REGULAMENTO DE DESENVOLVIMENTO DE SISTEMAS DE INFORMAÇÃO DO IFC

CAPÍTULO I
DAS DISPOSIÇÕES INICIAIS

Art. 1° O presente Regulamento disciplina o desenvolvimento e aprimoramento de sistemas de informação no âmbito do Instituto Federal Catarinense.

Art. 2º O desenvolvimento e aprimoramento de sistemas constitui responsabilidade da Coordenação Geral de Sistemas de Informação (CSI), unidade da Diretoria de Tecnologia da Informação (DTI), sob orientação do Comitê de Governança Digital (CGD).

CAPÍTULO II
DAS DEFINIÇÕES

Art. 3º Para os fins deste documento, considera-se:

I - Ambiente de Desenvolvimento Integrado (IDE's): Do inglês *Integrated Development Environment*, trata-se de um programa de computador que reúne características e ferramentas de apoio ao desenvolvimento de software com o objetivo de agilizar este processo.

II – Application Programming Interface (API): conjunto de regras ou protocolos que permitem que aplicativos de software se comuniquem entre si para trocar dados, recursos e funcionalidades.

II - Banco de dados: coleções organizadas de dados que se relacionam de forma a criar algum sentido (informação) e conferir mais eficiência a uma pesquisa ou a um estudo.

III - Controle de versão: software que tem como finalidade gerenciar diferentes versões no desenvolvimento de um documento qualquer.

IV - Escopo: características e funções que singularizam um produto, serviço ou resultado.

V - Framework: conjunto de classes implementadas em uma linguagem de programação específica, usadas para auxiliar o desenvolvimento de software.

VI - Linguagem de Programação: método padronizado para comunicar instruções para um computador. Pode ser também um conjunto de regras sintáticas e semânticas usadas para definir um programa de computador.

VII - Módulo: uma parte de sistema de informação que utiliza a mesma arquitetura tecnológica do sistema principal. É responsável por atividades que atendem a um assunto bem definido.

VIII - PDTIC: Plano Diretor de Tecnologia da Informação e Comunicação.

IX - Projeto: esforço temporário empreendido para criar um produto, serviço ou resultado exclusivo. Um projeto é temporário por ter uma data prevista para iniciar e uma data prevista para terminar.

X - Protocolo: convenção que controla e possibilita conexão, comunicação e transferência de dados entre dois sistemas computacionais.

XI - Requisito: definição documentada de uma propriedade ou comportamento que um produto ou serviço particular deve atender. Pode ser funcional, indicando uma funcionalidade de um sistema, ou não-funcional, indicando restrições dentro do sistema.

XII - Sistema de informação: conjunto de componentes inter-relacionados trabalhando juntos para coletar, recuperar, processar, armazenar e distribuir informações, com a finalidade de facilitar o planejamento, o controle, a coordenação, a análise e o processo decisório em organizações.

XIII - Wiki: Termo utilizado para identificar um tipo específico de coleção de documentos em hipertexto, ou o software colaborativo usado para criá-lo.

CAPÍTULO III
DA ABRANGÊNCIA

Art. 4º Todos os sistemas institucionais, sejam de origem dos *campi* ou da Reitoria, devem seguir este Regulamento, incluindo API's.

Art. 5º Os sistemas e/ou módulos a serem desenvolvidos devem estar alinhados ao planejamento estratégico e/ou PDTIC vigentes, exceto por previsão legal, devendo-se registrar o alinhamento ou dispositivo legal no documento que oficializa o início do projeto do sistema/módulo.

Parágrafo único. Caso o projeto não conste no planejamento estratégico e/ou plano diretor de TI vigentes, deve ser solicitada a sua inclusão na próxima revisão dos referidos documentos.

Art. 6º Devem ser observados os sistemas institucionais já existentes para aproveitamento e integração de informações, assim como evitar retrabalho.

Art. 7º Este Regulamento de Desenvolvimento de Sistemas tem como escopo o desenvolvimento dos sistemas de informação para uso do IFC.

§1º Não está contemplado nesse documento procedimento para aquisição de sistemas.

§2º Por desenvolvimento, entende-se novos sistemas e ajustes em sistemas já existentes. O mesmo se aplica a módulos de sistemas.

CAPÍTULO IV
DOS PAPÉIS E RESPONSABILIDADES

Art. 8º As tomadas de decisões sobre as demandas e prioridades do desenvolvimento de sistemas de informação, no âmbito do IFC, devem respeitar a distribuição de responsabilidades constantes neste Regulamento.

§1º Ao CGD, como responsável pela governança de TI no IFC, cabe o estabelecimento e a definição das prioridades no desenvolvimento de sistemas/módulos, quando necessário.

§2º À DTI, como responsável pela gestão de TI no IFC, cabe o acompanhamento do

andamento dos projetos de desenvolvimento de novos sistemas/módulos.

§3º À Coordenação Geral de Sistemas de Informação cabe o planejamento e monitoramento dos projetos de desenvolvimento de novos sistemas/módulos, em conjunto com a equipe executora.

§4º À equipe executora, nomeada pela Coordenação Geral de Sistemas de Informação, cabe o desenvolvimento, a execução, os testes e a implantação dos novos sistemas/módulos/api´s.

§5º A Pró-Reitoria demandante do sistema/módulo, representada pela área de negócio respectiva, deve auxiliar nas definições dos requisitos do novo sistema/módulo, sejam eles funcionais ou não funcionais, das regras de negócios, das justificativas legais, se for o caso e também nas atividades de testes, treinamento e na implantação definitiva.

CAPÍTULO V
DO GERENCIAMENTO DO PROJETO

Art. 9º Cada sistema a ser desenvolvido deve ser considerado como um projeto e, como tal, deve seguir premissas de gerenciamento de projetos, a ser definida em conjunto com a CSI.

§1º Sempre que possível, caberá ao coordenador Geral de Sistemas de Informação ser o gestor do projeto.

§2º Na impossibilidade de o coordenador Geral de Sistemas de Informação gerenciar o projeto, cabe a ele indicar um servidor para ser o gestor do projeto.

CAPÍTULO VI
DAS TECNOLOGIAS UTILIZADAS

Art. 10. Todas as tecnologias utilizadas devem ser submetidas a este Regulamento.

§1º Toda tecnologia utilizada para o desenvolvimento de sistemas, considerando-se todas as etapas do processo, desde o levantamento de requisitos até os testes finais, deve utilizar ferramentas gratuitas e, sempre que possível, de código aberto.

§2º Na inviabilidade de uso de licenças gratuitas e/ou de código aberto devem ser observados os trâmites dos marcos legais de contratação de TI, tal como previsto no PDTIC vigente.

§3º As linguagens de programação utilizadas devem ser definidas em conjunto com a CSI.

§4º Os frameworks utilizados devem ser definidos em conjunto com a CSI.

§5º As IDE’s utilizadas devem ser definidas em conjunto com a CSI.

§6º O banco de dados utilizado deve ser definido em conjunto com a CSI.

CAPÍTULO VII
DA GERÊNCIA DE CONFIGURAÇÃO

Art. 11. O propósito da gerência de configuração é estabelecer e manter a integridade de todos os produtos de trabalho do sistema, em todas as fases do desenvolvimento e disponibilizá-los a todos os envolvidos.

§1º Todos os sistemas desenvolvidos devem ser versionados por ferramenta com controle de versão, com utilização de tecnologia definida em conjunto com a CSI.

§2º O sistema de controle de versão Git deverá ser adotado como padrão institucional para gerenciamento de código-fonte.

§3º Todo sistema desenvolvido deverá possuir documentação técnica e funcional atualizada, armazenada em repositório institucional definido pela Coordenação Geral de Sistemas de Informação, contendo as informações necessárias para sua utilização, sustentação, evolução e manutenção, conforme padrões estabelecidos.

§4º A documentação mínima deverá contemplar, quando aplicável:

I. descrição da finalidade e das funcionalidades do sistema;

II. arquitetura da solução e diagramas técnicos;

III. tecnologias e dependências utilizadas;

IV. procedimentos de instalação, configuração e implantação;

V. integrações e interfaces com outros sistemas;

VI. documentação de APIs e serviços disponibilizados;

VII. modelo de dados e estrutura dos principais componentes;

VIII. procedimentos de backup e recuperação, quando aplicável;

IX. informações para suporte, manutenção e atualização do sistema;

X. orientações para usuários e administradores.

§5º Sempre que tecnicamente viável, a documentação deverá ser gerada ou atualizada de forma automatizada a partir dos artefatos do próprio sistema, visando garantir sua consistência e rastreabilidade.

CAPÍTULO VIII
DA INFRAESTRUTURA NECESSÁRIA

Art. 12. A unidade organizacional de TI responsável pela infraestrutura, na qual pretende-se hospedar o sistema/módulo a ser desenvolvido, deve ser consultada e envolvida desde o início do projeto.

§1º Na falta de infraestrutura de TI para uso do novo sistema, deve ser replanejado o projeto e, se aprovado, a aquisição necessária deve ser prevista no PDTIC vigente.

§2º Em caso de necessidade de materiais permanentes e/ou consumíveis para uso do novo sistema, devem ser contactadas as áreas responsáveis pelo seu fornecimento e, na falta

desses, o projeto deve ser replanejado.

CAPÍTULO IX
DO PROCESSO DE DESENVOLVIMENTO DO SISTEMA

Art. 13. Todos os sistemas desenvolvidos devem seguir um processo de desenvolvimento definido em conjunto com a CSI, considerando as especificidades de cada projeto.

CAPÍTULO X
DA INSTITUCIONALIZAÇÃO E DIVULGAÇÃO DO REGULAMENTO

Art. 14. O presente Regulamento deverá ser mantido e aprovado pela DTI e CGD, e todos os colaboradores devem ter conhecimento do documento.

§1º As condições mínimas para que o Regulamento seja revisado são:

I. Quando o Regimento Geral do IFC for alterado;
II. Quando o organograma do IFC for alterado;
III. Quando o Planejamento Estratégico do IFC for alterado;
IV. Quando necessário e decidido pelo CGD.

Art. 15. O presente Regulamento deverá ficar disponível em portal institucional.

CAPÍTULO XI
DO PORTFÓLIO DE SISTEMAS OFERECIDO PARA O PÚBLICO-ALVO DO IFC

Art. 16. Todos os sistemas de informação institucionais do IFC sob gerência da CSI devem ser registrados no catálogo de serviços de TI do IFC.

§1º Os sistemas deverão manter informações atualizadas em catálogo de serviços contendo, no mínimo:

I. nome do sistema;
II. finalidade;
III. responsável técnico;
IV. responsável negocial;
V. tecnologias utilizadas;
VI. integrações existentes;
VII. classificação de criticidade;
VIII. situação do ciclo de vida.

CAPÍTULO XII
DO USO DE INTELIGÊNCIA ARTIFICIAL NO DESENVOLVIMENTO DE SISTEMAS

Art. 17. A utilização de ferramentas de Inteligência Artificial (IA) poderá ser empregada nas atividades de desenvolvimento, manutenção, documentação, testes e suporte aos sistemas de informação institucionais.

§1º A utilização de ferramentas de IA não exime os desenvolvedores, analistas e gestores da responsabilidade pela qualidade, segurança, conformidade legal e funcionamento do software produzido.

§2º Todo código-fonte, documentação ou artefato gerado com apoio de IA deverá ser submetido à validação e revisão por servidor ou colaborador responsável antes de sua utilização em ambiente institucional.

§3º É vedado o compartilhamento de dados pessoais, dados sensíveis, informações sigilosas ou informações protegidas por legislação específica em ferramentas externas de IA sem autorização formal da área competente.

Art. 18. Poderão ser utilizadas ferramentas de IA para:

I. apoio à análise de requisitos;
II. geração e revisão de código-fonte;
III. elaboração de documentação técnica;
IV. criação de casos de teste;
V. análise de vulnerabilidades;
VI. apoio à tomada de decisão técnica;
VII. geração de protótipos e interfaces.

CAPÍTULO XIII
DA INTEGRAÇÃO E ENTREGA CONTÍNUA

Art. 19. Os projetos de software deverão, sempre que tecnicamente viável, utilizar processos automatizados de integração contínua e entrega contínua (CI/CD).

§1º Os processos automatizados poderão contemplar:

I. compilação do código;
II. execução de testes automatizados;
III. análise estática de código;
IV. verificação de vulnerabilidades;
V. geração de artefatos para implantação.

§2º As implantações em ambiente de produção deverão observar os procedimentos de homologação e autorização definidos pela área responsável.

CAPÍTULO XIV
DA GERÊNCIA DE CONFIGURAÇÃO E CONTROLE DE VERSÃO

Art. 20. Todo desenvolvimento deverá ocorrer em ramificações específicas, observando a estratégia de versionamento definida pela área de Tecnologia da Informação.

Art. 21. Alterações de código somente poderão ser incorporadas à linha principal de desenvolvimento mediante processo formal de revisão e aprovação.

§1º A revisão deverá considerar aspectos de:

I. qualidade do código;
II. aderência aos requisitos;
III. segurança da informação;
IV. conformidade com os padrões institucionais.

CAPÍTULO XV
DA SEGURANÇA NO DESENVOLVIMENTO DE SOFTWARE

Art. 22. Os sistemas de informação deverão ser desenvolvidos observando os princípios de Segurança da Informação desde sua concepção.

Art. 23. Os sistemas de informação desenvolvidos ou mantidos pela instituição deverão implementar mecanismos adequados de autenticação, autorização, controle de acesso, registro de auditoria e proteção de dados, compatíveis com o nível de criticidade do sistema e com as diretrizes de Segurança das Informações vigentes.

§1º Os sistemas destinados ao atendimento de usuários externos deverão, preferencialmente, utilizar mecanismos de autenticação federadas disponibilizadas pelo Governo Federal por meio da plataforma Gov.br, observadas as normas e os requisitos técnicos estabelecidos pelos órgãos competentes.

§2º A integração com a plataforma Gov.br deverá ser realizada por meio dos protocolos e padrões adotados pelo Governo Federal, observando os requisitos de segurança, privacidade e proteção de dados pessoais.

§3º A utilização de mecanismos próprios de autenticação deverá ser tecnicamente justificada e aprovada pela CGD.

§4º Sempre que aplicável, deverão ser observadas as diretrizes da Lei Geral de Proteção de Dados Pessoais – LGPD e demais normativos relacionados.

§ 5º Da Gestão de Dados em Ambientes de Homologação. Os ambientes de homologação deverão utilizar, obrigatoriamente, dados anonimizados ou descaracterizados, de forma a impedir a identificação ou associação, direta ou indireta, de pessoas. Fica vedada a utilização de dados pessoais identificáveis nesses ambientes, salvo mediante autorização formal e devidamente justificada, observadas as medidas de segurança e proteção de dados aplicáveis.

CAPÍTULO XVI
DA OBSERVABILIDADE E MONITORAMENTO

Art. 24. Os sistemas institucionais deverão disponibilizar mecanismos de registro e monitoramento que permitam a identificação de falhas, incidentes e degradações de desempenho.

Art. 25. Os registros de eventos deverão possibilitar a rastreabilidade das operações realizadas pelos usuários e pelos processos automatizados.

§1º Os registros deverão observar as normas institucionais de segurança e proteção de dados.

§2º A área de Tecnologia da Informação poderá definir padrões para centralização e retenção de logs.

CAPÍTULO XVII
DA ARQUITETURA E INTEGRAÇÃO DE SISTEMAS

Art. 26. Os sistemas desenvolvidos deverão priorizar arquiteturas que favoreçam escalabilidade, manutenibilidade, interoperabilidade e reutilização de componentes.

§1º Poderão ser adotadas arquiteturas monolíticas, modulares, orientadas a serviços ou baseadas em microsserviços, conforme a complexidade, os requisitos e as características da solução.

§2º Sempre que tecnicamente justificável, os sistemas poderão ser desenvolvidos utilizando arquiteturas desacopladas, com separação entre as camadas de apresentação (frontend) e de negócio (backend), promovendo a evolução independente dos componentes, o reaproveitamento de serviços e a interoperabilidade entre aplicações.

§3º Nas arquiteturas desacopladas, a comunicação entre frontend e backend deverá ocorrer por meio de APIs padronizadas, observando os requisitos de segurança, autenticação, documentação e governança definidos pela Diretoria de Tecnologia da Informação.

Art. 27. As integrações entre sistemas institucionais deverão ocorrer preferencialmente por meio de APIs padronizadas, documentadas e aderentes aos padrões tecnológicos definidos pela Diretoria de Tecnologia da Informação.

§1º As APIs desenvolvidas para consumo interno ou externo deverão possuir documentação técnica atualizada, mecanismos de autenticação e autorização, controle de versão e monitoramento de uso.

§2º A publicação, exposição e gerenciamento de APIs deverão ser realizados, preferencialmente, por intermédio do API Gateway Institucional, observadas as diretrizes de segurança, interoperabilidade e governança estabelecidas pela DTI.

§3º Exceções à utilização do API Gateway Institucional deverão ser justificadas tecnicamente e aprovadas pela área responsável pela arquitetura e governança de sistemas.

CAPÍTULO XVIII
DA ACESSIBILIDADE E EXPERIÊNCIA DO USUÁRIO

Art. 28. Os sistemas desenvolvidos para uso interno ou externo deverão observar os requisitos de acessibilidade digital estabelecidos pela legislação vigente.

Art. 29. Os sistemas destinados ao público externo deverão, sempre que possível, adotar os padrões definidos pelo Design System do Governo Federal e pelas diretrizes do Modelo de Acessibilidade em Governo Eletrônico – eMAG.

Art. 30. As interfaces deverão ser desenvolvidas considerando critérios de usabilidade, responsividade e experiência do usuário.

CAPÍTULO XIX
DA GOVERNANÇA E DO CICLO DE VIDA DOS SISTEMAS

Art. 31. Todo sistema institucional deverá possuir responsável técnico e responsável pela área de negócio.

Art. 32. Os sistemas deverão possuir plano de manutenção e atualização tecnológica compatível com sua relevância institucional.

Parágrafo único. Os sistemas considerados obsoletos ou sem utilização comprovada pela CSI poderão ser submetidos a processo formal de descontinuação.

CAPÍTULO XX
DAS DISPOSIÇÕES GERAIS

Art. 33. Os desenvolvedores dos sistemas devem verificar se estes são ou podem ser objeto de Registro de Propriedade Intelectual, devendo, em caso afirmativo, solicitar orientações do Núcleo de Inovação Tecnológica (NIT) quanto aos procedimentos cabíveis com fim de promover e acompanhar o processo de sua proteção, de acordo com as normas internas e legislação vigente.

Art. 34. Deve ser dada a devida transparência aos projetos de desenvolvimento de sistemas do IFC, por meio da publicação em portal institucional, permitindo-se sua consulta pelo público em geral.

Art. 35. As unidades de TI do IFC deverão informar à DTI a lista de sistemas desenvolvidos e/ou em uso em seus respectivos *campi* em um prazo de 90 (noventa) dias a contar da data de publicação deste Regulamento.

Art. 36. Os casos omissos e as eventuais dúvidas na aplicação do presente Regulamento serão resolvidos pelo CGD.

Art. 37. Este Regulamento entra em vigor na data de sua publicação.

REFERÊNCIAS

Laudon; Kenneth C.; Laudon; Jane Price (1999). *Sistema da Informação com Internet*. [S.l.: s.n.]

PMBOK, GUIA. Um guia do conhecimento em gerenciamento de projetos. **Quarta Edição**, v. 123, 2013.

PRESSMAN, Roger; MAXIM, Bruce. **Engenharia de Software-8ª Edição**. McGraw Hill Brasil, 2016.

PORTARIA NORMATIVA - ANEXOS Nº 5/2026 - ASSINST/REI (11.01.18.00.65)

(Nº do Protocolo: NÃO PROTOCOLADO)

(Assinado digitalmente em 03/11/2026 12:49)
RUDINEI KOCK EXTERCKOTER
REITOR

Visualize o documento original em https://sig.ifc.edu.br/documentos/ informando seu número: ***5****, ano:* ***2026****, tipo:* ***PORTARIA NORMATIVA - ANEXOS****, data de emissão:* ***03/11/2026*** *e o código de verificação:* ***a010199730***