

ORIENTAÇÃO TÉCNICA N.º 04/2025 - CGD/DTIC/PRODIN

ASSUNTO: Uso de ferramentas de Inteligência Artificial (IA) no âmbito do IFSC, com foco na proteção de dados pessoais e institucionais

Em vista do crescente uso de ferramentas de Inteligência Artificial (IA), para garantir a transparência, a finalidade, a segurança e a integridade no uso de ferramentas públicas, e ainda **considerando**:

- I. A utilização de ferramentas de Inteligência Artificial (IA) como apoio às atividades de ensino, pesquisa, extensão e administração;
- II. A disponibilização, pelo IFSC, de plataformas homologadas (Google e Microsoft), cuja adesão foi validada juridicamente (Ref. Processo SIPAC NUP 23292.028158/2019-57);
- III. A vigência da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD) e a ECA Digital (Lei Nº 15.211, de 17/09/2025);
- IV. A necessidade de consolidar diretrizes para a integridade acadêmica frente às novas tecnologias emergentes das quais não temos controle de acesso público;
- V. Os riscos inerentes ao uso de ferramentas não homologadas ("*Shadow AI*"), especialmente no que tange ao tratamento de dados pessoais para treinamento de modelos externos.

A Coordenadoria de Gestão de Dados (CGD) da Diretoria de Tecnologia da Informação e Comunicação (DTIC), **recomenda fortemente**:

1. Prioridade Institucional e Ferramentas Estratégicas

Servidores e alunos **não devem inserir, copiar ou compartilhar** dados pessoais de qualquer natureza em ferramentas de Inteligência Artificial externas ao pacote Google for Education ou Microsoft A1 Education (mediante autocadastro¹). Isso inclui, mas não se limita a:

- I. Nomes completos, CPFs, matrículas, endereços, e-mails ou telefones de estudantes e servidores.
- II. Dados de saúde: Informações sobre condições médicas, laudos, atestados ou qualquer dado relativo à saúde física ou mental de membros da comunidade acadêmica.
- III. Dados de menores de idade: É expressamente desaconselhado o uso de qualquer dado que possa identificar ou estar relacionado a estudantes menores de idade em plataformas de IA externas, dada a sua condição de vulnerabilidade segundo a legislação vigente.
- IV. Dados acadêmicos ou avaliativos que, em conjunto, possam identificar um indivíduo.
- V. Informações e documentos institucionais de acesso restrito ou uso interno.

¹ <https://ifsc.edu.br/en/web/guest/servicos-de-tecnologia>

1.1. Google for Education (Cadastro automatizado)

- I. Toda a comunidade acadêmica deve buscar priorizar o uso das funcionalidades de Inteligência Artificial disponíveis nas ferramentas do Google for Education (Google Docs, Google Slides, Google Meet, etc.) para a realização de suas atividades. O uso dessas ferramentas, no contexto da conta institucional (@ifsc.edu.br), garante que os dados permaneçam no ambiente controlado pelo contrato entre o IFSC e o Google, minimizando a exposição a serviços de terceiros.
- II. **Priorização de Uso:** A comunidade acadêmica deve priorizar o uso das funcionalidades de IA disponíveis nas ferramentas do Google for Education (Gemini no Docs, Slides, Meet, etc.), utilizando a conta institucional (@ifsc.edu.br).
- III. **Segurança e LGPD (Contratual):** Conforme o contrato vigente e a validação jurídica (Processo SIPAC NUP 23292.028158/2019-20 e COTA n. 00059/2019/PF/IFSC/PGF/AGU), o uso da conta institucional garante que os dados permaneçam no ambiente controlado pelo IFSC, não sendo utilizados para treinamento de modelos de IA do Google sem consentimento.

1.2. Ferramentas Microsoft (Mediante Cadastro Institucional)

- I. **Uso Homologado:** O uso do assistente Copilot e das ferramentas de Inteligência Artificial da Microsoft é permitido no contexto institucional, seguindo as diretrizes de segurança desta Orientação Técnica.
- II. **Priorização de Uso:** A comunidade acadêmica deve priorizar o uso das funcionalidades de IA disponíveis nas ferramentas do Microsoft A1 Education (Office 365, Copilot, etc.), utilizando a conta institucional (@ifsc.edu.br) mediante autocadastro².
- III. **Segurança e LGPD (Contratual):** Conforme o contrato vigente e a validação jurídica (Processo SIPAC NUP 23292.028158/2019-20 e COTA n. 00059/2019/PF/IFSC/PGF/AGU), o uso da conta institucional garante que os dados permaneçam no ambiente controlado pelo IFSC, não sendo utilizados para treinamento de modelos de IA da Microsoft sem consentimento conforme termos de uso referenciados.

2. Regras Críticas de Segurança de Dados

A utilização de dados pessoais para "treinar" modelos de IA de serviços externos representa um risco significativo. Uma vez fornecidos, esses dados podem ser armazenados indefinidamente, utilizados para fins diversos e até mesmo compartilhados com outras organizações sem o consentimento do titular. Isso viola a privacidade do indivíduo e pode expor o IFSC a questões legais no âmbito da LGPD.

2.1. Evitar de forma absoluta:

O maior risco regulatório reside no uso de Sistemas de IA de “uso particular” (ferramentas não geridas pelo IFSC). É **expressamente não recomendado** inserir:

- I. **Dados Pessoais Sensíveis** ou não anonimizados de qualquer membro da comunidade (alunos, servidores, terceiros).
- II. **Dados Institucionais Confidenciais** (informações estratégicas, não públicas, processos internos, dados de pesquisa restritos).
- III. **Dados de Menores:** É expressamente desaconselhado o uso de qualquer dado que possa identificar ou estar relacionado a estudantes menores de idade em plataformas de IA, conforme o novo ECA Digital (Lei Nº 15.211, de 17 de Setembro de 2025).

2.2. Risco em ferramentas externas ("Shadow AI")

- I. Muitas ferramentas de IA de uso pessoal (externas ao contrato do IFSC) utilizam os dados inseridos (prompts e arquivos) para treinar seus modelos. O IFSC não possui controle destes dados, mesmo que o login de uma ferramenta como ChatGPT, tenha se utilizado do e-mail @ifsc.edu.br ou @aluno.ifsc.edu.br, por isso é **desaconselhado** seu uso.
- II. Caso realmente seja necessário utilizar estas ferramentas em ambientes institucionais para fins diversos, só deve ser feito carregando dados públicos sem risco ao IFSC. É **mandatório** que o usuário configure sua conta para desativar o compartilhamento de dados para treinamento. (Veja o *Guia de Opt-Out no Anexo I*).

3. Integridade e Responsabilidade Acadêmica e Administrativa

3.1. Primazia Humana e Responsabilidade Integral

- I. **Primazia Humana:** A IA deve ser encarada como uma ferramenta de suporte, não como coautora. A responsabilidade final e a tomada de decisão cabe sempre ao humano revisor.
- II. **Responsabilidade Integral:** O usuário é integralmente responsável por verificar a precisão, adequação, originalidade e ausência de vieses no conteúdo gerado pela IA (incluindo "alucinações"). A responsabilidade por qualquer dano ou informação falsa, tende a recair sobre o humano que a validou.

3.2. Transparência e Citação (Integridade Acadêmica)

- I. **Transparência:** O uso de IA para gerar conteúdo (textos, códigos, imagens) exige citação ou declaração explícita de uso (com extensão do uso). Deve-se incluir declaração explícita detalhando quais ferramentas de IA utilizou e para quais finalidades no trabalho (ex: "para revisão gramatical", "para código base", "para brainstorming", "para análise preliminar", etc).
- II. **Conduta ética:** A omissão da declaração de uso de IA pode ser tratada como má conduta acadêmica (plágio ou similar). Não se deve considerar uma IA como parte autora (coautoria), mas sim ferramental (explicitando modelo e versão do algoritmo utilizado).
- III. **Responsabilização e corresponsabilidade:** O autor e orientador são responsáveis por verificar a fidedignidade, a veracidade das fontes e a qualidade do conteúdo gerado pela IA, garantindo a originalidade e a qualidade da produção. Eventuais erros, alucinações ou invenções realizadas pela IA, serão atribuídos aos revisores humanos que publicaram conteúdo gerado por IA sem checagem.

3.3. Usos de Alto Risco

- I. Não se deve submeter, como de autoria própria, trabalhos gerados integralmente por IA.
- II. Não se deve utilizar a IA para tomar decisões totalmente automatizadas que afetem direitos de discentes ou servidores sem supervisão humana qualificada.
- III. Não se deve usar as API Keys (Key for Application Program Interface - Chave para Interface de Programação de Aplicações), geradas com acesso do IFSC em sistemas externos a Instituição.

4. Governança e Procedimentos Institucionais

Cada servidor e estudante é responsável pelos dados que insere em plataformas digitais. A presente recomendação visa orientar e proteger toda a comunidade. O uso consciente da tecnologia é fundamental para garantir um ambiente digital seguro para todos.

4.1. Catálogo de Ferramentas de IA

- I. A Coordenadoria de Gestão de Dados (CGD) manterá um [Catálogo de Ferramentas de IA Sugeridas](#) que possuam algum tipo de licenciamento vinculado ao IFSC, detalhando as soluções sugeridas e suas formas de acesso institucional mais seguro.

4.2. Gestão de Incidentes

- I. Qualquer incidente de segurança ou eventuais vazamentos de dados pessoais, devem ser imediatamente comunicados à DTIC através dos e-mails csirt@ifsc.edu.br e encarregado.lgpd@ifsc.edu.br

4.3. Consentimento de Menores

- I. O uso de plataformas institucionais (Google/Microsoft) por estudantes menores de idade requer consentimento explícito dos responsáveis, conforme procedimento em implantação.
- II. O Termo de Consentimento de Dados será provido pelos setores durante a Matrícula para novos alunos para cumprimento do ECA Digital (Lei Nº 15.211, de 17 de Setembro de 2025).

4.4. Consulta e Orientação

- I. Para facilitar o processo de adequação, a Coordenadoria de Gestão de Dados (CGD) se coloca à disposição para, na medida do possível, tirar dúvidas pontuais sobre essa Orientação Técnica através do e-mail coord.gestao.dados@ifsc.edu.br
- II. Ao envolver dados pessoais deve-se procurar o Encarregado pela Proteção de Dados Pessoais (DPO) do IFSC, através de e-mail encarregado.lgpd@ifsc.edu.br ou formulário disponível em: <https://ifsc.edu.br/en/lgpd-lei-geral-de-protacao-de-dados>

4.5. Gestão de Incidentes e Regime Disciplinar

- I. Qualquer questão técnica de erro nas plataformas ou integrações de acesso que necessitem correções programáticas, devem ser comunicadas à DTIC através de suporte.ti@ifsc.edu.br
- II. O descumprimento desta Orientação sujeitará o infrator às sanções cabíveis, em conformidade com o Regulamento Disciplinar Discente ou o Regime Jurídico dos Servidores Públicos (Lei nº 8.112/1990).

5. Referências

A elaboração desta orientação técnica baseia-se nos seguintes documentos institucionais e termos de serviço das plataformas homologadas:

5.1. IFSC - Documentos Institucionais e Recomendações

- I. IFSC. Processo de Validação de Serviços de Nuvem (Google/Microsoft). Disponível em: https://sipac.ifsc.edu.br/public/jsp/processos/processo_detalhado.jsf?id=22942
- II. IFSC. PROJUR. COTA n. 00059/2019/PF/IFSC/PGF/AGU. (Ref. Processo SIPAC NUP 23292.028158/2019-20).

5.2. Google - Termos de Uso, Privacidade e FAQs

- I. Termos de Serviço (Education): https://workspace.google.com/terms/education_terms/
- II. Privacidade e LGPD (Cloud): <https://cloud.google.com/security/compliance/lqpd?hl=pt-BR>
- III. Gemini for Google Workspace FAQ - Education. Google Workspace for Education Help: <https://support.google.com/a/answer/14130944?hl=pt-PT>
- IV. Learn More About Google Workspace with Gemini. Google for Education: <https://edu.google.com/workspace-for-education/add-ons/gemini-education/>
- V. Google Workspace for Education data protection implementation guide. Google Services: https://services.google.com/fh/files/misc/google_workspace_edu_data_protection_implementation_guide.pdf
- VI. Compliance | Como o Google obedece às leis de proteção de dados. Google Safety Center: <https://business.safety.google/intl/pt-BR/compliance/>
- VII. Controles de privacidade e compartilhamento de dados no Google Cloud:
 - A. <https://cloud.google.com/terms/service-terms>
 - B. <https://cloud.google.com/vertex-ai/docs/generative-ai/data-governance>
 - C. <https://cloud.google.com/vertex-ai/docs/generative-ai/data-privacy>

5.3. Microsoft - Termos de Uso e Privacidade

- I. Declaração de Privacidade (Geral): <https://privacy.microsoft.com/pt-br/privacystatement>
- II. Privacidade de Dados (Azure OpenAI): <https://learn.microsoft.com/pt-br/legal/cognitive-services/openai/data-privacy>

5.4. OpenAI - Termos de Uso, Privacidade e FAQs

- I. <https://help.openai.com/en/articles/7730893-data-controls-faq>
- II. <https://openai.com/policies/api-data-usage-policies>
- III. <https://help.openai.com/en/articles/5722486-how-your-data-is-used-to-improve-model-performance>
- IV. https://openai.com/consumer-privacy/?utm_source=chatgpt.com

5.5. Guias e Documentos Externos

- I. **UNIVERSIDADE DO ESTADO DE SANTA CATARINA (UDESC)**. Biblioteca Universitária. Guia para uso ético da inteligência artificial generativa. Florianópolis, 2025. Disponível em: https://www.udesc.br/arquivos/udesc/documentos/Guia_IA_17607147749128_4769.pdf
- II. **ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, A CIÊNCIA E A CULTURA (UNESCO)**. Guia para a IA generativa na educação e na pesquisa. Paris: Unesco, 2024. Disponível em: <https://unesdoc.unesco.org/ark:/48223/pf0000390241>
- III. **UNIVERSIDADE FEDERAL DO CEARÁ (UFC)**. Portaria nº 39/2025 - PRPPG. Regulamenta o uso de Inteligência Artificial e ferramentas de verificação de similaridade em pesquisas da Pós-Graduação. Disponível em: <https://prppg.ufc.br/wp-content/uploads/2025/10/portaria-no-39-prppg-ufc.pdf>

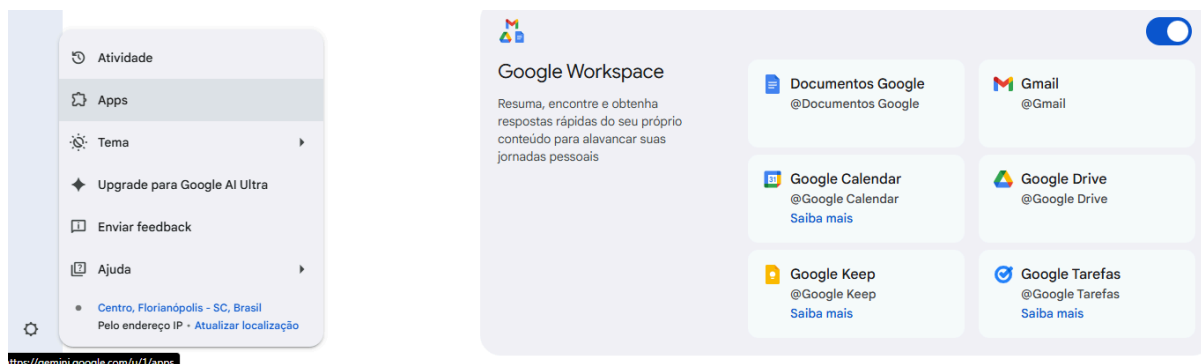
ANEXO I – GUIA DE OPT-OUT DE TREINAMENTO (USO DE IA PESSOAL)

Para minimizar os riscos de privacidade ao usar contas pessoais ou gratuitas em ferramentas de IA, siga estas instruções para solicitar que seus dados não sejam utilizados para treinamento:

- **Google (Conta Gmail Pessoal - Gemini):**
 - Acesse <https://myactivity.google.com/activitycontrols>;
 - Vá para "Atividade na Web e de apps";
 - Desative "Incluir o histórico do Chrome e a atividade em sites, apps e dispositivos que usam serviços do Google";
 - Prefira usar "Conversa Momentânea" no canto superior esquerdo no pontilhado:



- Desmarque as opções para compartilhar dados com outros Apps;
- Canto esquerdo inferior Configurações, Apps, desmarque as chaves azuis:



- **OpenAI (ChatGPT Pessoal - Vinculado ou não com login via e-mail do IFSC):**
 - Vá em "Settings" (Configurações);
 - Acesse "Data Controls" (Controlar dados);
 - Desative "Improve the model for everyone" (Melhorar o modelo para todo mundo);
 - Ao usar, no canto superior direito, clique no botão "Ativar chat temporário".

Farleir Luís Minozzo
Coordenadoria de Gestão de Dados
Florianópolis, 12 de Novembro de 2025.