

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

Estudo Técnico Preliminar 157/2025

1. Informações Básicas

Número do processo: 23305.020855.2025-94

2. Descrição da necessidade

2.1 Aquisição de Ferramenta de Gestão de Credenciais O Instituto Federal de Educação, Ciência e Tecnologia de São Paulo (IFSP), especificamente no âmbito de sua Diretoria de Tecnologia da Informação (DTI), enfrenta um cenário de risco latente relacionado à gestão de credenciais de alto privilégio (acessos administrativos a servidores, bancos de dados e infraestrutura de nuvem). Atualmente, a equipe técnica mitigou parcialmente o risco operacional através da adoção da solução Bitwarden. Contudo, este uso ocorre em um ambiente misto e não institucionalizado, onde:

- Parte dos servidores utiliza a versão gratuita, que não oferece recursos corporativos essenciais como trilhas de auditoria (logs) detalhadas, gestão centralizada de políticas de segurança e revogação imediata de acesso em caso de desligamento;
- Outra parcela, que necessita de recursos avançados, utiliza a versão Enterprise custeada com recursos próprios (Pessoa Física), o que gera uma anomalia administrativa onde servidores financiam ferramentas de trabalho do Estado.

2.2 Histórico de Adoção e Benchmarking Técnico A atual postura de segurança da equipe técnica não é fruto do acaso, mas resultado de um processo evolutivo de testes e validações de mercado. Previamente à consolidação do cenário atual, a DTI realizou a prospecção e homologação técnica de diversas soluções de gerenciamento de segredos, incluindo LastPass, KeePassXC e outras alternativas que oferecessem modalidades Open Source ou capacidade de auto-hospedagem (self-hosted). Nesta avaliação empírica, a solução Bitwarden apresentou a melhor aderência aos requisitos de interoperabilidade e segurança, sendo adotada como padrão técnico de facto pela equipe.

2.3 Diagnóstico de Risco e Precarização do Ambiente Não obstante a excelência técnica da ferramenta escolhida, sua utilização atual carece de amparo contratual, resultando em um ambiente misto e não institucionalizado, caracterizado pelas seguintes fragilidades:

- **Limitação da Versão Gratuita:** Parte dos servidores utiliza a versão Free, que, embora segura no armazenamento, não oferece recursos corporativos mandatórios para a Administração Pública, como trilhas de auditoria (logs) imutáveis, gestão centralizada de políticas de segurança e revogação instantânea de acesso (kill switch) em caso de desligamento ou exoneração.
- **Financiamento Privado de Ferramenta Pública:** A parcela de servidores que necessita de recursos avançados (como compartilhamento seguro de credenciais de infraestrutura) utiliza a versão Enterprise custeada com recursos próprios (Pessoa Física).
- **Investimento Pessoal em Hardware Crítico (FIDO2):** Agravando o cenário de anomalia administrativa, os servidores detentores dos níveis mais altos de privilégio (Acesso Root/Admin), visando blindar o acesso aos sistemas estruturantes do IFSP contra ataques de phishing e captura de credenciais, adquiriram, também com verba pessoal, chaves de segurança físicas (Hardware Tokens) compatíveis com o padrão FIDO2 /WebAuthn.

Configura-se, portanto, uma situação onde a segurança de dados do Estado e a blindagem contra acessos não autorizados dependem do financiamento voluntário e privado de seus agentes públicos. Tal modelo é insustentável a longo prazo, fere o princípio da impessoalidade e expõe a instituição ao risco de perda de acesso (lock-in pessoal) e descontinuidade operacional. A contratação visa, portanto, assumir a titularidade institucional dessas ferramentas (Software e Métodos de Autenticação), regularizando o passivo administrativo e elevando o nível de maturidade da segurança da informação.

2.4 O Problema da Soberania dos Dados Esta situação cria um grave risco de continuidade de negócio e soberania de dados. Como as contas atuais são vinculadas a e-mails pessoais ou geridas individualmente (Shadow IT), o IFSP não detém a titularidade efetiva do cofre de senhas. Se um servidor se desligar ou ficar indisponível, a Instituição pode perder o acesso a credenciais críticas armazenadas em cofres privados. Além disso, a falta de uma conta institucional (Enterprise/Corporativa) impede a aplicação forçada de políticas de segurança, como a exigência de Segundo Fator de Autenticação (2FA) e a conformidade plena com a LGPD.

2.5 A Solução Proposta Diante da previsão de expansão (13 novos campi) e da migração para nuvem, torna-se imperativo institucionalizar e regularizar o uso da ferramenta de gestão de senhas. A contratação visa migrar o cenário atual (contas dispersas e custeadas por PF) para uma solução corporativa centralizada, garantindo que as credenciais pertençam ao CNPJ do IFSP, e não ao CPF dos servidores. A aquisição de licenças Enterprise permitirá o

controle centralizado, auditoria forense de acessos e a padronização do ambiente de segurança para a equipe de TI, aproveitando a curva de aprendizado já consolidada e evitando custos de migração ou treinamento com novas ferramentas.

Esta contratação representa uma oportunidade estratégica para consolidar os protocolos de segurança voltados para o User Authentication Framework (UAF), alinhando-se às diretrizes do Plano de Desenvolvimento Institucional (PDI) 2024-2028 do IFSP. A implementação de um sistema de gerenciamento centralizado de senhas será fundamental para suportar o crescimento institucional planejado, garantir a conformidade regulatória e fortalecer significativamente a postura de segurança da informação da instituição. A solução proposta permitirá o controle centralizado e auditável de credenciais para 50 usuários, com capacidade de expansão conforme o crescimento da instituição, estabelecendo uma base sólida para a gestão segura de acessos em todos os campi e sistemas do IFSP.

2.6 Alinhamento Estratégico A contratação está diretamente alinhada aos seguintes objetivos estratégicos do PDI 2024-2028:

Objetivos Estratégicos Institucionais:

- N3 OEI 3: fortalecer a imagem do IFSP;
- N5 OEI 5: aperfeiçoar os sistemas informatizados e a governança do IFSP;
- N6 OEI 6: promover melhores condições de trabalho e qualidade de vida para os servidores; e
- N8 OEI 8: fortalecer a sustentabilidade ambiental e social nas ações institucionais.

Objetivos Estratégicos Específicos da Área de TI:

- M1 OE1: ampliar, padronizar e inovar a oferta de soluções e infraestrutura de TI;
- M3 OE3: aperfeiçoar continuamente a governança e gestão de TI; e
- M4 OE4: reforçar a gestão de riscos em TI e a segurança das informações da instituição e de seus usuários.

2.7 Benefícios Esperados A implementação do sistema de gerenciamento centralizado de senhas proporcionará os seguintes benefícios mensuráveis:

Benefícios de Segurança:

- Fortalecimento da segurança da informação através de controles robustos de acesso com criptografia de conhecimento zero e autenticação multifator;
- Redução significativa dos riscos de vazamento de dados e acessos não autorizados; e
- Eliminação de incidentes relacionados ao uso de senhas fracas ou reutilizadas.

Benefícios de Conformidade:

- Garantia do cumprimento integral das exigências da LGPD na gestão de dados pessoais;
- Implementação de trilhas de auditoria detalhadas para todos os acessos realizados; e
- Conformidade de 100% com os requisitos legais nos processos de gestão de credenciais.

Benefícios Operacionais:

- Aumento significativo na eficiência operacional através da centralização do gerenciamento de credenciais;
- Eliminação de retrabalhos e otimização dos processos de controle de acesso;
- Redução do tempo de resposta para controle de acessos aos sistemas críticos; e
- Melhoria das condições de trabalho dos servidores com simplificação dos processos de acesso.
- Aproveitamento do know-how técnico da equipe que já opera a solução, zerando custos de treinamento e tempo de adaptação (curva de aprendizado nula);
- Facilidade na migração dos cofres atuais (pessoais) para a conta corporativa (exportação/importação compatível).

Benefícios de Governança e Soberania de dados:

- Estabelecimento de controles centralizados que facilitam a auditoria e o monitoramento;
- Melhoria na governança de TI com gestão mais eficaz dos riscos relacionados ao acesso a sistemas críticos; e

- Capacidade de suporte ao crescimento institucional e à migração para nuvem mantendo padrões adequados de segurança.
- Transferência da titularidade das credenciais para a instituição (IFSP), eliminando o risco de retenção de acessos em contas pessoais;
- Regularização do uso da ferramenta, eliminando o custeio de licenças por parte dos servidores (compliance administrativo).
- Capacidade de revogação imediata de acessos em caso de exoneração ou mudança de lotação.

2.8 Riscos da Não Contratação A ausência desta solução expõe o IFSP aos seguintes riscos críticos:

Riscos Regulatórios e Legais:

- Não conformidade com a LGPD, podendo resultar em sanções legais e multas significativas;
- Responsabilização civil e criminal de gestores por negligência na proteção de dados institucionais; e
- Descumprimento de normas de segurança da informação aplicáveis à administração pública.

Riscos Operacionais:

- Perda ou comprometimento de dados críticos dos servidores e da instituição;
- Interrupção de serviços críticos essenciais, causando paralisação de atividades acadêmicas e administrativas; e
- Custos elevados para investigação forense, recuperação de sistemas e implementação de medidas corretivas emergenciais.

Riscos de Imagem e Reputação:

- Quebra de confiança institucional perante a comunidade acadêmica e a sociedade;
- Exposição negativa na mídia decorrente de incidentes de segurança da informação; e
- Comprometimento da credibilidade do IFSP como instituição de ensino superior pública.

Riscos de Segurança:

- Vazamento de informações pessoais e institucionais sensíveis;
- Aumento exponencial da vulnerabilidade a ataques cibernéticos; e
- Impossibilidade de rastreamento e auditoria de acessos não autorizados.

2.9 Valor a Ser Entregue

A contratação do sistema de gerenciamento centralizado de senhas entregará valor estratégico ao IFSP através da criação de um ambiente tecnológico seguro, auditável e em conformidade com as exigências legais. Esta solução será o elemento integrador das iniciativas de infraestrutura física, ampliação de serviços em nuvem e modernização tecnológica, garantindo que todos os recursos implantados estejam protegidos por um gerenciamento seguro e centralizado de credenciais. O sistema proporcionará controle granular de acessos, visibilidade completa das atividades dos usuários, e capacidade de resposta rápida a incidentes de segurança, estabelecendo uma base sólida para o crescimento sustentável da instituição e o cumprimento de sua missão educacional com excelência e segurança.

2.9.1 Consolidação do Cenário Institucional e Métricas

Conforme ilustrado no diagrama a seguir, a fundamentação para esta aquisição não é isolada, mas sim o resultado da convergência de quatro vetores estratégicos críticos que pressionam a infraestrutura de TI do IFSP. O **Cenário Institucional** atual exige uma resposta imediata para sustentar:

- **Expansão Estratégica e Migração Tecnológica:** A ferramenta é pré-requisito para garantir a governança de credenciais durante o planejamento dos **13 novos campi** e a transição da infraestrutura para um ambiente **100% em nuvem**.
- **Segurança e Conformidade:** Há uma necessidade urgente de reverter a gestão descentralizada (Situação Atual) e assegurar o **Compliance com a LGPD** na proteção de dados pessoais.

Em termos quantitativos, o projeto está dimensionado para atender **até 50 usuários** com privilégios administrativos, cobrindo integralmente o período de vigência do **PDI 2024-2028**, assegurando que o crescimento institucional previsto ocorra sobre uma base segura de autenticação.



Cenário Institucional

Expansão Estratégica

13 novos campi em planejamento com necessidade de gestão unificada de credenciais

Migração Tecnológica

Transição completa para infraestrutura em nuvem exige controles centralizados

Situação Atual

Gestão descentralizada por servidor cria vulnerabilidades críticas de segurança

Compliance LGPD

Necessidade urgente de conformidade com proteção de dados pessoais

50

Até 50 Usuários

13

Novos Campi

**2024-
2028**

PDI Vigente

100%

Nuvem

3. Área requisitante

Área Requisitante	Responsável
DTI-PRD	Leonardo Menzani Silva

4. Necessidades de Negócio

4.1. Conforme o inciso I do art. 11, da Instrução Normativa SGD/ME nº 1, de 2019, o IFSP identifica como necessidade de negócio primordial garantir a segurança, a gestão eficiente e o compartilhamento controlado das credenciais institucionais e senhas de sistemas críticos, com vistas ao atendimento de aspectos de confidencialidade, integridade e disponibilidade, bem como à conformidade com normativos de proteção de dados pessoais.

4.2. A contratação tem como objetivos de negócio:

- 4.2.1. Adotar um cofre digital seguro e centralizado, permitindo o armazenamento e o gerenciamento de credenciais institucionais e de equipes, mitigando riscos de exposição de senhas ou anotações inseguras em múltiplos ambientes.
- 4.2.2. Facilitar o controle de acesso a sistemas críticos, permitindo o provisionamento, desprovisionamento e compartilhamento seguro entre as equipes de TI, gestores e outros setores relevantes.
- 4.2.3. Aumentar a produtividade e reduzir o tempo e o esforço despendidos com solicitações de redefinição e recuperação de senhas, contribuindo para maior disponibilidade dos serviços.
- 4.2.4. Permitir rápida revogação de acessos em casos de desligamento de colaboradores ou mudança de funções, reduzindo o risco de acessos indevidos ou vazamentos.
- 4.2.5. Atender aos requisitos instituídos pela Lei Geral de Proteção de Dados (LGPD) e demais normativos federais quanto ao armazenamento, integridade e rastreabilidade do uso de credenciais de acesso, bem como a auditoria de atividades relacionadas.
- 4.2.6. A solução deve prover um ambiente seguro, centralizado, auditável e de fácil gestão para credenciais institucionais, com integração com mecanismos de autenticação forte (MFA) e relatórios gerenciais de acesso.
- 4.2.7. A solução deve prover padrão de segurança institucional, na mitigação de riscos relacionados à gestão de senhas e no atendimento às boas práticas e exigências regulatórias.

5. Necessidades Tecnológicas

5.1. Conforme o inciso I do art. 11, da IN SGD/ME nº 1, de 2019, as necessidades tecnológicas para a contratação do software de gerenciador de senha, abrange o alinhamento da solução às características, padrões e boas práticas do ambiente computacional do IFSP, buscando garantir desempenho, segurança e escalabilidade.

A solução deve ser aderente aos seguintes requisitos:

5.2. Compatibilidade e Integração: O software deverá ser compatível com os sistemas operacionais utilizados pelo IFSP (Windows, Linux, macOS, Android, iOS) e suportar autenticação integrada aos serviços de diretório institucional (LDAP, SAML e Active Directory).

5.3. Segurança da Informação: É fundamental que toda a comunicação com o serviço adote criptografia de ponta a ponta (TLS 1.2+), armazenamento cifrado das credenciais (*AES-256 ou superior, SHA-256 ou superior, RSA para criptografia de chave pública*), autenticação multifatorial (MFA) e controles de acesso detalhados.

5.4. Gestão Centralizada: A solução deverá possibilitar o gerenciamento das contas, permissões e grupos de usuários de forma centralizada, com recursos para auditoria detalhada, geração de relatórios de uso, rastreamento de acessos e integração com Single Sign-On (SSO).

5.5. Padrões de Mercado e Conformidade: O software deverá atender a padrões internacionais de segurança (ISO /IEC 27001, NIST, OWASP) e à legislação de proteção de dados (LGPD). Toda documentação e suporte devem estar disponíveis em português.

5.6. Escalabilidade e Flexibilidade: O software precisa incorporar recursos que viabilizem adição futura de usuários e equipes, adaptação a mudanças nos processos internos, automação de tarefas de provisionamento e atualização contínua do produto.

5.7. Infraestrutura: A solução deve funcionar sem degradação de desempenho nos ambientes atuais de rede, suportando acessos web, aplicativos móveis e extensões de navegador, inclusive em ambientes restritos por firewall.

5.8. Boas Práticas: Devem ser seguidas práticas consolidadas de administração de senhas, com políticas customizáveis de complexidade, rotação de senhas e validação contra banco de dados de senhas vazadas.

5.9. Competências e Suporte Técnico: Deve ser diretamente apoiada tanto pela equipe de TIC interna quanto por suporte oficial do fornecedor, assegurando capacitação operacional e atualizações regulares.

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

6.1. A escolha da solução de software de gerenciamento de senhas envolve a observância de requisitos funcionais, não funcionais e externos imprescindíveis ao atendimento pleno da necessidade do IFSP, bem como à economicidade da contratação.

6.1.1. Requisitos Internos Funcionais

6.1.1.1. Cadastro, armazenamento seguro, compartilhamento controlado e auditoria de senhas, notas seguras e outros dados sensíveis para uso institucional.

6.1.1.2. Suporte a diferentes tipos de credenciais (senhas únicas, senhas rotativas, chaves de acesso a sistemas, tokens OTP, entre outros).

6.1.1.3. Criação de grupos/equipes para organização dos acessos, com possibilidade de delegação e fluxos de aprovação.

6.1.1.4. Disponibilização de relatórios gerenciais para o acompanhamento de uso, eventuais tentativas de acesso indevido e monitoramento de senhas fracas ou expostas.

6.1.2. Requisitos Internos Não Funcionais

6.1.2.1. Garantia de disponibilidade do serviço com acesso multiplataforma (web, mobile, desktop) e compatibilidade com políticas de firewall/rede do IFSP.

6.1.2.2. Se aplicável Interface intuitiva, responsiva, com acessibilidade para pessoas com deficiência conforme WCAG 2.1.

6.1.2.3. Conformidade com os padrões de segurança do IFSP: criptografia de dados, autenticação multifatorial, gestão de logs, backups diários, e controle rígido de permissões.

6.1.2.4. Integração com diretórios corporativos (LDAP/SAML/Active Directory) e soluções de Single Sign-On (SSO).

6.1.2.5. Suporte técnico e documental em português, com atualizações regulares sem impacto operacional.

6.1.3. Requisitos Externos

6.1.3.1. Atendimento integral à LGPD (Lei 13.709/2018) e à legislação vigente sobre proteção de dados em ambiente institucional.

6.1.3.2. Cumprimento dos padrões de TIC do Governo Federal, notadamente os elencados na IN SGD/ME nº 1/2019 e demais normativas sobre segurança da informação.

6.1.3.3. Conformidade com normas técnicas internacionais relevantes (ISO/IEC 27001, ISO/IEC 27002, NIST, OWASP).

7. Estimativa da demanda - quantidade de bens e serviços

Distribuição de Servidores por Área - DTI

Tabela de Alocação de Recursos Humanos

Quantidade	Área/Departamento	Descrição Completa
9	CDSE-DTI	Coordenação de Desenvolvimento de Sistemas Educacionais
7	CDSA-DTI	Coordenação de Desenvolvimento de Sistemas Administrativos
7	CSTI-DTI	Coordenação de Suporte Técnico em Informática
3	CCETI-DTI	Coordenação de Contratos Estratégicos de TI
2	CAOTI-DTI	Coordenação de Arquitetura e Operações de TI
1	CASC-DTI	Coordenação de Arquitetura e Segurança Cibernética
1	CGTI-DTI	Coordenação de Governança de TI
1	DADSI-DTI	Diretoria Adjunta de Desenvolvimento de Sistemas
1	DSI-DTI	Diretoria de Sistemas de Informação
7	Concurso	Vagas que serão providas pelo concurso.
1	DTI-PRD	Diretoria de Tecnologia da Informação - Produção
40	TOTAL GERAL	Total de Servidores Alocados

Distribuição por Categoria

Coordenações (7 áreas): 30 servidores (75%)

- Desenvolvimento de Sistemas: 16 servidores (40%)
- Suporte Técnico: 7 servidores (17,5%)
- Contratos Estratégicos: 3 servidores (7,5%)
- Arquitetura e Operações: 2 servidores (5%)
- Arquitetura e Segurança: 1 servidor (2,5%)
- Governança: 1 servidor (2,5%)

Diretorias (3 áreas): 3 servidores (7,5%)

- Desenvolvimento, Sistemas e Produção: 3 servidores

Provimento por Concurso(previsto): 7 servidores (17,5%)

Justificativa da Divergência de Quantitativos

Identificou-se uma divergência entre o quantitativo apresentado no Documento de Formalização da Demanda (DFD) e os resultados obtidos neste estudo técnico. Esta diferença decorre da ausência de uma análise pormenorizada dos quantitativos no DFD, que apresenta um valor estimativo de 50 licenças.

O presente estudo realizou um levantamento detalhado das necessidades reais, resultando em um quantitativo de **40 licenças** efetivamente necessárias para atender às demandas identificadas, conforme demonstrado na tabela acima.

Estratégia de Contratação

Para esta contratação, adotaremos o quantitativo de **40 licenças**, baseado na análise técnica detalhada realizada. Como medida preventiva para eventuais necessidades adicionais que possam surgir durante a execução contratual, estabeleceu-se a possibilidade de majoração do contrato em até **25%**, conforme previsto na legislação vigente.

Esta abordagem garante:

- Eficiência na aplicação dos recursos públicos
- Flexibilidade para atender demandas imprevistas
- Adequação às necessidades reais identificadas no estudo técnico
- Conformidade com os princípios da economicidade e razoabilidade

8. Levantamento de soluções

O mercado disponibiliza uma ampla variedade de ferramentas gratuitas e comerciais. Para o levantamento de soluções de gerenciamento de senhas, adotou-se uma abordagem que combinou a revisão de literatura com uma pesquisa interna, informal, junto à equipe de Tecnologia da Informação.

Utilizou-se do artigo *“Proteção e segurança para o idoso no meio da tecnologia da informação”*, de Souza, A. B. (2020). **Embora centrado na vulnerabilidade digital de pessoas idosas, o estudo traz reflexões pertinentes ao contexto institucional.** A fragilidade no ambiente digital, apontada pela pesquisa, pode ser associada também à realidade do Instituto Federal, que conta com cerca de 5 mil servidores em uma ampla faixa etária, abrangendo desde jovens até idosos. Essa diversidade de perfis reforça a necessidade de soluções robustas, capazes de assegurar a proteção de todos os usuários.

O artigo discute produtos relevantes para a segurança digital, entre os quais se destacam:

- Authy ou Authenticator: Ferramentas de autenticação de dois fatores, essenciais para adicionar uma camada extra de segurança ao acesso a contas. O Authenticator, em particular, gera códigos aleatórios, mitigando significativamente o risco de ataques virtuais.
- Bitwarden: Descrito como um cofre e gerador de senhas multiplataforma (desktop, navegadores e dispositivos móveis). O artigo ressalta o Bitwarden por ser um serviço gratuito e de código aberto, de fácil utilização e com elevado poder de proteção. É apresentado como uma ferramenta capaz de criar senhas fortes e verificar se credenciais já foram comprometidas ou vazaram em incidentes de segurança.

Diante dessa análise, o Bitwarden foi definido como base de referência para o estudo, considerando tanto sua versão gratuita quanto a empresarial. A escolha não foi arbitrária; uma pesquisa informal interna com os servidores da área de TI revelou um dado interessante: a totalidade dos profissionais que utilizam ferramentas de gerenciamento de senhas em seu dia a dia já emprega espontaneamente a versão gratuita do Bitwarden. Este cenário representa uma vantagem estratégica, ao demonstrar um conhecimento prático (know-how) já consolidado e disseminado entre a equipe de TI. Ter um produto já familiar e utilizado por nossos servidores de TI, facilita enormemente os processos de implementação, suporte e, crucialmente, a disseminação e adoção da ferramenta por toda a comunidade do IFSP. A existência de um produto homologado e ativamente utilizado pela equipe de TI, independentemente de ser gratuito ou não, simplifica a sua divulgação e aprimora as políticas de segurança da informação em toda a instituição. A familiaridade pré-existente com o Bitwarden garante uma transição mais suave, menor curva de aprendizado e maior engajamento dos usuários, fortalecendo a postura de segurança digital do Instituto Federal. Portanto, foram consideradas as soluções abaixo:

Solução 1: Aquisição de software de gerenciamento de senhas e acesso a sistemas. Marca Bitwarden - Produto: Empresa - Pago.

Solução 2: Softwares gratuitos individual - Marca Bitwarden - Produto: individual - Gratuito.

Solução 3: Cada servidor individualmente gerencia a sua maneira as suas senhas.

9. Análise comparativa de soluções

ANÁLISE COMPARATIVA DE SOLUÇÕES:				
Requisito	Solução	Sim	Não	Não se aplica
A solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	x		
	Solução 2	x		
	Solução 3	x		
A solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1		x	
	Solução 2	x		
	Solução 3			x
A solução é aderente às políticas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1		x	
	Solução 2		x	
	Solução 3			x
A solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1		x	
	Solução 2		x	
	Solução 3		x	
A solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1		x	
	Solução 2		x	
	Solução 3		x	

Categoria	Critério	Descrição	Solução 1: software de gerenciamento de senhas e acesso a sistemas. Marca Bitwarden - Produto: Empresa - Pago	Solução 2: Softwares gratuitos individual - Marca Bitwarden - Produto: individual - Gratuito	Solução 3: Cada servidor individualmente gerencia a sua maneira as suas senhas.
	Escalabilidade	Capacidade da solução de crescer sem comprometer desempenho.	atende	não atende - os recursos são limitados	não atende - por se tratar de uma solução individual não escalável.
	Interoperabilidade	Funcionar com outros sistemas sem adaptações especiais.	atende	não atende	não atende

Tecnológicos	Flexibilidade	Facilidade de modificação /expansão para novas necessidades.	atende	não atende	não atende
	Inovação	Incorporação de novas tecnologias e práticas.	atende parcialmente	não mensuravel	não mensuravel
	Resiliência	Recuperação rápida de falhas, garantindo continuidade.	atende	não mensuravel	não atende
	Padronização	Aderência a padrões oficiais, facilitando manutenção.	atende	atende	não atende
	Compatibilidade Infraestrutura	Funcionamento sem exigir adaptações custosas.	atende	atende	não atende
Gestão de Riscos	Gestão de Riscos	Avaliação de riscos de segurança, operação e conformidade.	atende	não atende	não atende
	Governança de Dados	Controles de acesso, segregação de funções, auditoria.	atende	não atende	não atende
	Aderência EGD / Gov. Digital	Compatibilidade com padrões e diretrizes da Estratégia de Governo Digital.	atende	atende	não atende
	Vendor lock-in / Portabilidade	Nível de dependência do fornecedor e facilidade de migração de dados.	atende	atende	não atende
	Monitoramento e Indicadores	Disponibilidade de SLAs e KPIs claros de desempenho.	atende	não atende	não atende
	Suporte e Manutenção	Qualidade e disponibilidade de suporte técnico.	atende	não atende	não mensurável
	Experiência do Usuário	Interface intuitiva, facilidade de uso e satisfação.	atende	não mensurável	não mensurável

Negócios	Treinamento	Necessidade de treinamento formal para operação.	atende	não mensurável	não mensurável
	Custos de Treinamento	Custos adicionais de capacitação (instrutor, materiais).	não aplica	não aplica	não mensurável
	Tempo de Implementação	Período necessário para disponibilização da solução.	atende	não mensurável	não mensurável
	Custo Total de Propriedade (TCO)	Custos de aquisição, implantação, operação e manutenção.	alto	baixo	baixo
	Economicidade	Uso racional dos recursos financeiros.	atende	atende	atende
	Eficácia	Alcance dos resultados esperados.	atende	não atende - não permite gestão centralizada de equipes	não atende - não permite gestão centralizada de equipes
	Eficiência	Alcançar resultados com menor uso de recursos.	atende	não atende - não permite gestão centralizada de equipes	não atende - não permite gestão centralizada de equipes
	Efetividade	Impacto real em resolver problemas e gerar valor.	atende	não atende - não permite gestão centralizada de equipes	não atende - não permite gestão centralizada de equipes
Legais	Conformidade (LGPD e normas)	Aderência às normas legais aplicáveis.	atende	atende	não mensurável
	Auditoria Independente	Possibilidade de auditoria externa da solução.	atende	não atende - não permite gestão centralizada de equipes	não atende - não permite gestão centralizada de equipes
	Gestão de Logs e Auditoria	Geração de registros seguros e auditáveis.	atende	não atende - não permite gestão centralizada de equipes	não atende - não permite gestão centralizada de equipes
				não atende	

	Segurança da Informação	Proteção contra acessos não autorizados e vulnerabilidades.	atende	- não permite gestão centralizada de equipes	não atende - não permite gestão centralizada de equipes
	Backup e Recuperação de Dados	Políticas claras de backup e recuperação.	atende	atende	não mensurável
Sociais, Ambientais e Acessibilidade	Sustentabilidade	Redução de impactos ambientais e sociais.	atende	atende	não mensurável
	Certificações Ambientais	Possui ISO 14001, EPEAT ou equivalentes.	não aplica	não aplica	não aplica
	Acessibilidade Digital	Conformidade com padrões eMAG/WCAG.	atende	atende	não mensurável

]



Análise Comparativa de Soluções

Gerenciamento de Senhas e Acesso a Sistemas

Bitwarden Enterprise

Solução Completa

92%

Atende 23 de 25 critérios avaliados

Bitwarden Individual

Limitações Críticas

48%

Falha em gestão centralizada e auditoria

Gestão Individual

Inadequada

28%

Não escalável e sem padronização

• Vantagens do Bitwarden Enterprise

- ✓ **Gestão Centralizada:** Controle total sobre equipes e políticas
- ✓ **Escalabilidade:** Cresce conforme a organização sem perder performance
- ✓ **Interoperabilidade:** Integra com sistemas existentes sem adaptações
- ✓ **Auditoria Completa:** Logs detalhados e trilhas de auditoria
- ✓ **Conformidade Legal:** Atende LGPD e normas de segurança
- ✓ **Suporte Profissional:** Assistência técnica especializada 24/7
- ✓ **Backup Seguro:** Políticas robustas de recuperação de dados
- ✓ **Flexibilidade:** Adapta-se facilmente a novas necessidades

• Limitações das Alternativas

- ✗ **Sem Gestão de Equipes:** Impossibilita controle centralizado
- ✗ **Auditoria Limitada:** Não gera logs adequados para compliance
- ✗ **Escalabilidade Zero:** Não cresce com a organização
- ✗ **Suporte Inexistente:** Sem assistência profissional
- ✗ **Riscos de Segurança:** Gestão descentralizada aumenta vulnerabilidades
- ✗ **Falta de Padronização:** Cada servidor com regras próprias
- ✗ **Conformidade Duvidosa:** Dificuldade em atender requisitos legais
- ✗ **Eficiência Baixa:** Múltiplos pontos de gestão geram retrabalho

Critério	Bitwarden Enterprise	Bitwarden Individual	Gestão Individual
Gestão Centralizada de Equipes	✓ Atende	✗ Não Atende	✗ Não Atende
Escalabilidade	✓ Atende	✗ Recursos Limitados	✗ Não Escalável
Auditoria e Compliance	✓ Atende	✗ Sem Gestão Central	✗ Sem Gestão Central
Interoperabilidade	✓ Atende	✗ Não Atende	✗ Não Atende
Gestão de Riscos	✓ Atende	✗ Não Atende	✗ Não Atende
Suporte Técnico	✓ Profissional	✗ Limitado	? Não Mensurável

Recomendação

A solução recomendada é o Bitwarden Enterprise. Este sistema atende aos requisitos de gestão centralizada, auditoria completa, escalabilidade e conformidade legal, representando o melhor custo-benefício em termos de segurança e eficiência operacional.

10. Registro de soluções consideradas inviáveis

Em atendimento ao § 1º do art. 11 da IN SGD/ME nº 1/2019, este Estudo Técnico Preliminar registra de forma sucinta as soluções de gerenciamento de senhas avaliadas e consideradas inviáveis para a necessidade do IFSP, apresentando breve descrição e justificativa para descarte, dispensando-se a apuração detalhada do custo total de propriedade (TCO).

Solução 2: Softwares gratuitos individuais - Bitwarden (uso pessoal e não gerenciado)

- **Descrição:** Utilização da versão gratuita do Bitwarden por cada servidor, de modo individual e sem centralização, gerenciamento unificado, suporte institucional ou recursos de governança e auditoria.
- **Justificativa da inviabilidade:** esta solução não atende aos requisitos de escalabilidade, interoperabilidade, flexibilidade e resiliência necessários para o ambiente institucional. Sua natureza individual impossibilita a gestão centralizada de credenciais, limita recursos de auditoria, não provê controle ou delegação de acessos, e não permite integração com diretórios, SSO, ou outros sistemas institucionais, conforme verificado na comparação de requisitos técnicos e de negócios. Além disso, não oferece suporte técnico especializado, dificultando a adoção institucional segura e o suporte ao crescimento projetado do IFSP.

Solução 3: Gestão individualizada de senhas por cada servidor, sem ferramenta padronizada

- **Descrição:** Permite que cada servidor administre e armazene suas próprias senhas e credenciais da maneira que julgar conveniente, sem orientação centralizada, aplicação de boas práticas institucionais ou utilização de soluções tecnológicas específicas.
- **Justificativa da inviabilidade:** esta abordagem é considerada inadequada para a realidade do IFSP, pois não atende aos critérios mínimos de segurança da informação, governança, rastreabilidade e gerenciamento de riscos exigidos por normas federais e pelo contexto de proteção de dados sensíveis. Não permite auditoria, nem a mitigação de incidentes associados ao uso de senhas fracas, vazadas ou compartilhadas indevidamente. Tal cenário acarreta risco elevado de não conformidade à LGPD, comprometimento de dados institucionais, falhas operacionais e exposição institucional a sanções legais, como evidenciado nos itens de análise.

Portanto, ambas as soluções supracitadas foram descartadas deste processo por não atenderem de maneira suficiente e eficaz aos padrões tecnológicos, regulatórios e de governança exigidos pela administração pública e pela estratégia institucional do IFSP.

11. Análise comparativa de custos (TCO)

Itens que compõem os custos das soluções:

Id	Solução Viável 1: Aquisição de software de gerenciamento de senhas e acesso a sistemas. Marca Bitwarden - Produto: Empresa - Pago.		Valor
1	Custo inicial de aquisição;		
	Valor Unitário em Dólar Americano: Cotação do dólar 19/08/2025 - 14:37 Fonte: Banco Central https://www.bcb.gov.br/estabilidadefinanceira/fechamentodolar		US\$ 6,00
	Valor Unitário em Real		R\$ 32,83
	Quantidade		40
	Total mês		R\$ 1.313,18

Total ano	R \$ 15.758,21

ID	Solução Viavel 2: Softwares gratuitos individual - Marca Bitwarden - Produto: individual - Gratuito	Valor
2	Custo inicial de aquisição;	R\$ 0,00
	Total ano	R\$ 0,00

ID	Solução Viavel 3: Cada servidor individualmente gerencia a sua maneira as suas senhas.	Valor
3	Custo inicial de aquisição;	R\$ 0,00
	Total ano	R\$ 0,00

Projeção de Custos para Implementação do Bitwarden (10 Anos)

Solução Viavel 1: Aquisição de software de gerenciamento de senhas e acesso a sistemas. Marca Bitwarden - Produto: Empresa - Pago											
Componentes de custo											
Reajuste Cambial Dólar Americano	5,4716										
Ano	1	2	3	4	5	6	7	8	9	10	Total
Valor anual em Reais	R\$ 15.758,21	15758,208	15758,208	15758,208	15758,208	15758,208	15758,208	15758,208	15758,208	15758,208	R\$ 157.582,08

12. Descrição da solução de TIC a ser contratada

A solução de TIC a ser contratada consiste na aquisição de licenciamento do Bitwarden Enterprise, software de gerenciamento centralizado de senhas, destinado à equipe da Diretoria de Tecnologia da Informação (DTI) e áreas correlatas do IFSP. O principal objetivo é promover a gestão centralizada, segura, eficiente e auditável das credenciais institucionais, substituindo práticas individuais dispersas e aumentando o nível de segurança em todos os ambientes críticos.

O Bitwarden Enterprise será utilizado como cofre digital corporativo, permitindo controle total das credenciais de acesso a sistemas institucionais sob responsabilidade da equipe de TIC. A solução proporciona recursos robustos de gerenciamento de senhas, chaves de acesso, tokens OTP e notas seguras, todos armazenados de forma criptografada, com autenticação multifatorial e trilhas completas de auditoria. O sistema viabiliza administração de grupos, permissões, fluxos de aprovação, integração com diretórios institucionais (LDAP, SAML, Active Directory) e provisionamento/desprovisionamento ágil conforme mudanças na equipe.

A solução atende aos critérios de segurança da informação, conformidade regulatória (LGPD e normas federais), escalabilidade e integração multiplataforma, com funcionamento garantido em Windows, Linux, macOS, Android, iOS, navegadores e dispositivos móveis. Garante-se, assim, proteção contra acessos não autorizados, vazamento de senhas e dificuldades no rastreamento de operações críticas.

Devido à ampla utilização da versão gratuita do Bitwarden pelos servidores da DTI em atividades pessoais, não é necessário treinamento formal para adoção do sistema corporativo. O conhecimento prévio da ferramenta entre os principais usuários elimina a curva de aprendizagem, garantindo rápida adesão e eficácia no uso desde o início da operação.

A contratação abrange 40 licenças do Bitwarden Enterprise, com possibilidade de expansão conforme as necessidades institucionais. Inclui atualizações regulares, suporte especializado do fornecedor e todos os recursos premium voltados à segurança, automação e governança.

Com a contratação, o IFSP assegura uma solução centralizada, moderna, de rápida implantação e totalmente aderente aos padrões atuais de segurança digital do setor público federal.

13. Estimativa de custo total da contratação

Valor (R\$): 15.758,21

ITEM	ESPECIFICAÇÃO	CATSER	MÉTRICA OU UNIDADE DE MEDIDA	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	Licenciamento de Software Bitwarden Enterprise	26077	Unidade	40	R\$ 32,83 Mensal	R\$ 15.758,21 Anual

O não parcelamento é justificado pela inviabilidade técnica e econômica, considerando a natureza indivisível do objeto, necessidade de padronização, aumento de custos administrativos e risco de comprometimento da execução, conforme art. 23, §1º da Lei 14.133/21.

14. Justificativa técnica da escolha da solução

A escolha pelo licenciamento do Bitwarden Enterprise como solução de gerenciamento centralizado de senhas para o IFSP foi motivada por uma análise técnica detalhada, que considerou múltiplos aspectos qualitativos e a avaliação comparativa das alternativas disponíveis.

A tabela de análise comparativa (item 9) evidenciou que o Bitwarden Enterprise (solução 1) é a única opção capaz de atender plenamente aos requisitos institucionais de escalabilidade, interoperabilidade, gerenciamento centralizado, auditabilidade e adequação aos padrões de segurança exigidos pelo IFSP e pela legislação vigente. Dentre os principais fatores técnicos que fundamentaram a decisão destacam-se:

- **Gestão centralizada:** O Bitwarden Enterprise permite o controle unificado de credenciais por equipes, definição granular de perfis e permissões, e provisionamento/desprovisionamento imediato, reduzindo o risco de acessos indevidos após alterações de equipe.
- **Recursos avançados de segurança:** Oferece criptografia de ponta a ponta, autenticação multifatorial, auditoria de acessos detalhada, geração de relatórios gerenciais e integração nativa com diretórios institucionais (LDAP, SAML, Active Directory), além de suportar práticas robustas de rotação e complexidade de senhas.
- **Aderência regulatória e técnica:** A solução satisfaz integralmente os requisitos da LGPD, e padrões do IFSP, garantindo conformidade legal e proteção de dados pessoais e institucionais.
- **Escalabilidade e flexibilidade:** Bitwarden Enterprise pode ser expandido para incluir novos usuários e atender a eventuais mudanças organizacionais sem impactar o desempenho ou comprometer a segurança, o que é fundamental diante da abertura de novos campi e ampliação do uso institucional.
- **Compatibilidade e integração:** funciona em todos os sistemas operacionais e plataformas utilizados no IFSP (Windows, Linux, macOS, Android, iOS, navegadores), sem necessidade de infraestrutura adicional ou adaptações dispendiosas.

- **Eficiência operacional e rápida adoção:** Como a equipe de TIC já utiliza a versão gratuita da ferramenta em âmbito pessoal, a migração para o ambiente corporativo será natural, dispensando treinamentos formais, minimizando riscos de resistência e acelerando a produtividade.
- **Governança e rastreabilidade:** A gestão centralizada e a capacidade de geração de trilhas de auditoria permitem a rápida detecção, investigação e resposta a incidentes de segurança, contribuindo para a governança de TI e mitigação de riscos operacionais e regulatórios.

Consideração dos riscos: as alternativas descartadas (uso de software gratuito individualizado e gestão descentralizada) representam riscos críticos à segurança, governança e conformidade, pois não oferecem mecanismos para controle institucional, segregação adequada de acessos, auditoria confiável, nem atendimento à LGPD—expondo a instituição a vulnerabilidades, sanções e danos à reputação.

Relação com os benefícios esperados: A adoção do Bitwarden Enterprise está diretamente vinculada aos benefícios estratégicos mapeados: eleva o nível de segurança da informação, fortalece a postura de governança digital, aumenta a eficiência operacional, simplifica auditorias, reduz custos e riscos de incidentes, e assegura alinhamento com as práticas de gestão de credenciais no setor público. Trata-se, assim, de uma escolha fundamentada na excelência técnica e na adequação institucional, com impacto imediato e sustentável para o IFSP.

15. Justificativa econômica da escolha da solução

A escolha pela contratação do Bitwarden Enterprise como solução de gerenciamento centralizado de senhas no IFSP está fundamentada não apenas na sua superioridade técnica, mas também na análise criteriosa dos aspectos econômicos, garantindo o cumprimento dos princípios da economicidade, eficiência e racionalização do gasto público.

Custo Total de Propriedade (TCO): Embora o investimento inicial para aquisição das licenças empresariais do Bitwarden seja superior às alternativas baseadas em soluções gratuitas ou gestão individualizada, a avaliação global do custo total de propriedade demonstra que esta opção representa a solução mais vantajosa para a Administração, quando considerados os riscos mitigados, custos indiretos evitados e benefícios agregados à instituição. A proporcionalidade entre custo e valor agregado foi evidenciada nos seguintes pontos:

- **Prevenção de perdas e incidentes:** A gestão centralizada e segura das credenciais reduz significativamente os riscos de vazamento de dados, acessos indevidos e incidentes de segurança, que, se materializados, poderiam gerar prejuízos financeiros, multas legais (decorrentes da LGPD) e custos elevados com respostas emergenciais e investigações forenses.
- **Redução de custos operacionais:** A solução elimina o retrabalho associado a redefinições frequentes de senhas, agiliza o processo de concessão e revogação de acessos, automatiza procedimentos e reduz o tempo de resposta das equipes de TIC, resultando em ganhos de produtividade e economia de horas de trabalho.
- **Dispensa de treinamento formal:** A experiência e familiaridade prévia dos servidores com a versão gratuita do Bitwarden eliminam a necessidade de investimento adicional em capacitação, contribuindo para uma adoção imediata e sem custos extras associados à curva de aprendizagem.
- **Flexibilidade orçamentária:** A possibilidade de majoração contratual, prevista em até 25%, permite que o IFSP adeque dinamicamente o quantitativo de licenças adquiridas, otimizando o uso dos recursos financeiros de acordo com a expansão institucional ou eventuais necessidades temporárias.
- **Custos transparentes e previsíveis:** O modelo de licenciamento anual proporciona clareza para o planejamento orçamentário, evitando despesas imprevistas e alinhando os compromissos financeiros ao ciclo de gestão pública.
- **Valor agregado às práticas de governança:** O Bitwarden Enterprise reforça a conformidade regulatória, atende a padrões federais, agrega valor institucional e potencializa o retorno do investimento aplicado em infraestrutura e segurança da informação.

Esses elementos, consolidados na análise comparativa de soluções, comprovam que a contratação do Bitwarden Enterprise será não apenas tecnicamente adequada, mas, sobretudo, uma escolha financeiramente sustentável, atendendo plenamente aos interesses públicos e estratégicos do IFSP.

16. Benefícios a serem alcançados com a contratação

A contratação do Bitwarden Enterprise para gestão centralizada de senhas proporcionará uma série de benefícios estratégicos, operacionais e institucionais ao IFSP, com impactos positivos tanto para a Administração quanto para a comunidade acadêmica e a sociedade.

Benefícios Diretos às Atividades do IFSP:

- **Fortalecimento da segurança da informação:** adoção de práticas avançadas de proteção de credenciais institucionais, reduzindo drasticamente o risco de vazamento de dados, acessos não autorizados e incidentes de segurança cibernética.
- **Governança e conformidade:** atende integralmente aos requisitos da LGPD e demais normativos federais, assegurando o controle adequado sobre dados pessoais e confidenciais, além de gerar trilhas de auditoria confiáveis para fiscalizações e investigações.
- **Gestão centralizada e eficiente:** simplifica e padroniza o gerenciamento de credenciais entre equipes e sistemas, permitindo controle total de acessos, provisionamento e desprovisionamento rápidos, e mitigação de riscos relacionados a movimentações internas e desligamentos.
- **Melhoria da produtividade:** redução do tempo e do esforço investidos pelas equipes de TIC em processos manuais de redefinição e recuperação de senhas, possibilitando maior foco em iniciativas estratégicas de tecnologia.
- **Facilidade de adoção:** com a equipe já familiarizada com a ferramenta, a implantação é imediata e sem necessidade de treinamento adicional, promovendo eficácia desde o início da operação.

Benefícios Institucionais e para a Sociedade:

- **Reforço à imagem institucional:** consolidando o IFSP como referência em governança digital, proteção de dados e adoção de boas práticas de segurança.
- **Apoio ao crescimento sustentável:** A solução suportará a abertura de novos campi e a migração de serviços para a nuvem, garantindo expansão segura, escalável e alinhada ao Plano de Desenvolvimento Institucional (PDI).
- **Transparência e rastreabilidade:** possibilita o monitoramento detalhado das operações digitais, contribuindo para transparência institucional e proteção do patrimônio informacional.
- **Confiabilidade para a comunidade:** garante a proteção dos dados pessoais de servidores, alunos e parceiros institucionais, fortalecendo a confiança de toda a comunidade acadêmica e administrativa no ambiente tecnológico do IFSP.

Benefícios para Públicos Alvos Relacionados à Contratação:

- **Servidores:** condições mais seguras e práticas de trabalho, com processos de acesso padronizados, menos vulnerabilidades e ambiente digital protegido.
- **Equipe de TIC:** ferramenta robusta, centralizada, confiável e de fácil administração, otimizando rotinas, reduzindo incidentes operacionais e agregando valor ao serviço prestado.
- **Gestores:** parâmetros claros de controle, capacidade de auditoria e visibilidade sobre usos das credenciais, subsidiando decisões e fortalecendo a gestão de riscos.
- **Sociedade e comunidade acadêmica:** segurança, transparência e responsabilidade na administração de dados institucionais, promovendo o interesse público e a reputação positiva da entidade.

Esses resultados, alinhados aos objetivos estratégicos do IFSP, reforçam a relevância e a necessidade da contratação da solução Bitwarden Enterprise, consolidando os avanços tecnológicos e de segurança no ambiente institucional.

17. Providências a serem Adotadas

Para viabilizar a execução contratual e garantir o pleno funcionamento do Bitwarden Enterprise na estrutura do IFSP, algumas providências e adequações deverão ser realizadas pela equipe responsável e demais áreas envolvidas:

- **Formalização da contratação:** realização do procedimento licitatório ou contratação direta (conforme legislação vigente), com especificação detalhada dos requisitos e quantitativos necessários.
- **Orientação sobre boas práticas:** realização de comunicações institucionais e orientação dos usuários cadastrados quanto às normas de utilização, reposição e compartilhamento de credenciais, reforçando padrões de segurança já consolidados.

Cabe destacar que, em razão do conhecimento prévio da ferramenta por parte da equipe de TIC, não haverá necessidade de treinamentos iniciais, o que facilitará a implantação e adesão à solução. Ademais, o ambiente tecnológico atual do IFSP comporta a instalação e operação do Bitwarden Enterprise nas principais plataformas utilizadas institucionalmente.

Dessa forma, as providências elencadas garantirão a adequada preparação e operação do sistema, assegurando todos os benefícios esperados com a contratação.

18. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

18.1. Justificativa da Viabilidade

A solução é viável, pois atende plenamente aos requisitos de segurança, governança e conformidade, sem necessidade de ajustes estruturais.

19. Responsáveis

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

JAILTON SOARES DE ARAUJO

Membro da comissão de contratação



Assinou eletronicamente em 17/12/2025 às 14:40:27.

LUIS AUGUSTO DIAS CESAR

Membro da comissão de contratação



Assinou eletronicamente em 17/12/2025 às 14:41:46.

LUIZ FERNANDO POSTINGEL QUIRINO

Membro da comissão de contratação



Assinou eletronicamente em 17/12/2025 às 14:40:50.

DEIR OLIVEIRA DE OLIVEIRA

Autoridade competente

LEONARDO MENZANI SILVA

Autoridade competente



Assinou eletronicamente em 17/12/2025 às 14:51:43.

Documento Digitalizado Público

Estudo Técnico Retificado e Assinado.

Assunto: Estudo Técnico Retificado e Assinado.
Assinado por: Jailton Soares
Tipo do Documento: Estudo Técnico
Situação: Finalizado
Nível de Acesso: Público
Tipo do Conferência: Cópia Simples

Documento assinado eletronicamente por:
■ **Jailton Soares de Araujo, TEC DE TECNOLOGIA DA INFORMACAO**, em 17/12/2025 15:25:11.

Este documento foi armazenado no SUAP em 17/12/2025. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse <https://suap.ifsp.edu.br/verificar-documento-externo/> e forneça os dados abaixo:

Código Verificador: 2284874
Código de Autenticação: 05c69d84ea

