Política de Privacidade

Sistema de Gestão de Projetos Integradores (SGPI)

Data de vigência: xx/xx/xxxx **Última atualização:** 16/10/2025

Este documento explica, de forma direta e com linguagem humana, como o SGPI coleta, usa, protege e descarta os dados das pessoas que interagem com o sistema — coordenadores, professores, orientadores e alunos. O texto está alinhado à Lei Geral de Proteção de Dados (LGPD) e foi pensado para ser fácil de ler.

1. Quais dados são coletados (por perfil)

Coordenador / Professor / Orientador

Nome completo, email institucional, Cargo, foto (opcional), registros de log de atividades, identificação de acesso (login).

Aluno

Nome completo, email institucional, turma, notas, documentos enviados (documentos, apresentações, anexos), foto (opcional), registros de acesso e atividade.

Dados técnicos e não pessoais

Endereço IP, carimbo de data/hora (timestamp), tipo de dispositivo e navegador, registros de erro e logs de auditoria.

2. Finalidades detalhadas por tipo de dado

Para manter transparência, listamos abaixo por finalidade o que usamos e por quê:

Gestão acadêmica e administrativa: nome, notas, histórico, documentos — para matrícula, avaliação e comunicações formais.

Comunicação: email institucional — para avisos sobre prazos, reuniões, feedbacks e suporte técnico.

Acompanhamento de projetos: documentos, notas e histórico — para orientar e avaliar o progresso dos projetos integradores.

Segurança e auditoria: logs, IP, timestamps — para detectar e responder a incidentes e proteger o sistema.

Melhoria do sistema: dados agregados e anonimizados — para analisar uso, corrigir bugs e planejar melhorias.

3. Base legal (LGPD) por tipo de tratamento

Indicamos a base legal que justifica cada uso de dados:

Execução de contrato / relação educacional: Dados acadêmicos e pessoais necessários para atividades curriculares, matrículas e comunicação institucional.
Cumprimento de obrigação legal: Armazenamento de históricos e registros quando exigidos por normas educacionais e fiscais.

Legítimo interesse: Logs e metadados para segurança, prevenção de fraudes e melhorias operacionais (avaliado para minimizar impacto aos titulares).

Consentimento: Uso de imagens, envio de comunicações promocionais/eventos opcionais e funcionalidades extras que não são essenciais ao serviço.

4. Onde os dados ficam e como protegemos

Armazenamento:

Os dados ficam em servidores da instituição e/ou provedores de nuvem contratados. Fornecedores autorizados assinam contratos que exigem proteção e confidencialidade.

Medidas de segurança técnicas e organizacionais:

- Criptografia de senhas e dados sensíveis em trânsito e, quando aplicável, em repouso.
- Controle de acesso por perfis, com privilégios mínimos para cada função.
- Backups regulares com testes de restauração.
- Firewalls, monitoramento de logs e análise de eventos de segurança.
- Política de senhas e autenticação (recomendação de MFA quando possível).
- Treinamento periódico da equipe técnica sobre boas práticas e proteção de dados. Procedimento em caso de incidente

Se houver suspeita de violação de dados, a equipe técnica seguirá um plano de resposta: identificar o incidente, conter e mitigar o risco, avaliar o impacto, comunicar os titulares afetados e autoridades quando exigido pela LGPD, e revisar ações para evitar recorrência.

5. Compartilhamento e tratadores (third parties)

- Compartilhamos dados somente quando necessário e com as devidas garantias:

  Internamente: coordenação, professores e setor técnico — acesso restrito e justificado.

- Com provedores de hospedagem e serviços (por exemplo: backup, email transacional) sob contrato que obriga confidencialidade.
- Com autoridades públicas, quando houver ordem judicial ou obrigação legal.

Ao compartilhar com terceiros, exigimos cláusulas contratuais que imponham padrões de segurança compatíveis com a LGPD e limitam o uso dos dados ao serviço contratado.

6. Tempo de retenção e descarte seguro

Prazos e critérios:

Durante o vínculo: Todos os dados necessários para o vínculo acadêmico são mantidos enquanto o usuário estiver ativo na instituição.

Período pós vínculo: Após desligamento ou formatura, os registros acadêmicos e administrativos podem ser mantidos por até 5 anos ou conforme exigência legal.

Exclusão/anonimização: Passado o prazo, os dados pessoais são excluídos de backups e sistemas ou anonimizados para uso estatístico, respeitando procedimentos seguros.

7. Compartilhamento de Dados

Os dados pessoais armazenados no SGPI são acessados e utilizados de forma controlada, respeitando as funções e permissões de cada tipo de usuário no sistema.

O **perfil de gestão** é o responsável por **delegar cargos e atribuições** dentro do sistema, controlando quais usuários (como coordenadores, professores, orientadores e alunos) terão acesso a determinadas informações ou funcionalidades. Essa delegação segue critérios institucionais e visa garantir que cada usuário visualize e manipule apenas os dados necessários para o desempenho de suas atividades acadêmicas e administrativas.

O compartilhamento de dados é restrito ao ambiente interno da instituição, podendo ocorrer apenas entre departamentos diretamente envolvidos na gestão de projetos e atividades acadêmicas. Caso seja necessário o compartilhamento com terceiros (por exemplo, serviços de hospedagem, manutenção ou auditoria do sistema), isso será feito de forma segura e conforme as disposições da LGPD, assegurando que os parceiros adotem medidas de proteção compatíveis com as exigências legais.

Nenhum dado pessoal é comercializado ou divulgado publicamente. Todo acesso e compartilhamento são registrados e monitorados para garantir transparência e segurança.

8. Revisão, aprovação e responsabilidade

Este rascunho deve ser revisado pela coordenação do curso e, preferencialmente, pela assessoria jurídica da instituição. Após ajustes, a coordenação aprovará e publicará a versão final. A equipe técnica do SGPI é responsável pela implementação das medidas técnicas descritas.

9. Implementação prática no sistema

Recomendações para colocar em prática:

- Inserir link visível para a Política no rodapé do sistema e nas páginas de cadastro/login.
- Exigir aceite explícito (checkbox) durante o cadastro, com link direto para a política; registrar data e versão do aceite.
- Exibir aviso de atualização quando política for alterada e solicitar novo aceite quando mudanças afetarem direitos ou uso de dados.
- Implementar formulário ou endpoint interno para receber pedidos de titulares e gerar protocolos automaticamente.

10. Informações de contato do encarregado (DPO) e canal de privacidade

Para dúvidas ou solicitações sobre dados pessoais, entre em contato com o encarregado (DPO) ou canal responsável: **Email:** https://fateczl.cps.sp.gov.br

11. Registro de versões e histórico de alterações

Versão 1.0 — 16/10/2025: Política inicial redigida e formatada para implantação no SGPI.