurações futuras.

Essa abordagem proporciona melhor aproveitamento dos recursos públicos investidos, reduzindo desperdícios e assegurando maior eficiência na execução contratual.

d) Economia de escala decorrente da contratação integrada

A contratação conjunta dos materiais, equipamentos e serviços necessários à implantação da solução permite maior eficiência econômica decorrente da consolidação dos quantitativos previstos.

A aquisição integrada favorece a obtenção de condições comerciais mais vantajosas, redução de custos logísticos, otimização do processo de instalação e melhor aproveitamento da mobilização das equipes técnicas responsáveis pela execução do objeto.

Além disso, a centralização da contratação contribui para a simplificação dos procedimentos administrativos e para a redução dos custos indiretos relacionados à gestão contratual.

e) Geração de patrimônio público permanente

Diferentemente das alternativas baseadas em locação ou terceirização integral dos serviços, a solução escolhida resulta na incorporação definitiva dos equipamentos e da infraestrutura ao patrimônio do IFSP.

Os investimentos realizados passam a compor os ativos permanentes da instituição, assegurando autonomia administrativa sobre os recursos tecnológicos implantados e ampliando o retorno institucional decorrente da aplicação dos recursos públicos.

A geração de patrimônio próprio fortalece a capacidade operacional do Campus Diadema e reduz a dependência de contratações recorrentes para disponibilização de recursos essenciais ao funcionamento da unidade.

f) Sustentabilidade financeira da infraestrutura implantada

A solução adotada foi concebida considerando a possibilidade de crescimento futuro do campus e a necessidade de ampliação gradual da infraestrutura tecnológica.

A utilização de arquitetura modular e escalável permite que futuras expansões sejam realizadas de forma planejada, aproveitando a infraestrutura já existente e reduzindo os custos associados a novas implantações.

Essa característica favorece a sustentabilidade financeira da solução e contribui para a preservação dos investimentos realizados pela Administração Pública.

g) Maior previsibilidade orçamentária

A implantação integral da solução possibilita melhor controle dos custos associados ao ciclo de vida da infraestrutura tecnológica do campus, reduzindo a ocorrência de despesas emergenciais decorrentes de falhas sistêmicas, incompatibilidades técnicas ou necessidade de adequações não previstas.

A previsibilidade dos custos de manutenção e operação contribui para o adequado planejamento orçamentário da unidade, favorecendo a gestão eficiente dos recursos institucionais.

Conclusão

A partir das análises realizadas, conclui-se que a solução integrada selecionada apresenta viabilidade econômica e vantajosidade global, representando a alternativa que melhor equilibra investimento inicial, desempenho operacional, durabilidade, custos de manutenção e potencial de expansão futura.

Embora demande maior aporte inicial de recursos, a solução proporciona menor custo total de propriedade ao longo do ciclo de vida da infraestrutura, elimina retrabalhos, reduz custos operacionais, gera patrimônio público permanente e assegura maior autonomia tecnológica ao IFSP.

Dessa forma, a solução escolhida demonstra-se economicamente justificável e compatível com os princípios da economicidade, eficiência, planejamento, sustentabilidade e obtenção da proposta mais vantajosa para a Administração Pública, previstos na Lei nº 14.133/2021, especialmente em seus arts. 5º, 11 e 18.

Considerando o valor estimado da contratação, os benefícios institucionais decorrentes da implantação integrada da infraestrutura e os custos evitados ao longo do tempo, verifica-se que a solução adotada representa a melhor aplicação dos recursos públicos destinados à estruturação tecnológica do IFSP – Campus Diadema, assegurando condições adequadas para o desenvolvimento das atividades acadêmicas e administrativas da unidade e preservando o interesse público que orienta a presente contratação.

16. Justificativa da Estruturação do Objeto

A estruturação do objeto em **lote único**, composto por três macrogrupos tecnicamente integrados — **Projeto Rede de Dados Local**, **Projeto CFTV** e **Projeto Controle de Acesso** — fundamenta-se na necessidade de assegurar plena integração física, lógica e operacional da infraestrutura tecnológica e dos sistemas de segurança eletrônica a serem implantados no **IFSP – Campus Diadema**.

Conforme planilha orçamentária, o objeto encontra-se organizado em três conjuntos principais:

I – **Projeto Rede de Dados Local**, contemplando cabeamento estruturado Cat6, conectores, patch cords, patch panels, racks, switches gerenciáveis, access points Wi-Fi, firewall, infraestrutura física de rede, backbone óptico, DIO, fusões ópticas, projetores multimídia, suportes, extensores HDMI e serviços de instalação, configuração, validação e homologação da rede;

II – **Projeto CFTV**, contemplando NVR, disco rígido para gravação contínua, câmeras IP, switches PoE, racks, patch panels, caixas de proteção, cabeamento, postes, suportes, TV de monitoramento, concertina, grades de proteção e serviços de infraestrutura, instalação, configuração e testes;

III – **Projeto Controle de Acesso**, contemplando catracas com leitores faciais, catraca acessível PNE/PCD, cancelas automáticas, controladores faciais, kits de fechos eletroímãs, botoeiras, fontes, acionadores de emergência, portões auxiliares, fechamento em aço inox, software de gerenciamento integrado, serviços de instalação, validação e infraestrutura dedicada.

Embora esses macrogrupos possam ser identificados separadamente para fins de organização orçamentária e descritiva, eles compõem uma **solução única e integrada**, destinada à implantação da infraestrutura tecnológica e de segurança do Campus Diadema. A divisão do objeto em lotes independentes mostraria-se tecnicamente inadequada e economicamente desvantajosa, pois os componentes compartilham infraestrutura física, lógica, elétrica, endereçamento, segmentação de rede, protocolos de comunicação, equipamentos ativos e sistemas de gerenciamento.

A infraestrutura de rede de dados constitui a base operacional dos demais sistemas. O CFTV depende da rede estruturada, dos switches, dos pontos de dados, da alimentação PoE e da adequada segmentação lógica para transmissão, gravação e acesso às imagens. Da mesma forma, o controle de acesso depende da rede lógica, dos pontos de energia, dos controladores, do software integrado e da comunicação com os demais sistemas de segurança.

A implantação do backbone óptico, dos racks, dos switches gerenciáveis, dos pontos de acesso sem fio e do firewall deve ocorrer de forma coordenada com os sistemas de CFTV e controle de acesso, a fim de garantir desempenho, disponibilidade, segurança da informação e interoperabilidade entre os subsistemas.

A fragmentação do objeto em múltiplos lotes poderia acarretar:

- incompatibilidades técnicas entre equipamentos, softwares, protocolos e padrões de configuração fornecidos por empresas distintas;
- dificuldades de integração entre rede de dados, CFTV e controle de acesso;
- indefinição de responsabilidade técnica em caso de falhas de comunicação, gravação, autenticação, acesso ou desempenho;
- sobreposição de garantias e dificuldade de acionamento de suporte;
- retrabalhos decorrentes de falhas de projeto, instalação ou parametrização;
- aumento dos custos administrativos e operacionais com múltiplos contratos;
- maior complexidade na fiscalização, validação, certificação e homologação;
- risco de comprometimento da Prova de Conceito, dos testes integrados e da entrega funcional da solução;
- atraso na implantação da infraestrutura necessária ao início das atividades acadêmicas e administrativas do campus.

Sob a ótica da gestão contratual, o lote único possibilita responsabilização técnica centralizada, cronograma único de implantação, compatibilização entre projeto executivo, instalação, configuração, testes, treinamento e homologação, bem como maior eficiência na fiscalização do contrato.

Além disso, a contratação integrada permite economia de escopo, reduzindo custos de mobilização, logística, retrabalho e coordenação entre fornecedores. Também favorece a padronização tecnológica e a entrega de solução funcional, certificada e homologada de forma conjunta.

A opção pelo lote único não decorre de mera conveniência administrativa, mas da interdependência técnica entre os elementos da solução. O objeto envolve infraestrutura física, rede lógica, backbone óptico, equipamentos ativos,

CFTV, controle de acesso, software de gerenciamento e serviços técnicos especializados, cuja execução dissociada poderia comprometer a integridade funcional da solução.

Dessa forma, considerando a natureza integrada do objeto, a dependência entre os subsistemas, a necessidade de compatibilidade técnica e a importância de garantir uma única responsabilidade pela implantação, configuração, testes e homologação, conclui-se que a estruturação em **lote único**, organizado em três macrogrupos — **Rede de Dados Local, CFTV e Controle de Acesso** — é tecnicamente necessária, economicamente vantajosa e juridicamente adequada.

Assim, a contratação em lote único assegura interoperabilidade, continuidade operacional, padronização tecnológica, segurança, eficiência administrativa e adequada responsabilização pela entrega da solução integrada destinada ao **IFSP – Campus Diadema**, em conformidade com os princípios do planejamento, eficiência, economicidade e seleção da proposta mais vantajosa previstos na Lei nº 14.133/2021.

17. Benefícios a serem alcançados com a contratação

A contratação da solução integrada de infraestrutura tecnológica e segurança eletrônica para o Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – IFSP, Campus Diadema proporcionará benefícios diretos, estruturantes e mensuráveis à Administração Pública, contribuindo para a adequada implantação da unidade e para o desenvolvimento seguro e eficiente de suas atividades acadêmicas e administrativas.

A solução contempla a implantação integrada de infraestrutura de rede de dados, backbone óptico, equipamentos ativos de rede, conectividade sem fio corporativa, sistema de videomonitoramento (CFTV), sistema de controle de acesso de pessoas e veículos, recursos audiovisuais destinados aos ambientes de ensino e serviços técnicos especializados de instalação, configuração, certificação, testes e homologação.

Sob a perspectiva operacional, institucional e estratégica, a contratação permitirá consolidar ambiente tecnológico moderno, seguro, integrado e padronizado, alinhado às diretrizes corporativas de Tecnologia da Informação e Comunicação do IFSP e às necessidades decorrentes da implantação do Campus Diadema.

Os principais benefícios esperados são os seguintes:

a) Melhoria da segurança física e patrimonial

- Monitoramento contínuo das áreas internas e externas do campus, mediante utilização de sistema de CFTV baseado em tecnologia IP;
- Gravação e armazenamento de imagens em alta resolução, possibilitando consulta posterior e apoio à apuração de ocorrências;
- Controle automatizado e rastreável do acesso de pessoas, mediante utilização de catracas e controladores com reconhecimento facial;
- Controle do acesso de veículos por meio de cancelas automatizadas e dispositivos integrados ao sistema de segurança;
- Redução dos riscos relacionados a invasões, furtos, depredações e demais incidentes patrimoniais;
- Maior agilidade na resposta a ocorrências, em razão da integração entre os sistemas de monitoramento e controle de acesso.

b) Disponibilização de infraestrutura tecnológica adequada ao funcionamento do campus

- Implantação de infraestrutura de rede estruturada compatível com as necessidades administrativas e acadêmicas da unidade;
- Disponibilização de backbone óptico de alta capacidade, assegurando desempenho adequado para os serviços institucionais;
- Implantação de conectividade sem fio corporativa em áreas estratégicas do campus;
- Disponibilização de infraestrutura tecnológica apta a suportar sistemas acadêmicos, administrativos e demais aplicações institucionais;
- Garantia de condições adequadas para o início e continuidade das atividades da unidade.

c) Melhoria do desempenho e da confiabilidade dos serviços de Tecnologia da Informação

- Maior estabilidade e disponibilidade dos serviços de rede;
- Redução de falhas decorrentes de infraestruturas improvisadas ou fragmentadas;
- Segmentação adequada do tráfego de dados, assegurando melhor utilização dos recursos computacionais disponíveis;
- Proteção da infraestrutura institucional por meio da utilização de equipamentos de segurança perimetral compatíveis com as necessidades do campus;
- Ampliação da capacidade de gerenciamento e monitoramento dos ativos tecnológicos.

d) Fortalecimento da governança e da segurança da informação

- Implementação de mecanismos que favoreçam a confidencialidade, integridade, disponibilidade e rastreabilidade das informações institucionais;
- Alinhamento às diretrizes estabelecidas pela Política de Segurança da Informação do IFSP;
- Contribuição para o atendimento às disposições da Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018);
- Ampliação da capacidade institucional de monitoramento e gestão dos ativos de TIC;
- Maior controle sobre eventos relacionados ao acesso físico às dependências da instituição.

e) Otimização da gestão operacional

- Centralização da gestão dos sistemas de segurança e controle de acesso;
- Simplificação dos processos relacionados ao gerenciamento do fluxo de pessoas e veículos;
- Maior eficiência na identificação e resolução de falhas operacionais;
- Redução do tempo necessário para manutenção e suporte dos sistemas implantados;
- Padronização dos procedimentos técnicos relacionados à infraestrutura tecnológica do campus.

f) Suporte às atividades acadêmicas e administrativas

- Disponibilização de recursos tecnológicos adequados ao desenvolvimento das atividades de ensino;
- Implantação de equipamentos audiovisuais destinados ao apoio às atividades pedagógicas e institucionais;
- Disponibilização de infraestrutura de rede compatível com ambientes administrativos, laboratórios e salas de aula;
- Ampliação das condições de utilização de ferramentas digitais e recursos tecnológicos pela comunidade acadêmica;
- Contribuição para a melhoria da experiência dos usuários dos serviços institucionais.

g) Escalabilidade e sustentabilidade tecnológica

- Possibilidade de expansão futura da infraestrutura implantada sem necessidade de reestruturação integral dos sistemas;
- Facilidade de incorporação de novos equipamentos e serviços à arquitetura tecnológica existente;
- Aproveitamento da infraestrutura instalada para atendimento de demandas futuras decorrentes da expansão do campus;
- Redução dos custos associados a adequações estruturais posteriores;
- Preservação dos investimentos realizados pela Administração Pública.

h) Eficiência administrativa e econômica

- Redução de custos decorrentes de retrabalhos e intervenções corretivas futuras;
- Diminuição da necessidade de contratações emergenciais relacionadas à infraestrutura tecnológica;
- Maior previsibilidade dos custos de manutenção e operação dos sistemas implantados;
- Racionalização dos recursos humanos envolvidos na gestão da infraestrutura tecnológica e dos sistemas de segurança;
- Incorporação dos equipamentos e da infraestrutura ao patrimônio permanente do IFSP.

i) Benefícios institucionais e estratégicos

- Implantação de ambiente tecnológico compatível com os padrões adotados nos campi do IFSP;
- Fortalecimento da imagem institucional do IFSP como organização comprometida com inovação, segurança e qualidade dos serviços prestados;
- Contribuição para a continuidade das atividades acadêmicas e administrativas do Campus Diadema;
- Apoio ao processo de expansão da Rede Federal de Educação Profissional, Científica e Tecnológica;
- Alinhamento ao planejamento institucional e às estratégias de desenvolvimento da infraestrutura do IFSP.

Síntese

A execução da presente contratação proporcionará ganhos concretos relacionados à segurança física, à conectividade institucional, à governança de Tecnologia da Informação, à eficiência administrativa e à sustentabilidade dos investimentos realizados pela Administração Pública.

A solução permitirá que o IFSP – Campus Diadema disponha de infraestrutura tecnológica moderna, integrada, segura e escalável, compatível com o início de suas atividades acadêmicas e administrativas e preparada para acompanhar o crescimento futuro da unidade, assegurando a adequada prestação dos serviços educacionais e o atendimento ao interesse público.

18. Providências a serem Adotadas

Para a efetiva implementação da solução integrada de infraestrutura tecnológica e segurança eletrônica destinada ao Instituto Federal de Educação, Ciência e Tecnologia de São Paulo – IFSP, Campus Diadema, deverão ser observadas as providências administrativas, técnicas e operacionais descritas a seguir, sob responsabilidade do Campus Diadema, com apoio das áreas técnicas competentes da Reitoria, especialmente da Diretoria de Tecnologia da Informação e demais unidades envolvidas na gestão da contratação.

a) Planejamento e instrução processual

- Consolidação e formalização dos documentos que compõem a fase preparatória da contratação, incluindo Estudo Técnico Preliminar, Termo de Referência, mapa de riscos, pesquisa de preços e demais documentos exigidos pela legislação vigente;
- Validação das especificações técnicas pela área demandante e pelos setores técnicos responsáveis pela infraestrutura de Tecnologia da Informação e Comunicação;
- Verificação da disponibilidade orçamentária para suportar a contratação pretendida;
- Inclusão da demanda nos instrumentos de planejamento institucional aplicáveis;
- Encaminhamento do processo às instâncias competentes para análise e autorização da contratação.

b) Procedimento licitatório

- Realização do procedimento licitatório na modalidade Pregão Eletrônico, observando-se as disposições da Lei nº 14.133/2021, da regulamentação aplicável e das normas internas do IFSP;
- Elaboração e publicação do edital de licitação e respectivos anexos;
- Condução da fase externa do certame, incluindo análise das propostas, julgamento, habilitação e adjudicação do objeto;
- Realização de diligências e esclarecimentos eventualmente necessários ao adequado julgamento das propostas;
- Realização de Prova de Conceito (PoC), quando prevista no Termo de Referência, visando à validação prática da solução ofertada pela licitante provisoriamente classificada em primeiro lugar.

c) Formalização da contratação

- Emissão da respectiva Nota de Empenho;
- Celebração do instrumento contratual ou documento equivalente, conforme definido no edital;
- Publicação dos atos necessários à eficácia da contratação;

- Designação formal do gestor do contrato e dos fiscais técnico e administrativo, nos termos do art. 117 da Lei nº 14.133/2021;
- Capacitação dos servidores responsáveis pelo acompanhamento e fiscalização da execução contratual, quando necessário.

d) Providências prévias ao início da execução

- Disponibilização dos ambientes e áreas necessárias à execução dos serviços;
- Realização de reuniões iniciais entre a Administração e a contratada para alinhamento das atividades, cronograma e responsabilidades;
- Apresentação, pela contratada, do Projeto Executivo da solução, contemplando infraestrutura de rede, backbone óptico, sistema de CFTV, controle de acesso e demais elementos previstos na contratação;
- Análise e aprovação do Projeto Executivo pela Administração antes do início da implantação;
- Definição do cronograma executivo detalhado de implantação.

e) Execução contratual

- Acompanhamento sistemático da execução dos serviços pela equipe designada;
- Implantação da infraestrutura física necessária ao funcionamento dos sistemas;
- Execução do cabeamento estruturado metálico e do backbone óptico;
- Instalação dos equipamentos ativos de rede;
- Implantação do sistema de videomonitoramento;
- Implantação do sistema de controle de acesso de pessoas e veículos;
- Configuração, parametrização e integração dos subsistemas;
- Realização dos testes funcionais previstos no Termo de Referência;
- Correção de eventuais inconformidades identificadas durante a execução.

f) Entregas técnicas e documentais

A contratada deverá apresentar, ao longo da execução contratual e ao final dos serviços, a documentação técnica pertinente, incluindo, no mínimo:

- Projeto Executivo aprovado;
- Documentação técnica atualizada da solução implantada ("as built");
- Diagramas lógicos e físicos da infraestrutura instalada;
- Relatórios de certificação do cabeamento estruturado;
- Relatórios de testes dos enlaces ópticos;
- Relatórios de configuração e validação dos equipamentos instalados;
- Relatórios de testes integrados dos sistemas;
- Manuais técnicos e operacionais dos equipamentos e softwares fornecidos;
- Certificados de garantia dos equipamentos e serviços executados;
- Relação consolidada dos bens fornecidos.

g) Fiscalização e recebimento do objeto

- Monitoramento contínuo da execução contratual pelos fiscais designados;
- Registro das ocorrências relevantes em instrumentos próprios de fiscalização;
- Verificação do atendimento integral das especificações técnicas estabelecidas no Termo de Referência;
- Realização dos testes de aceitação previstos para homologação da solução;
- Emissão do Termo de Recebimento Provisório, nos termos da legislação vigente;
- Verificação do saneamento de eventuais pendências identificadas no recebimento provisório;
- Emissão do Termo de Recebimento Definitivo após a confirmação do pleno atendimento das obrigações contratuais.

h) Capacitação e transferência de conhecimento

- Realização de treinamento técnico-operacional destinado aos servidores indicados pela Administração;
- Orientação quanto à utilização dos sistemas de videomonitoramento e controle de acesso;
- Transferência das informações necessárias à operação cotidiana da infraestrutura implantada;

- Esclarecimento sobre procedimentos básicos de manutenção operacional e acionamento de suporte técnico.

i) Providências pós-implantação

- Inclusão dos bens adquiridos no sistema patrimonial do IFSP;
- Arquivamento da documentação técnica e contratual pertinente;
- Monitoramento inicial do desempenho da solução implantada;
- Acompanhamento do período de garantia dos equipamentos e serviços;
- Avaliação da necessidade de futuras ampliações ou integrações com outras soluções institucionais;
- Atualização dos registros internos relacionados aos ativos de Tecnologia da Informação e Comunicação.

Síntese

As providências acima descritas são indispensáveis para assegurar a adequada implementação da solução proposta, garantindo que a contratação seja conduzida de forma planejada, transparente e alinhada aos princípios da legalidade, eficiência, economicidade, segregação de funções e busca da proposta mais vantajosa para a Administração Pública.

A adoção dessas medidas contribuirá para o êxito da implantação da infraestrutura tecnológica e dos sistemas de segurança eletrônica do IFSP – Campus Diadema, assegurando a entrega de solução funcional, integrada e compatível com as necessidades institucionais da unidade.

19. Declaração de Viabilidade

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

19.1. Justificativa da Viabilidade com Restrições

A equipe declara a contratação viável, nos termos estabelecidos neste estudo.

20. 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](#).

DOUGLAS FRANCISQUINI TOLEDO

Agente de contratação



Assinou eletronicamente em 28/07/2026 às 20:31:39.

JOSE ROBERTO DA SILVA

Agente de contratação



Assinou eletronicamente em 28/07/2026 às 16:58:51.

CLAUDIA ALMERINDA DE SOUZA OLIVEIRA

Autoridade competente



Assinou eletronicamente em 29/07/2026 às 10:13:33.