SEMA
Secretaria
de Estado de
Meio Ambiente

Governo de
Mato
Grosso

PROCESSO DE DESENVOLVIMENTO DE SOFTWARE (PDS)

Versão 2.0

Contrato 071/2024/SEMA-FUNADIF

Cuiabá/MT • Agosto de 2026

SUMÁRIO

1. Introdução

> **LEITURA ORIENTADA:** O desenvolvimento, a manutenção, a sustentação e a evolução de soluções de software constituem atividades estratégicas para a Secretaria de Estado de Meio Ambiente de Mato Grosso — SEMA/MT, pois apoiam a execução das políticas públicas ambientais, a prestação de serviços à sociedade, a gestão institucional e a tomada de decisões baseada em dados.

A ausência de um processo institucional integrado pode ocasionar demandas incompletas, decisões não rastreáveis, retrabalho, baixa previsibilidade, falhas de comunicação, soluções fragmentadas, riscos de segurança e dificuldades no acompanhamento das entregas realizadas por equipes internas ou fornecedores contratados.

O Processo de Desenvolvimento de Software — PDS da SEMA/MT estabelece princípios, papéis, atividades, critérios, artefatos, controles e registros aplicáveis a todo o ciclo de vida das iniciativas de software, desde a identificação e o registro formal da necessidade até a análise, priorização, especificação, planejamento, contratação ou acionamento da execução, desenvolvimento, testes, homologação, aceite, implantação, recebimento, sustentação, evolução e eventual descontinuação da solução.

O processo é coordenado pela Superintendência de Tecnologia da Informação — STI e executado de forma colaborativa pelas unidades competentes, pelas áreas demandantes, pelas equipes técnicas, pela fiscalização e gestão contratual e, quando aplicável, pelas empresas contratadas. As atribuições específicas de cada participante são detalhadas no Capítulo 9 deste documento.

O PDS adota abordagem adaptável, iterativa e proporcional ao porte, à complexidade, à criticidade, aos riscos e à modalidade de execução de cada iniciativa. Assim, os controles e artefatos exigidos deverão ser suficientes para assegurar qualidade, segurança, conformidade, rastreabilidade e valor público, sem impor burocracia desnecessária às demandas de menor complexidade.

O processo deverá acompanhar a evolução das práticas de engenharia de software, arquitetura, gestão, segurança, automação e governança, sem vincular permanentemente a instituição a tecnologias específicas. Ferramentas institucionais poderão ser definidas para operacionalizar o processo, desde que seus papéis, fontes oficiais de informação e regras de integração sejam formalmente estabelecidos.

Este documento constitui instrumento institucional vivo, sujeito a avaliação e melhoria contínua, devendo ser atualizado sempre que mudanças organizacionais, legais, contratuais, metodológicas ou tecnológicas produzirem impacto relevante no processo.

1.1 Objetivo do Processo de Desenvolvimento de Software

O Processo de Desenvolvimento de Software da SEMA/MT tem como objetivo estabelecer um modelo institucional integrado, padronizado, rastreável e proporcional para a gestão de demandas e para o ciclo de vida das soluções de software.

Especificamente, o PDS visa:

a) padronizar o registro, a triagem, a análise, a priorização e o acompanhamento das demandas de software;

b) estabelecer responsabilidades claras entre áreas demandantes, unidades de tecnologia, equipes técnicas, governança, infraestrutura, fiscalização, gestão contratual e fornecedores;

c) assegurar que necessidades institucionais sejam transformadas em requisitos, histórias de usuário, regras de negócio e critérios de aceite suficientemente claros, testáveis e rastreáveis;

d) orientar o planejamento, a contratação, a emissão e o acompanhamento de Ordens de Serviço e demais instrumentos de execução contratual;

e) garantir a qualidade funcional, técnica, arquitetural, operacional e de segurança dos produtos de software;

f) disciplinar os processos de validação técnica, homologação funcional, aceite, recebimento contratual, implantação e encerramento;

g) assegurar rastreabilidade entre demanda, requisito, modelo, código, teste, versão, homologação, aceite, medição e recebimento;

h) promover conformidade com o Regimento Interno, a legislação aplicável, as normas institucionais e as obrigações contratuais;

i) integrar processos, ferramentas, repositórios e evidências, evitando duplicidade e divergência de informações;

j) apoiar a medição de desempenho, qualidade, fluxo, segurança, conformidade e geração de valor público;

k) promover melhoria contínua e preservação do conhecimento institucional; e

l) aplicar controles e artefatos de forma proporcional ao porte, à complexidade, à criticidade e ao risco de cada iniciativa.

1.2 Escopo do Processo de Desenvolvimento de Software (PDS)

O PDS aplica-se às iniciativas de software conduzidas, contratadas, mantidas ou governadas pela SEMA/MT, independentemente da unidade demandante, da modalidade de execução, da tecnologia utilizada ou da origem dos recursos.

O escopo compreende:

I — Modalidades de atuação

desenvolvimento interno;

desenvolvimento por fábrica de software ou outro fornecedor contratado;

manutenção corretiva, adaptativa, evolutiva e preventiva;

sustentação e suporte especializado;

modernização, migração e descontinuação de sistemas; e

aquisição ou contratação de soluções que envolvam customização, integração ou desenvolvimento.

II — Tipos de solução

sistemas corporativos e departamentais;

aplicações web e móveis;

portais e serviços digitais;

APIs, integrações e serviços de interoperabilidade;

automações de processos e soluções de RPA;

soluções de BI, dados, ciência de dados e inteligência artificial;

componentes, bibliotecas e serviços reutilizáveis; e

soluções low-code ou no-code, quando aplicável.

III — Processos abrangidos

identificação e registro formal da necessidade;

triagem e análise pela TI;

levantamento, especificação e validação dos requisitos;

priorização e gestão do backlog;

análise de viabilidade, arquitetura, segurança, infraestrutura e estimativa;

planejamento da execução e, quando aplicável, contratação ou emissão de Ordem de Serviço;

desenvolvimento, testes, revisão, integração e entrega;

validação técnica, homologação funcional e tratamento de pendências;

implantação, aceite, medição, recebimento e encerramento; e

monitoramento, sustentação, evolução e descontinuação.

O PDS integra-se aos processos de contratação pública, gestão contratual, segurança da informação, governança de dados, gestão de serviços e infraestrutura de TIC, sem substituir os normativos específicos aplicáveis a essas matérias.

1.3 Público-Alvo

O PDS destina-se a todos os participantes envolvidos na identificação, análise, priorização, especificação, execução, fiscalização, homologação, implantação, sustentação e governança das soluções de software da SEMA/MT.

Público	Participação no PDS
Alta Administração e STI	Direcionamento, aprovação de prioridades e resolução de conflitos estratégicos.
Área demandante	Identificação e justificativa da necessidade.
Gestor do negócio	Definição funcional, validação de requisitos, homologação e confirmação do valor entregue.
Usuários-chave e homologadores	Elicitação, validação de cenários e execução da homologação.
CSTI	Triagem, análise, refinamento, coordenação técnica, acompanhamento e validação.
CPQSI	Governança, metodologia, conformidade e avaliação do processo.
CITI	Infraestrutura, ambientes, bancos de dados, redes, operação e segurança técnica da infraestrutura.
Gerência de Atendimento e Suporte Técnico	Registro de incidentes, suporte e feedback de usuários.
Arquitetos, analistas e especialistas	Requisitos, arquitetura, dados, segurança, integração e testes.
Fábrica de software ou fornecedor contratado	Estimativa, desenvolvimento, testes, correções, documentação e entrega dos produtos, conforme contrato e Ordem de Serviço.
Fiscal técnico	Acompanhamento e avaliação técnica da execução contratual.
Fiscal requisitante	Verificação do atendimento à necessidade institucional.
Fiscal administrativo	Verificação das obrigações administrativas e documentais.
Gestor do contrato	Coordenação da gestão contratual e formalização das decisões de sua competência.
Encarregado e áreas de privacidade	Orientação e avaliação de aspectos relacionados à proteção de dados.
Auditoria e controle	Verificação de conformidade, rastreabilidade e regularidade.

1.4 Princípios e Diretrizes Gerais

O PDS é orientado pelos princípios de transparência, sustentabilidade, segurança da informação, foco em resultados, rastreabilidade, interoperabilidade, reutilização de soluções, arquitetura corporativa, entrega de valor público, melhoria contínua,

conformidade normativa e segurança e privacidade desde a concepção (Security by Design e Privacy by Design).

Além desses princípios, o PDS observará:

Proporcionalidade: os controles, artefatos e aprovações deverão ser adequados ao porte, à complexidade, à criticidade e ao risco da iniciativa;

Fonte oficial da informação: cada tipo de informação deverá possuir ferramenta ou repositório oficial, evitando duplicidade, divergência e perda de rastreabilidade;

Segregação de funções: as responsabilidades de especificar, executar, validar, homologar, fiscalizar e receber deverão ser distribuídas de forma compatível com a governança e com a modalidade de execução;

Rastreabilidade ponta a ponta: toda entrega deverá ser relacionada à sua demanda de origem, requisitos, critérios de aceite, implementação, testes, homologação, versão, medição e recebimento;

Decisão baseada em critérios e evidências: priorizações, aprovações, exceções, homologações e recebimentos deverão ser justificados e registrados;

Documentação viva e integrada: sempre que possível, os registros serão mantidos nas ferramentas utilizadas pelo processo, evitando documentos paralelos e desatualizados;

Automação responsável: automações poderão apoiar validações, geração de documentos, integração e monitoramento, sem substituir decisões que exijam manifestação formal de autoridade competente;

Responsabilidade funcional do negócio: a área demandante permanecerá responsável por validar a necessidade, aprovar os requisitos e homologar a solução;

Qualidade incorporada ao fluxo: requisitos, arquitetura, segurança, testes, observabilidade e documentação serão tratados continuamente durante o ciclo de vida; e

Independência tecnológica: a adoção de ferramentas deverá observar padrões institucionais e permitir evolução, integração, portabilidade e preservação do conhecimento.

A governança do processo e a execução técnica observarão as competências definidas no Regimento Interno e detalhadas no Capítulo 9. A CPQSI atuará na governança, metodologia, conformidade e avaliação do processo; a CSTI, na coordenação e validação técnica dos produtos e serviços de software; e a CITI, na infraestrutura e segurança técnica

dos ambientes, sem prejuízo das responsabilidades das áreas demandantes, da fiscalização, da gestão contratual e dos fornecedores.

1.5 Aplicabilidade do PDS

O PDS é de observância obrigatória para as iniciativas de software conduzidas, contratadas, mantidas ou acompanhadas pela SEMA/MT.

Sua aplicação alcança servidores, gestores, áreas demandantes, equipes técnicas, homologadores, fiscais, gestores contratuais e fornecedores, respeitadas as competências institucionais e contratuais de cada participante.

A obrigatoriedade refere-se à observância dos princípios, papéis, registros, decisões, controles e critérios aplicáveis. A quantidade e o detalhamento dos artefatos deverão ser proporcionais ao porte, à complexidade, à criticidade, ao risco e à modalidade da iniciativa, conforme matriz de aplicabilidade definida neste PDS.

As contratações, termos de referência, estudos técnicos, contratos, Ordens de Serviço e demais instrumentos relacionados ao desenvolvimento, manutenção ou sustentação de software deverão incorporar ou referenciar as disposições aplicáveis deste PDS.

As atividades e decisões deverão ser registradas nas ferramentas ou repositórios institucionais definidos, assegurando rastreabilidade, integridade, autoria e histórico.

Eventuais dispensas, adaptações ou exceções deverão ser justificadas, avaliadas quanto aos riscos, aprovadas pela autoridade competente e registradas no processo correspondente.

Em caso de conflito, prevalecerão a legislação, os normativos estaduais, as disposições contratuais válidas e as competências estabelecidas no Regimento Interno, devendo o PDS ser posteriormente atualizado quando necessário.

1.6 Modelo Institucional de Execução do PDS

O PDS será operacionalizado de forma integrada, observando-se a atribuição de uma fonte oficial para cada conjunto de informações.

O Redmine será utilizado como plataforma de registro e acompanhamento das demandas, fluxos, responsáveis, prioridades, requisitos, histórias de usuário, critérios de

aceite, tarefas, defeitos, versões, evidências, homologações e decisões, conforme parametrização institucional.

O GovFlow atuará como camada de automação e orquestração, apoiando a validação de dados obrigatórios, a aplicação das regras do PDS, a geração de estruturas e documentos, a integração entre ferramentas e a consolidação de indicadores.

O Enterprise Architect será utilizado para modelagem e gestão dos elementos arquiteturais, processos, requisitos complexos, casos de uso, modelos de dados, integrações e demais artefatos técnicos definidos como aplicáveis.

Os repositórios Git e as ferramentas de integração e entrega contínuas constituirão as fontes oficiais para código-fonte, versionamento, revisão, pipelines, testes automatizados, análises de segurança e pacotes de entrega.

Os documentos administrativos e contratuais permanecerão registrados nos processos e sistemas oficiais competentes, mantendo-se no Redmine os vínculos e as referências necessárias à rastreabilidade.

As regras detalhadas de uso, integração, responsabilidade e precedência entre essas ferramentas serão definidas nos capítulos específicos deste PDS.

1.7 Governança e Atualização do PDS

O PDS será mantido sob coordenação da STI, com participação das unidades competentes e das áreas envolvidas em sua execução.

As propostas de alteração deverão ser fundamentadas em mudanças legais, regimentais, contratuais, tecnológicas ou processuais, em resultados de auditorias, indicadores, lições aprendidas ou necessidades de melhoria.

Cada versão deverá possuir histórico de alterações, responsáveis, data de aprovação, vigência e relação dos capítulos afetados.

O documento deverá ser revisado periodicamente e sempre que ocorrer mudança relevante que comprometa a aderência entre o processo documentado e a prática institucional.

Guias, catálogos, templates, checklists, configurações e procedimentos operacionais poderão ser atualizados de forma controlada sem exigir a reedição integral do PDS, desde que não alterem papéis, competências ou princípios aprovados.

1.8 Visão executiva do PDS

A síntese visual a seguir apresenta a lógica institucional do PDS em uma única página, reunindo propósito, problemas enfrentados, pilares, papéis, fases, ferramentas, benefícios, resultados e indicadores. Ela deve ser usada como porta de entrada para gestores, áreas demandantes, equipes técnicas, fiscalização e fornecedores.

Leitura orientada: o infográfico resume o processo, mas não substitui os requisitos, responsabilidades, gates, critérios e anexos do PDS. Em caso de dúvida, prevalece o conteúdo normativo dos capítulos e instrumentos oficiais.

Infográfico Executivo do PDS

Visão estratégica, governança, benefícios e ecossistema do Processo de Desenvolvimento de Software da SEMA/MT.

TECNOLOGIA COM PROPÓSITO | GESTÃO COM GOVERNANÇA | VALOR PÚBLICO PARA A SOCIEDADE

1. PROPÓSITO DO PDS

- Padronizar o ciclo de vida do software
- Integrar negócio, TI, fiscalização e fábrica
- Aumentar qualidade, segurança, rastreabilidade e previsibilidade
- Apoiar valor público e continuidade dos serviços

2. PROBLEMAS QUE O PDS RESOLVE

- Demandas sem padronização
- Baixa rastreabilidade
- Fragilidade em homologação, aceite e recebimento
- Dependência excessiva de pessoas ou fornecedor
- Falta de integração entre requisitos, código, testes e operação

3. PILARES DO PDS

- Governança
- Requisitos e backlog
- Arquitetura e integração
- Qualidade e testes
- Segurança e privacidade
- Riscos e métricas
- Sustentação e melhoria contínua

4. PAPÉIS PRINCIPAIS

- Área Demandante
- Gestor do Negócio
- CSTI
- CPQSI
- CITI
- Fábrica de Software
- Fiscalização / Gestão Contratual
- Governança

5. FASES DO PROCESSO

1. Demanda
2. Análise
3. Priorização
4. Execução
5. Testes
6. Homologação
7. Recebimento
8. Implantação
9. Sustentação

6. ECOSSISTEMA DE FERRAMENTAS

- **REDMINE** — gestão operacional e rastreabilidade
- **GovFlow** — automação, validação e orquestração
- **ENTERPRISE ARCHITECT** — modelagem e arquitetura
- **GitLab** — código, versionamento e pipelines
- **CI/CD E DEVSECOPS** — qualidade, testes e segurança
- **OPENSHIFT / AMBIENTES** — execução e operação

7. BENEFÍCIOS INSTITUCIONAIS

- Mais transparência
- Melhor governança
- Melhor qualidade das entregas
- Mais segurança e conformidade
- Menor retrabalho
- Melhor gestão da fábrica
- Melhor acompanhamento por indicadores
- Mais continuidade e sustentabilidade

8. RESULTADOS ESPERADOS

- Entregas mais previsíveis
- Homologação e recebimento mais consistentes
- Requisitos mais claros
- Melhor integração entre áreas
- Testes mais robustos
- Melhor suporte à tomada de decisão

9. INDICADORES DE SUCESSO

- Lead time
- Qualidade das entregas
- Defeitos em produção
- Cumprimento de SLA
- Vulnerabilidades tratadas
- Satisfação do usuário
- Valor público entregue

2. Contextualização e Fundamentos

2.1 Papel Estratégico do Software na SEMA/MT

> **LEITURA ORIENTADA:** As soluções de software constituem ativos estratégicos para a Secretaria de Estado de Meio Ambiente de Mato Grosso — SEMA/MT, pois apoiam a formulação e a execução de políticas públicas, a fiscalização ambiental, o licenciamento, o monitoramento dos recursos naturais, a gestão administrativa e a prestação de serviços à sociedade.

Essas soluções não devem ser compreendidas apenas como produtos tecnológicos. Cada sistema integra processos de negócio, dados, regras, pessoas, infraestrutura, serviços digitais e responsabilidades institucionais. Consequentemente, seu desenvolvimento, manutenção e evolução devem estar vinculados aos objetivos da organização e aos resultados públicos que se pretende alcançar.

As iniciativas de software podem envolver sistemas corporativos, serviços digitais, aplicações móveis, integrações, geotecnologias, automações, análise de dados e inteligência artificial. A adoção dessas tecnologias deverá ocorrer de forma responsável, segura, interoperável e compatível com a arquitetura e a capacidade institucional da SEMA/MT.

As necessidades de software deverão ser formalmente registradas pelas áreas demandantes, analisadas e qualificadas pelas unidades competentes de tecnologia, priorizadas segundo critérios institucionais e conduzidas conforme o fluxo estabelecido neste PDS. A execução poderá ser realizada por equipes internas ou fornecedores contratados, preservando-se, em qualquer modalidade, a governança, a rastreabilidade, a qualidade e a responsabilidade da SEMA/MT sobre os resultados.

O valor de uma iniciativa deverá ser avaliado não apenas pelo volume de funcionalidades produzidas, mas também por sua contribuição para a eficiência dos processos, o atendimento ao cidadão, a segurança jurídica, a qualidade dos dados, a redução de riscos e o alcance dos objetivos institucionais.

2.2 Alinhamento com Políticas Públicas, Governo Digital e Sustentabilidade

As iniciativas de software da SEMA/MT deverão estar alinhadas às políticas públicas, ao planejamento institucional, às diretrizes de governo digital e aos objetivos ambientais e administrativos da Secretaria.

Esse alinhamento deve ser demonstrado desde o registro da demanda, mediante a identificação do problema a ser solucionado, do resultado esperado, dos usuários ou processos beneficiados e, quando aplicável, da obrigação legal, do risco ou do objetivo estratégico relacionado.

No contexto deste PDS, a sustentabilidade será considerada em múltiplas dimensões:

- Ambiental: uso responsável dos recursos computacionais e adoção de soluções compatíveis com os objetivos ambientais da instituição.
- Técnica: arquiteturas manuteníveis, interoperáveis, observáveis e capazes de evoluir.
- Operacional: documentação adequada, capacitação, continuidade e transferência de conhecimento.
- Econômica: avaliação dos custos de desenvolvimento, infraestrutura, licenciamento, manutenção e substituição.
- Institucional: redução da dependência de pessoas, tecnologias ou fornecedores específicos e preservação do conhecimento organizacional.

A aplicação dos critérios de sustentabilidade será proporcional ao porte e à criticidade da iniciativa. Os projetos de maior impacto deverão documentar as decisões arquiteturais, os custos de ciclo de vida, as alternativas avaliadas e os riscos de continuidade.

A sustentabilidade não será medida apenas pela adoção de tecnologias modernas, mas pela capacidade de a solução permanecer útil, segura, economicamente justificável e tecnicamente sustentável ao longo do tempo.

2.3 Fundamentos de Proteção de Dados Pessoais e Privacidade

A proteção de dados pessoais constitui requisito transversal do Processo de Desenvolvimento de Software da SEMA/MT. As iniciativas que realizem tratamento de

dados pessoais deverão observar a legislação aplicável, as orientações da autoridade competente e os normativos institucionais de privacidade e segurança.

A proteção de dados deverá ser considerada desde a identificação da demanda, abrangendo o levantamento da finalidade do tratamento, das categorias de dados, dos titulares, dos agentes envolvidos, dos compartilhamentos, dos prazos de retenção, das bases legais aplicáveis e dos riscos aos direitos e às liberdades dos titulares.

A utilização de consentimento não será presumida como regra geral. A base legal deverá ser definida conforme a finalidade e o contexto do tratamento, especialmente quando relacionado à execução de políticas públicas, ao cumprimento de obrigações legais ou ao exercício das competências institucionais da SEMA/MT.

Os requisitos de privacidade e segurança deverão ser proporcionais à natureza dos dados, ao contexto do tratamento, à exposição da solução, à criticidade do serviço e aos riscos identificados. Quando aplicável, deverão ser realizadas avaliação de risco, mapeamento do fluxo de dados e elaboração de Relatório de Impacto à Proteção de Dados Pessoais — RIPD.

Os sistemas deverão incorporar os princípios de privacidade desde a concepção e por padrão, incluindo, conforme aplicável:

- limitação da coleta ao necessário;
- transparência sobre o tratamento;
- controle de acesso;
- proteção contra acesso, alteração, perda ou divulgação indevidos;
- rastreabilidade das operações relevantes;
- retenção e descarte adequados;
- atendimento aos direitos dos titulares; e
- prevenção e resposta a incidentes.

O Capítulo 7 estabelece os requisitos, controles, responsabilidades, procedimentos e evidências aplicáveis à proteção de dados pessoais e à segurança. Os indicadores relacionados serão disciplinados no Capítulo 13, e os modelos documentais serão mantidos nos anexos ou repositórios institucionais correspondentes.

2.4 Fundamentos de Governança de TI, Dados e Arquitetura Corporativa

O PDS integra-se à governança de tecnologia da informação, à governança de dados e à arquitetura corporativa da SEMA/MT, de modo que as iniciativas de software sejam avaliadas e conduzidas como parte de um portfólio institucional, e não como soluções isoladas.

A governança de TI deverá assegurar:

- alinhamento das iniciativas aos objetivos institucionais;
- definição clara das responsabilidades e autoridades decisórias;
- priorização transparente das demandas;
- gestão dos recursos e da capacidade de execução;
- monitoramento de riscos, desempenho e conformidade;
- acompanhamento das contratações e dos resultados; e
- avaliação contínua do valor entregue.

A governança de dados deverá assegurar que os dados produzidos, utilizados ou compartilhados pelos sistemas sejam tratados como ativos institucionais, observando qualidade, integridade, disponibilidade, segurança, interoperabilidade, rastreabilidade, responsabilidade e uso adequado.

A arquitetura corporativa deverá apoiar a análise dos impactos das iniciativas sobre processos, aplicações, dados, integrações, infraestrutura e serviços. As decisões arquiteturais relevantes deverão ser documentadas, justificadas e relacionadas às respectivas demandas e requisitos.

O Redmine, o GovFlow, o Enterprise Architect, os repositórios de código e as demais ferramentas institucionais deverão operar de forma integrada e com responsabilidades definidas. A adoção dessas ferramentas não substitui a governança: ela fornece os registros, modelos, evidências e mecanismos de automação necessários à sua execução.

Os papéis institucionais são detalhados no Capítulo 9, os mecanismos de governança no Capítulo 8, o fluxo operacional no Capítulo 3 e as ferramentas no Capítulo 10.

2.5 Orientação a Valor Público e Gestão por Evidências

As iniciativas de software deverão demonstrar o valor público que se pretende produzir. Esse valor pode decorrer, entre outros fatores, de:

- melhoria do atendimento ao cidadão;
- aumento da eficiência administrativa;
- redução de prazos e retrabalho;
- cumprimento de obrigação legal ou regulatória;
- redução de riscos ambientais, operacionais, financeiros ou de segurança;
- aumento da transparência e da qualidade das informações;
- melhoria da fiscalização, do licenciamento ou do monitoramento;
- integração de processos e dados; e
- redução de custos ou melhor aproveitamento dos recursos públicos.

A justificativa, a priorização, o acompanhamento e a avaliação das iniciativas deverão utilizar informações verificáveis. As decisões relevantes deverão ser registradas, incluindo critérios utilizados, responsáveis, data, justificativa e impactos esperados.

As métricas não deverão ser utilizadas apenas para contabilizar entregas, mas também para avaliar fluxo, qualidade, segurança, previsibilidade, adoção e resultados institucionais.

2.6 Integração entre Negócio, Tecnologia e Execução Contratada

O desenvolvimento de software é uma responsabilidade compartilhada entre as áreas de negócio, as unidades de tecnologia, as equipes de governança, a infraestrutura, a fiscalização contratual e, quando aplicável, os fornecedores contratados.

A área demandante é responsável por justificar a necessidade, fornecer conhecimento do negócio, validar requisitos, participar do refinamento, homologar funcionalmente a solução e confirmar o atendimento ao resultado esperado.

As unidades de tecnologia são responsáveis por qualificar a demanda, analisar a solução, estruturar os requisitos, avaliar impactos, coordenar tecnicamente a execução, acompanhar entregas e realizar as validações de sua competência.

Quando a execução for contratada, a empresa deverá estimar, desenvolver, testar, corrigir, versionar, documentar e entregar os produtos conforme o contrato, a Ordem de Serviço, os requisitos, os critérios de aceite e os padrões estabelecidos.

A homologação funcional será realizada pela área demandante com base nos itens, critérios e evidências registrados nas ferramentas institucionais. A fiscalização e a gestão contratual deverão acompanhar a execução, verificar as evidências, formalizar os termos e realizar o recebimento conforme as competências e os instrumentos aplicáveis.

Nenhuma ferramenta ou automação elimina a necessidade de manifestação formal dos responsáveis pelo requisito, pela validação técnica, pela homologação ou pelo recebimento.

2.7 Referenciais Normativos e Metodológicos do PDS

O PDS utiliza referenciais reconhecidos de engenharia de software, análise de negócios, gestão, governança, segurança, qualidade, proteção de dados e contratação pública, conforme sua aplicabilidade ao contexto da SEMA/MT.

Entre os referenciais adotados ou considerados, destacam-se:

- ISO/IEC/IEEE 12207, para processos do ciclo de vida de software;
- ISO/IEC/IEEE 29148, para engenharia de requisitos;
- ISO/IEC 25010, para características de qualidade de produto;
- BABOK, para análise de negócios;
- Scrum, Kanban e práticas de gestão de projetos, para planejamento e gestão do trabalho;
- NIST Secure Software Development Framework — SSDF, OWASP SAMM e OWASP ASVS, para desenvolvimento seguro;
- COBIT e normativos institucionais, para governança de tecnologia e controles;
- Lei Geral de Proteção de Dados Pessoais — LGPD, normas e orientações da Autoridade Nacional de Proteção de Dados — ANPD;
- Legislação de governo digital, contratação pública e demais normas federais e estaduais aplicáveis.

A referência a uma norma, método ou framework não implica declaração automática de conformidade integral. O PDS adota princípios e práticas compatíveis, conforme a necessidade institucional, a criticidade da iniciativa e a capacidade de implementação e verificação.

As versões aplicáveis dos referenciais deverão ser mantidas em catálogo institucional controlado, evitando dependência de versões tecnológicas ou normativas desatualizadas.

3. Estrutura do PDS

Demanda	Triagem	Análise	Priorização	Execução	Testes	Homologação	Implantação	Sustentação

LEITURA ORIENTADA: Este capítulo estabelece o fluxo operacional institucional do Processo de Desenvolvimento de Software da SEMA/MT. O processo abrange a gestão da demanda, a análise e a priorização, a especificação, a execução interna ou contratada, os testes, a homologação, o aceite, o recebimento, a implantação, a sustentação e o encerramento.

O fluxo deve ser aplicado de forma proporcional ao porte, à complexidade, à criticidade, aos riscos e à modalidade de execução de cada iniciativa. Os capítulos técnicos detalham métodos e práticas; este capítulo define a sequência institucional, os pontos de decisão, os registros e as evidências necessários para que uma demanda avance com segurança e rastreabilidade.

3.1 Visão geral do processo institucional

O processo institucional inicia-se com o registro formal da necessidade e termina com o encerramento controlado da demanda, sua transição para sustentação ou a descontinuação da solução. O ciclo não é estritamente linear: retornos para complementação, correção ou replanejamento são permitidos, desde que registrados e justificados.

O macrofluxo de referência é composto pelas seguintes etapas:

- Identificação e registro formal da necessidade;
- Verificação de completude e triagem pela TI;
- Análise preliminar, classificação e decisão de continuidade;
- Elicitação, refinamento e validação dos requisitos;
- Priorização e gestão do backlog;
- Análise da solução, viabilidade, riscos e estimativa;
- Planejamento e autorização da execução interna ou contratada;
- Desenvolvimento, integração contínua e produção de evidências;
- Testes e validação técnica;
- Homologação funcional pela área demandante;
- Aceite, medição e recebimento, quando aplicável;
- Implantação, monitoramento inicial e entrada em operação;
- Sustentação, evolução, encerramento ou descontinuação.

A responsabilidade de cada participante é definida no Capítulo 9. As ferramentas institucionais apoiam o fluxo, mas não substituem as manifestações formais de aprovação, homologação, aceite ou recebimento.

3.1.1 Representação gráfica do fluxo completo

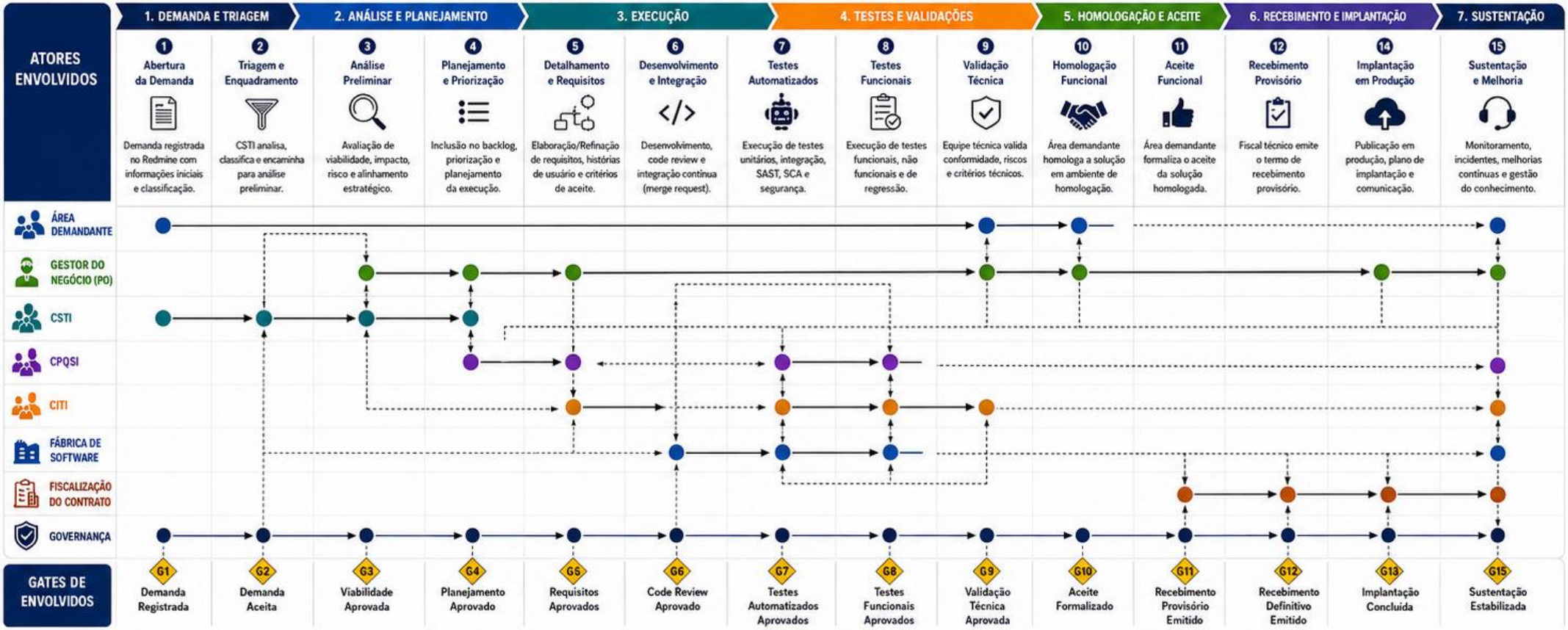
A Figura abaixo apresenta o fluxo ponta a ponta do PDS, desde a abertura da demanda até a sustentação e a melhoria contínua. As raias identificam os participantes; as setas demonstram execução, apoio, consulta ou monitoramento; e os gates representam pontos formais de controle e decisão.

Regra de interpretação: a figura é uma visão consolidada. A numeração oficial, as condições de entrada e saída e as autoridades de aprovação dos gates são as definidas nas Seções 3.14 e 9 deste PDS.

FLUXO COMPLETO DO PDS – PLANO DE DESENVOLVIMENTO DE SISTEMAS – SEMA/MT

Processo ponta a ponta: da demanda à sustentação, com integração entre negócio, TI, fiscalização e fábrica de software

PDS v2.0



LEGENDA

- Executa
- Apoia / Consulta
- Observa / Monitora
- Negócio / Área Demandante
- Governança / TI
- Comitês e Instâncias
- Execução (Fábrica / TII)
- Fiscalização
- Governança e Controle

FERRAMENTAS E FONTES OFICIAIS

Redmine	Fonte primária de demandas, requisitos, histórias, tarefas, testes e releases.
GovFlow	Orquestração de processos, aprovações, workflows e trilhas.
Enterprise Architect	Modelagem de processos, dados, regras e arquitetura de solução.
GitLab	Repositório de código, merge requests, ambientee e CI/CD.
OpenShift	Ambientes, containers, deploy, pipelines e execução.
Observabilidade	Monitoramento, logs, métricas, alertas e tracing.

PRINCIPAIS SAÍDAS / ARTEFATOS

- Formulário de Demanda
- Análise Preliminar
- História de Usuário / Requisitos
- Critérios de Aceite
- Plano de Trabalho / Backlog
- Código Fonte e Testee Request
- Relatórios de Testes (unitários, integração, funcionais, não funcionais, segurança)
- Relatório de Validação Técnica
- Termo de Homologação
- Termo de Aceite
- Termo de Recebimento Provisório
- Termo de Recebimento Definitivo
- Plano de Implantação e Relatório de Implantação
- Relatórios de Incidentes, Problemas e Mudanças
- Indicadores e Métricas

PRINCÍPIOS QUE NORTEIAM O FLUXO

- Transparência e Rastreabilidade
- Qualidade e Segurança desde o início
- Padronização e Reuso
- Foco no Valor Público e Resultados
- Conformidade Legal e Normativa
- Melhoria Contínua
- Integração e Colaboração
- Governança e Accountability

OBSERVAÇÕES IMPORTANTES

- Todas as demandas devem iniciar no Redmine.
- Nenhuma execução deve ocorrer sem análise, planejamento e aprovação das instâncias competentes.
- Testes automatizados e validação técnica são obrigatórios.
- Homologação não se confunde com aceite, e estes não se confundem com recebimento.
- Recebimento definitivo está condicionado ao período de observação e estabilidade da solução em produção.
- Mudanças emergenciais seguirão o fluxo de Gestão de Mudanças e poderão utilizar o processo de Hotfix.
- Todos os artefatos e decisões devem estar registrados nas ferramentas oficiais.

3.2 Princípios operacionais do fluxo

- Rastreabilidade ponta a ponta: toda entrega deve ser relacionada à demanda de origem, aos requisitos, à implementação, aos testes, à versão, à homologação e ao recebimento;
- Fonte oficial da informação: cada tipo de registro deve possuir repositório institucional definido, evitando duplicidade e divergência;
- Proporcionalidade: controles e artefatos devem variar conforme criticidade, risco e complexidade;
- Segregação de funções: especificação, execução, validação, homologação e recebimento devem ser distribuídos de forma compatível com o risco e a modalidade de execução;
- Gestão por evidências: decisões de avanço devem estar apoiadas em registros verificáveis;
- Qualidade e segurança incorporadas: requisitos, testes, segurança, observabilidade e documentação devem ser tratados continuamente;
- Retorno controlado: qualquer retorno de etapa deve indicar motivo, responsável, pendências e nova condição de saída;
- Automação responsável: GovFlow e pipelines podem validar, integrar e gerar evidências, sem substituir decisões institucionais.

3.3 Macroprocesso de gestão da demanda

3.3.1 Identificação e registro formal

Toda iniciativa deve iniciar por registro formal no Redmine ou por integração institucional que gere registro equivalente. Solicitações recebidas por e-mail, reunião, mensagem ou documento externo somente ingressam no fluxo após sua formalização.

O registro inicial deve conter, no mínimo:

- área demandante e Gestor do Negócio;
- problema, necessidade ou oportunidade;
- justificativa e resultado esperado;
- público ou processo afetado;
- urgência e data requerida, quando houver;
- obrigação legal, risco ou vínculo estratégico, quando aplicável;

- anexos, referências e evidências disponíveis;
- indicação preliminar de dados pessoais, integrações ou criticidade.

Saída da etapa: demanda registrada, identificada e apta à verificação de completude.

3.3.2 Verificação de completude e triagem

A CSTI realiza a triagem para verificar a suficiência das informações, a competência da TI, a existência de demanda semelhante, o tipo de atendimento e a necessidade de participação de outras unidades.

A triagem pode resultar em:

- aceite para análise;
- devolução para complementação;
- reclassificação;
- vinculação a demanda existente;
- encaminhamento a outro processo ou unidade;
- arquivamento motivado.

Demandas incompletas não avançam para análise de solução. A devolução deve indicar objetivamente os dados faltantes e o responsável pela complementação.

3.3.3 Classificação da demanda

A demanda deve ser classificada para determinar o fluxo e os controles aplicáveis. A taxonomia institucional deve contemplar, conforme aplicável: novo projeto, evolução, manutenção corretiva, adaptativa ou evolutiva, sustentação, incidente, problema, mudança, integração, API, automação, relatório, BI, ciência de dados, inteligência artificial, dívida técnica, segurança, obrigação legal e atendimento emergencial.

Também deve ser atribuído perfil preliminar de complexidade e criticidade, sujeito a revisão durante a análise.

3.3.4 Análise preliminar e decisão de continuidade

A análise preliminar verifica alinhamento institucional, benefício esperado, dependências conhecidas, riscos iniciais, capacidade disponível e necessidade de aprofundamento. A decisão de continuidade não representa autorização de desenvolvimento; significa apenas que a demanda possui mérito e informações suficientes para refinamento ou avaliação mais detalhada.

3.4 Análise, refinamento e requisitos

3.4.1 Elicitação e compreensão do negócio

A área demandante, o Gestor do Negócio, usuários-chave e a CSTI devem construir entendimento comum do problema e do resultado esperado. Podem ser utilizadas entrevistas, workshops, observação, análise documental, protótipos, BPMN, jornadas, casos de uso e outras técnicas adequadas.

3.4.2 Estruturação dos requisitos

Os requisitos devem ser registrados de maneira clara, verificável e rastreável. O conjunto pode incluir:

- requisitos de negócio e de stakeholders;
- histórias de usuário, épicos e funcionalidades;
- regras de negócio;
- critérios de aceite, preferencialmente em formato Dado-Quando-Então quando adequado;
- requisitos não funcionais de segurança, desempenho, disponibilidade, acessibilidade, interoperabilidade, privacidade, observabilidade e manutenção;
- modelos de processo, dados, integrações e arquitetura, quando aplicáveis;
- restrições, premissas, dependências e riscos.

3.4.3 Histórias de usuário e critérios de aceite

Histórias de usuário são o formato preferencial para itens incrementais do backlog. Devem indicar papel, necessidade e benefício, mas não substituem regras de negócio, requisitos não funcionais ou documentação técnica necessária.

Cada item apto ao desenvolvimento deve possuir critérios de aceite objetivos e testáveis. Critérios vagos, como “funcionar corretamente” ou “ser intuitivo”, devem ser substituídos por condições observáveis.

3.4.4 Validação dos requisitos

O Gestor do Negócio valida o conteúdo funcional. A CSTI valida clareza, consistência, viabilidade preliminar e rastreabilidade. Requisitos complexos ou arquiteturalmente relevantes devem ser relacionados aos modelos mantidos no Enterprise Architect.

3.4.5 Definition of Ready

Um item somente será considerado pronto para planejamento ou execução quando possuir informações suficientes para estimativa e desenvolvimento. A Definition of Ready deve considerar, conforme aplicável: objetivo compreendido, responsável de negócio identificado, critérios de aceite definidos, dependências mapeadas, riscos relevantes avaliados, requisitos não funcionais registrados e dúvidas críticas resolvidas.

3.5 Priorização e gestão do backlog

A priorização deve combinar valor público, urgência, risco, obrigação legal, dependências, esforço, capacidade e impacto. Demandas legais, incidentes críticos e vulnerabilidades graves podem receber tratamento excepcional, desde que a justificativa e a autoridade decisória sejam registradas.

O backlog deve possuir níveis coerentes, tais como portfólio, projeto ou produto, épico, funcionalidade, história, tarefa e subtarefa. A decomposição deve preservar o vínculo com a demanda original.

A ordenação do backlog não será definida exclusivamente pela área técnica nem exclusivamente pela área demandante. Deve resultar de decisão institucional que considere valor funcional, capacidade, riscos e restrições técnicas.

As alterações de prioridade, escopo ou versão devem registrar justificativa, responsável, data e impacto.

3.6 Análise da solução e viabilidade

A análise da solução determina a abordagem mais adequada para atender à necessidade. Deve avaliar, proporcionalmente:

- reutilização, aquisição, integração, configuração, automação ou desenvolvimento;
- arquitetura e aderência a padrões institucionais;
- impactos sobre aplicações, dados, integrações e infraestrutura;
- segurança, privacidade e riscos;
- capacidade técnica e operacional;
- custos de ciclo de vida e sustentabilidade;
- estratégia de migração, coexistência ou descontinuação;

- estimativa de esforço, prazo e recursos;
- modalidade de execução interna, contratada ou compartilhada.

Decisões arquiteturais relevantes devem ser documentadas, justificadas e vinculadas à demanda. A análise pode resultar em aprovação, replanejamento, divisão em incrementos, contratação, protótipo, prova de conceito, suspensão ou não execução.

3.7 Planejamento e acionamento da execução

3.7.1 Execução interna

Na execução interna, a CSTI organiza capacidade, responsáveis, iterações, entregas, riscos e dependências. O planejamento deve identificar o incremento esperado, a versão, os critérios de conclusão e os ambientes necessários.

3.7.2 Execução contratada

A execução por fábrica ou fornecedor depende de instrumento formal compatível, como Ordem de Serviço. Nenhuma atividade contratual deve iniciar sem escopo autorizado, responsáveis identificados e critérios de medição definidos.

A Ordem de Serviço ou instrumento equivalente deve relacionar, conforme aplicável:

- demanda e itens de backlog abrangidos;
- produtos e resultados esperados;
- critérios de aceite e evidências;
- estimativa e unidade de medição;
- prazo, marcos e versão;
- responsabilidades da contratada e da SEMA/MT;
- requisitos técnicos, de segurança e documentação;
- regras de homologação, medição, glosa e recebimento.

3.7.2.1 Estimativa, validação e medição por Unidade de Serviço Técnico

Quando o instrumento contratual adotar a Unidade de Serviço Técnico — UST ou outra unidade de mensuração, a estimativa deverá ser elaborada com base no catálogo de serviços, nos critérios de complexidade, nas condições contratuais e nos produtos efetivamente necessários à execução da demanda.

A estimativa apresentada pela contratada deverá conter memória de cálculo suficiente para permitir sua análise, incluindo, conforme aplicável:

a) identificação da demanda, dos requisitos, das histórias de usuário e dos itens de backlog abrangidos;

b) produtos ou serviços do catálogo contratual utilizados;

c) quantidade, unidade, nível de complexidade e respectiva justificativa;

d) premissas, restrições, dependências e riscos considerados;

e) atividades de desenvolvimento, testes, documentação, implantação, sustentação ou transferência de conhecimento incluídas;

f) prazo estimado e composição do esforço;

g) indicação de componentes existentes que serão reutilizados;

h) identificação de eventual sobreposição, dependência ou duplicidade entre os itens estimados; e

i) valor total estimado e saldo contratual correspondente.

A análise da estimativa deverá verificar sua aderência ao escopo, aos requisitos aprovados, ao catálogo contratual, ao histórico de serviços semelhantes, à complexidade técnica, à proporcionalidade do esforço e às evidências apresentadas.

A aprovação da estimativa não poderá ocorrer apenas com base no valor global informado pela contratada. Divergências deverão ser registradas e submetidas a esclarecimento, complementação, revisão ou negociação técnica antes da emissão da Ordem de Serviço.

A análise poderá envolver a CSTI, o Fiscal Técnico, especialistas designados e outras unidades competentes, conforme a natureza e a complexidade da demanda. Quando não houver capacidade técnica suficiente para validar determinada estimativa, essa limitação deverá ser formalmente registrada e encaminhada para apoio especializado, sem que a ausência de conhecimento resulte em aprovação automática.

A medição deverá considerar os produtos efetivamente executados, entregues, validados e aceitos, observando os critérios contratuais. Itens não executados, incompletos, recusados, não rastreáveis, sem evidências ou em desacordo com os critérios de aceite não deverão ser medidos como integralmente concluídos.

Alterações de escopo, complexidade, quantidade ou premissas após a emissão da Ordem de Serviço deverão ser formalmente avaliadas e autorizadas antes de produzirem efeito sobre a medição, o prazo ou o valor.

A estimativa aprovada, sua memória de cálculo, as manifestações técnicas, as divergências, as revisões e a medição final deverão permanecer vinculadas à demanda e à Ordem de Serviço nos repositórios institucionais definidos.

3.7.3 Planejamento iterativo

O uso de Scrum, Kanban ou outra abordagem não altera as responsabilidades institucionais. Os papéis ágeis serão designados por iniciativa. Sprints e cerimônias devem produzir decisões e registros úteis, evitando documentação ritualística sem valor.

3.8 Desenvolvimento e integração contínua

A execução técnica transforma itens prontos do backlog em incrementos versionados. O trabalho deve ocorrer em repositórios Git/GitLab institucionais, com associação entre itens do Redmine, branches, commits, merge requests, pipelines e versões.

Durante o desenvolvimento, devem ser observados:

- padrões de codificação e arquitetura;
- revisão por pares ou mecanismo equivalente;
- controle de dependências e segredos;
- testes automatizados adequados;
- integração contínua;
- documentação técnica viva;
- evidências produzidas automaticamente sempre que possível;
- atualização do status e das pendências no Redmine.

A contratada é responsável pela qualidade de sua implementação e pela correção das não conformidades atribuíveis à entrega. A CSTI acompanha e valida, sem assumir a execução material da fábrica.

3.9 Testes e validação técnica

A etapa de testes verifica o atendimento aos requisitos funcionais e não funcionais e a aptidão da entrega para homologação. Deve combinar testes da equipe executora, testes automatizados, avaliações de qualidade, segurança e validação técnica da SEMA/MT.

Os controles podem incluir testes unitários, integração, sistema, regressão, desempenho, acessibilidade, segurança, SAST, SCA, DAST, análise de contêiner e infraestrutura como código, conforme criticidade e aplicabilidade.

Defeitos e vulnerabilidades devem ser registrados, classificados e vinculados à entrega. O avanço para homologação depende do atendimento aos quality gates definidos ou de exceção formal com risco residual aceito pela autoridade competente.

3.10 Homologação funcional

A homologação funcional é realizada pela área demandante, sob responsabilidade do Gestor do Negócio e com participação dos homologadores designados. A CSTI prepara a versão, o ambiente, os itens de homologação e as evidências técnicas.

A homologação deve registrar, para cada item: versão testada, cenário, resultado esperado, resultado obtido, evidência, responsável, data e situação.

Resultados possíveis:

- aprovado;
- aprovado com ressalvas sem impedimento;
- reprovado e devolvido para correção;
- bloqueado por impedimento externo;
- cancelado ou substituído por decisão formal.

A homologação parcial somente será admitida quando o escopo liberado for identificável, utilizável e não comprometer segurança, integridade ou continuidade.

3.11 Aceite, medição e recebimento

A validação técnica, a homologação funcional, o aceite e o recebimento são atos distintos. A conclusão de testes técnicos não substitui a homologação do negócio; a homologação não substitui a verificação contratual.

Quando houver execução contratada, o processo deve reunir:

- parecer ou validação técnica;
- registros de homologação e aceite funcional;
- produtos e evidências previstos;
- medição do esforço ou dos produtos;
- avaliação de SLA e níveis de serviço;
- registro de não conformidades e glosas, quando aplicáveis;
- recebimento provisório e definitivo conforme o contrato;
- autorização de faturamento pela autoridade competente.

O Redmine deve manter os vínculos com os termos e documentos administrativos registrados nos sistemas oficiais competentes.

3.12 Implantação e entrada em operação

A implantação deve ser planejada e autorizada com base na criticidade da solução. O plano deve contemplar, conforme aplicável: janela, responsáveis, pacote de release, scripts, migração de dados, backup, rollback, comunicação, indisponibilidade prevista, smoke tests e monitoramento inicial.

A decisão de prosseguir, interromper ou reverter deve possuir autoridade definida. Implantações manuais e emergenciais devem ser registradas e posteriormente regularizadas no fluxo.

Após a entrada em produção, a equipe responsável deve acompanhar disponibilidade, erros, desempenho, segurança e comportamento dos fluxos críticos durante período compatível com o risco.

3.13 Sustentação, evolução e encerramento

A transição para sustentação deve definir responsáveis, canais, níveis de serviço, documentação, monitoramento, base de conhecimento e tratamento de incidentes.

Correções e evoluções relevantes devem originar novos itens rastreáveis, preservando vínculo com a versão e o incidente ou demanda que lhes deu origem.

O encerramento requer, conforme aplicável:

- entrega e homologação concluídas;

- recebimentos formalizados;
- documentação atualizada;
- pendências residuais registradas;
- lições aprendidas e riscos remanescentes;
- responsáveis pela operação definidos;
- backlog residual ou roadmap atualizado;
- arquivamento dos vínculos e evidências.

A descontinuação de sistemas deve possuir plano próprio para dados, integrações, usuários, retenção, segurança e desligamento de infraestrutura.

3.14 Gates do processo

Os gates são pontos de controle que impedem o avanço de demandas sem condições mínimas. O nível de rigor deve ser proporcional ao perfil da iniciativa.

Gate	Condição de entrada	Condição de saída / decisão
G1 - Pronta para análise	Demanda formalmente registrada	Informações mínimas completas e responsável de negócio identificado.
G2 - Pronta para priorização	Triagem e análise preliminar concluídas	Valor, urgência, risco, dependências e escopo inicial conhecidos.
G3 - Pronta para execução	Requisitos e solução suficientemente definidos	Itens atendem à Definition of Ready; estimativa e modalidade de execução aprovadas.
G4 - Pronta para testes	Implementação integrada e versionada	Build disponível, revisão concluída e testes básicos aprovados.
G5 - Pronta para homologação	Validação técnica e quality gates atendidos	Versão, ambiente, critérios e evidências disponibilizados.
G6 - Pronta para produção	Homologação e aprovações concluídas	Plano de implantação, rollback, segurança e operação validados.
G7 - Pronta para recebimento	Produtos implantados ou entregues conforme instrumento	Pareceres, medição, SLA, aceite e documentos reunidos.
G8 - Pronta para encerramento	Recebimentos e transição concluídos	Documentação, pendências, operação e lições aprendidas registradas.

3.15 Estados e transições no Redmine

O Redmine deve representar o fluxo institucional por estados e transições controladas. A parametrização poderá evoluir sem alteração integral do PDS, desde que preserve o significado dos macroestados e as responsabilidades aprovadas.

Macroestado	Finalidade	Exemplos de transição
Registrada	Formalizar a necessidade	Para complementação ou triagem.
Em triagem	Verificar completude e classificação	Para análise, devolvida, duplicada ou arquivada.
Em análise/refinamento	Detalhar necessidade, requisitos e solução	Para validação do negócio, priorização ou suspensão.
Priorizada / Backlog	Aguardar planejamento conforme ordem institucional	Para planejamento, replanejamento ou cancelamento.
Planejada / Autorizada	Definir versão, capacidade ou OS	Para execução.
Em execução	Desenvolver e produzir evidências	Para validação técnica ou bloqueio.
Em validação técnica	Verificar qualidade e conformidade	Para correção ou homologação.
Em homologação	Validar funcionalmente	Para correção, aceite ou bloqueio.
Pronta para implantação	Aguardar autorização e janela	Para produção ou retorno.
Em produção / Monitoramento	Acompanhar estabilização	Para sustentação ou rollback.
Em recebimento	Formalizar medição e recebimentos	Para encerramento ou pendência contratual.
Encerrada	Concluir demanda com rastreabilidade	Reabertura somente mediante justificativa e autorização.

Transições críticas devem exigir campos obrigatórios, responsáveis e evidências. O GovFlow poderá validar essas condições e impedir avanços inconsistentes.

3.16 Rastreabilidade entre ferramentas

A rastreabilidade deve permitir reconstruir a história completa da entrega. O vínculo mínimo esperado é:

Demanda no Redmine → requisitos e modelos → item de backlog → branch/commit/merge request → pipeline e testes → versão/release → homologação → implantação → parecer, medição e recebimento.

Informação	Fonte oficial principal	Vínculo esperado
Demanda, backlog, workflow e aprovações	Redmine	Identificadores únicos e relações entre itens.
Processos, arquitetura, UML e modelos de dados	Enterprise Architect	Referência ou identificador registrado no Redmine.
Código, IaC e documentação versionável	Git/GitLab	Commits e merge requests vinculados aos itens.
Automação e validação de regras	GovFlow	Registros de execução e retorno ao Redmine.
Builds, testes e scans	Pipeline CI/CD	Resultados associados à versão e ao item.
Documentos administrativos e contratuais	Sistema oficial competente	Número do processo, documento ou termo referenciado no Redmine.

3.17 Fluxos alternativos e exceções

O processo deve prever, registrar e controlar situações que não seguem o caminho principal.

Situação	Tratamento mínimo
Demanda incompleta	Devolver com lista objetiva de pendências e responsável pela complementação.
Duplicidade	Relacionar à demanda existente e registrar decisão de consolidação ou encerramento.
Cancelamento	Registrar motivo, autoridade, impactos e tratamento de artefatos já produzidos.
Emergência ou incidente crítico	Aplicar fluxo acelerado com controles mínimos, regularização posterior e análise de causa.
Mudança de escopo	Avaliar impacto em prazo, custo, risco, versão e OS; obter nova aprovação.
Bloqueio externo	Registrar impedimento, responsável, prazo de reavaliação e impacto.
Falha na homologação	Criar ou vincular defeitos, retornar à execução e preservar evidências da reprovação.
Exceção de quality gate	Exigir justificativa, risco residual, prazo de correção e aceite da autoridade competente.
Rollback	Executar plano, registrar causa, impacto, evidências e decisão sobre nova implantação.
Execução sem fábrica	Aplicar os mesmos princípios de rastreabilidade, qualidade, segurança e segregação compatíveis.
Reabertura de item encerrado	Exigir justificativa e decisão formal; preferir nova demanda quando houver novo escopo.

3.18 Artefatos e registros mínimos

Os artefatos devem ser produzidos conforme a matriz de aplicabilidade do PDS. Sempre que a informação estiver estruturada em ferramenta oficial, não é necessário duplicá-la em documento estático.

Categoria	Registros mínimos
Demanda	Registro formal, responsável, justificativa, classificação e decisão de triagem.
Requisitos	Histórias ou especificações, regras, critérios de aceite e validação do negócio.
Solução	Análise técnica, riscos, estimativa e decisões arquiteturais relevantes.
Execução	Backlog planejado, responsáveis, versão ou OS, código e evidências.
Qualidade	Testes, defeitos, scans, validação técnica e exceções.
Homologação	Cenários, resultados, evidências e decisão funcional.
Implantação	Plano, autorização, release, rollback e monitoramento inicial.
Contrato	Medição, SLA, pareceres, glosas e termos de recebimento.
Encerramento	Pendências, documentação, transição, lições e decisão final.

3.19 Melhoria contínua do processo

Os dados do Redmine, GovFlow, repositórios, pipelines, operação e contratos devem alimentar indicadores de fluxo, qualidade, segurança, previsibilidade e resultados. Gargalos, retornos frequentes, defeitos recorrentes e exceções devem gerar ações de melhoria no PDS, nas ferramentas, na capacitação ou nos contratos.

Alterações de workflow, campos, gates ou automações devem ser testadas em ambiente de homologação, documentadas, versionadas e comunicadas aos participantes antes da aplicação em produção.

Nome do Evento	Descrição do Evento	Atividades do Evento	Participantes do Evento
Sprint	Ciclo de trabalho de tempo fixo (1 a 4 semanas), que contém todos os demais eventos do Scrum.	Execução do trabalho planejado. Criação de incrementos. Adaptação contínua do plano. Revisão e melhoria do processo.	*Product Owner.* *Scrum Master.* Desenvolvedores.
Sprint Planning	Evento que inicia o *Sprint* e define o objetivo, os itens do *backlog* selecionados e o plano de execução.	Definição do *Sprint Goa*l. Seleção de itens do *Product Backlog*. Planejamento técnico do trabalho a ser realizado	*Product Owner.* *Scrum Master.* Desenvolvedores.
Daily Scrum	Reunião diária de 15 minutos focada na inspeção do progresso e no planejamento para as próximas 24 horas.	Compartilhamento do progresso. Identificação de impedimentos. Atualização do *Sprint Backlog*. Planejamento do próximo dia de trabalho.	Desenvolvedores. **Obs**.: *Product Owner* e *Scrum Master* podem participar se forem desenvolvedores.
Sprint Review	Evento de inspeção do incremento desenvolvido e adaptação do *Product Backlog* com base no *feedback*.	Demonstração do incremento realizado. Coleta de *feedback* dos *stakeholders*. Atualização das prioridades no *Product Backlog*.	*Product Owner.* *Scrum Master.* Desenvolvedores. *Stakeholders.*
Sprint Retrospective	Evento final do Sprint focado na melhoria contínua do processo, equipe e ferramentas utilizadas.	Avaliação do que funcionou e o que pode melhorar. Identificação de ações corretivas. Planejamento de melhorias para o próximo Sprint.	*Product Owner.* *Scrum Master.* Desenvolvedores.

Metodologia	Pontos-Chave	Benefícios	Aplicação Prática
OWASP SAMM (Software Assurance Maturity Model)	Modelo de maturidade para segurança em software, dividido em domínios (Governança, Construção, Verificação e Operações).	Fornece diagnóstico do nível atual de maturidade em segurança; permite evolução gradual com metas claras.	Avaliar a maturidade das equipes de TI e segurança; identificar prioridades de investimento (ex.: testes automatizados ou análise de riscos).
NIST SP 800-53 / SP 800-64	Catálogo de controles técnicos e diretrizes de ciclo de vida de sistemas.	Referência global em segurança; estrutura clara para requisitos mínimos de proteção.	Definir controles mínimos obrigatórios (ex.: criptografia, segregação de funções, auditoria de logs) em sistemas ambientais críticos.
ISO/IEC 27001 e 27005	Padrão internacional para gestão de segurança da informação e análise de riscos.	Normas auditáveis; alinhamento com sistemas de gestão da informação (SGSI).	Estruturar processos de análise de riscos institucionais; atender a exigências de auditoria e órgãos de controle.
CI/CD Seguro (DevSecOps)	Integração de segurança em pipelines automatizados (SAST, DAST, SCA, testes de conformidade).	Automação contínua; agilidade e redução de erros humanos; aplicável em qualquer ciclo iterativo.	Configurar pipelines em Git/Redmine; aplicar verificações automáticas em cada commit; gerar evidências de segurança rastreáveis.

Atividade BPMN	Controle aplicado	Ferram. / integração	Resp.	Evidência Gerada
Login do Solicitante	Autenticação multifator (MFA)	Camunda + Keycloak (OIDC/SAML)	Equipe TI (CSTI)	Log de autenticação no IdP
Upload de Documentos	Validação de assinatura digital ICP-Brasil	Módulo de verificação integrado	CSTI	Relatório de integridade do documento
Análise Técnica	Controle de acesso por perfil (RBAC)	LDAP/AD integrado ao Camunda	CSTI	Registro de execução com ID do usuário
Aprovação Final	Dupla validação (Four Eyes Principle)	Regras BPMN + Camunda Engine	CSTI	Log de dupla aprovação
Emissão da Licença	Registro de auditoria criptografado	Banco de auditoria + ELK	CPQSI	Trilha de auditoria assinada digitalmente

Risco Identificado	Prob.	Impacto	Controle implementado	Status
Acesso indevido de usuário sem perfil autorizado	Alta	Alto	RBAC integrado ao LDAP/AD	Ativo
Documentos falsificados ou adulterados	Média	Alto	Validação de assinatura digital ICP-Brasil	Ativo
Aprovação por um único servidor sem supervisão	Média	Alto	Dupla validação (Four Eyes Principle)	Ativo
Alteração não registrada em histórico de processo	Baixa	Médio	Logs assinados digitalmente e enviados ao ELK	Ativo

Atividade/Controle	Resp. direto	Nível de Governança	Ferram. / integração	Evidência/Entrega
Configuração e manutenção de pipelines	CSTI	Operacional	Git, CI/CD, SonarQube, Trivy	Logs de execução, relatórios de build
Correção de vulnerabilidades em código	Equipes de Desenvolvimento	Operacional	Git, Redmine	Commit vinculado à issue de segurança
Definição de políticas e padrões	CPQSI	Tático	Normas internas, checklists LGPD	Políticas publicadas, relatórios validados
Validação de relatórios de segurança	CPQSI	Tático	Redmine, ELK, Grafana	Relatórios de conformidade revisados
Acompanhamento de indicadores estratégicos	NGER	Estratégico	Dashboards, Redmine, Grafana	Painéis de resultados, atas de reuniões
Auditoria de conformidade	Órgãos de Controle	Estratégico	Redmine, ELK, relatórios de auditoria	Pareceres de conformidade, recomendações

Indicador	Meta / SLA	Resp.	Ferramenta	Period.	Evidência
% de builds interrompidos por falhas de segurança	≤ 5%	CSTI / Devs	Git, CI/CD, SonarQube, Trivy	Semanal	Relatórios de build
MTTR (tempo médio para corrigir vulnerabilidades)	≤ 72h	Devs / CPQSI	Redmine, Git	Mensal	Issues resolvidas, commits vinculados
Disponibilidade de sistemas críticos (SLA)	≥ 99,5%	CSTI	Zabbix, Grafana	Diário/Mensal	Dashboards de disponibilidade
% de requisitos LGPD implementados	100% em sistemas ativos	CPQSI	Redmine, Camunda, relatórios LGPD	Trimestral	Relatórios de conformidade
MTTD (tempo médio para detectar incidentes)	≤ 1h	CSTI / CPQSI	ELK, Zabbix, WAF	Mensal	Logs de incidentes
% de incidentes tratados no prazo do SLA	≥ 95%	CSTI / CPQSI	Redmine, ELK, Grafana	Mensal	Relatórios de resposta

Issue	Descrição	Critérios de segurança	Evidências	Status
#254 – Upload de Documentos	Implementar upload de documentos do empreendedor	Assinatura digital ICP-Brasil obrigatória; validação de integridade SHA-256	Log de validação; Relatório de teste automatizado	Concluído
#310 – Análise Técnica	Desenvolver módulo para análise de documentos	Acesso restrito por RBAC; registro de log assinado digitalmente	Print de auditoria no Camunda; Log no ELK	Em andamento
#412 – Emissão de Licença	Automatizar emissão de licença após aprovação técnica e jurídica	Dupla validação (Four Eyes Principle); autenticação multifator	Registro no Redmine + Log de aprovação no sistema	Pendente
#501 – Vulnerabilidade detectada CI	Correção de falha crítica em biblioteca de geoprocessamento identificada no CI	Patch aplicado em até 72h; verificação SCA em pipeline	Commit vinculado à issue; Relatório do Trivy	Concluído

4. Metodologias e Práticas de Engenharia

LEITURA ORIENTADA: Este capítulo estabelece como métodos de gestão, práticas de engenharia, automação e decisões arquiteturais devem ser selecionados e aplicados no Processo de Desenvolvimento de Software da SEMA/MT. Ele complementa o fluxo institucional definido no Capítulo 3, sem repetir suas etapas, papéis, gates ou registros.

As práticas descritas deverão ser adotadas de forma proporcional ao porte, à complexidade, à criticidade, aos riscos e à modalidade de execução da iniciativa. A escolha de um método ou ferramenta não altera as competências regimentais, contratuais ou decisórias definidas no Capítulo 9.

4.1 Princípios de adaptação do método

O PDS não impõe uma única metodologia para todas as iniciativas. A abordagem deverá ser escolhida conforme a natureza do trabalho, a previsibilidade do escopo, o grau de inovação, a urgência, as dependências, a capacidade da equipe, a modalidade de contratação e a necessidade de controle institucional.

a) adequação ao contexto: o método deve servir ao trabalho e não o contrário;

b) transparência: backlog, prioridades, bloqueios, decisões e progresso devem ser visíveis;

c) entrega incremental: sempre que viável, o valor deve ser entregue em parcelas verificáveis;

d) limitação do trabalho em andamento: a capacidade deve ser respeitada para reduzir filas e retrabalho;

e) inspeção e adaptação: indicadores, feedback e lições aprendidas devem orientar ajustes;

f) rastreabilidade: decisões, alterações e evidências devem permanecer vinculadas à demanda;

g) proporcionalidade: demandas simples não devem receber o mesmo peso documental de sistemas críticos; e

h) independência tecnológica: regras institucionais não devem depender de uma ferramenta específica.

4.2 Seleção da abordagem de gestão e execução

A abordagem deverá ser registrada no Redmine ou no instrumento de planejamento correspondente, com justificativa suficiente para permitir auditoria e revisão posterior. A combinação de práticas é permitida quando favorecer o controle e a entrega.

Contexto predominante	Abordagem recomendada	Observações
Produto com evolução incremental e equipe estável	Scrum ou modelo iterativo	Adequado quando há objetivo de produto, backlog priorizado e ciclos regulares.
Manutenção, sustentação e fluxo contínuo	Kanban	Adequado para demandas variáveis, incidentes e necessidade de limitar trabalho em andamento.
Evolução com fluxo contínuo e cadências periódicas	Scrumban	Combina planejamento e revisão em cadências com gestão visual contínua.
Projeto com marcos legais, contratuais ou entregas formais	Modelo híbrido	Combina planejamento preditivo, gates institucionais e execução incremental.
Correção crítica ou emergência	Fluxo emergencial controlado	Exige justificativa, autorização, registro, testes proporcionais e regularização posterior.

A escolha de Scrum não implica que a CSTI seja automaticamente Product Owner nem que a CPQSI seja automaticamente Scrum Master. Os papéis de produto, facilitação e execução serão designados por iniciativa, preservadas as responsabilidades institucionais estabelecidas no Capítulo 9.

4.3 Métodos ágeis e fluxo contínuo

Os métodos ágeis poderão ser utilizados para organizar o trabalho em ciclos curtos, promover colaboração entre negócio e tecnologia, reduzir riscos de entendimento e antecipar validações. Sua adoção deverá produzir transparência e aprendizado, e não apenas cerimônias.

No Scrum, quando adotado, deverão existir objetivo de produto ou de entrega, backlog ordenado, planejamento do ciclo, acompanhamento frequente, revisão do incremento e retrospectiva. No Kanban, deverão existir fluxo visual, políticas explícitas, limites de trabalho em andamento, gestão de bloqueios e medição do tempo de fluxo.

Em qualquer abordagem, o Redmine será utilizado como registro operacional do trabalho, salvo exceção formalmente aprovada. Quadros auxiliares podem ser utilizados, desde que não criem uma fonte paralela ou divergente de informação.

4.4 Eventos, cadências e gestão visual

Eventos e cadências deverão existir somente quando contribuírem para decisão, coordenação, inspeção ou aprendizado. Não é obrigatória a produção de atas extensas para todas as reuniões. Decisões, impedimentos, responsáveis e prazos relevantes deverão ser registrados de forma objetiva na demanda, issue, versão ou documento oficial correspondente.

a) planejamento: define objetivo, escopo do ciclo, capacidade e riscos;
b) acompanhamento: torna visível o progresso, os bloqueios e as dependências;
c) refinamento: melhora clareza, testabilidade, estimativa e prontidão dos itens;
d) revisão ou demonstração: apresenta o incremento e coleta feedback;
e) retrospectiva: identifica melhorias no processo e ações responsáveis; e
f) reunião de governança ou contratual: trata prioridades, riscos, medições, decisões e providências formais.

4.5 Gestão de backlog, limites de trabalho e previsibilidade

O backlog deverá representar o trabalho autorizado e priorizado, mantendo vínculo com a demanda original, os requisitos, os critérios de aceite e a versão ou entrega planejada. Itens sem clareza mínima não deverão entrar em execução.

A equipe deverá explicitar a capacidade disponível, os limites de trabalho em andamento, as dependências e os bloqueios. O acúmulo de itens iniciados e não concluídos deve ser tratado como risco de fluxo. Previsões deverão ser baseadas em capacidade, histórico e incerteza, evitando compromissos sem fundamento técnico.

Alterações relevantes de prioridade ou escopo deverão ser registradas com justificativa, autoridade decisória e análise de impacto, conforme o Capítulo 3.

4.6 DevSecOps e automação do ciclo de entrega

DevSecOps é a integração contínua entre desenvolvimento, segurança e operação, com automação, colaboração, feedback rápido e responsabilidade compartilhada. Sua aplicação deverá acompanhar o fluxo: requisito, código, integração, testes, verificações de segurança, empacotamento, implantação, observabilidade e aprendizado.

A segurança e a qualidade devem ser incorporadas desde o refinamento da demanda, e não adicionadas apenas ao final. Os controles específicos, critérios de severidade e responsabilidades são definidos no Capítulo 7; as ferramentas homologadas são tratadas no Capítulo 10; e os indicadores são consolidados no Capítulo 13.

a) requisitos de segurança e privacidade definidos conforme risco;
b) versionamento de código, configuração e infraestrutura;
c) revisão por pares e proteção de branches;
d) testes automatizados em níveis adequados;
e) análise estática de código (SAST);
f) análise de dependências e componentes (SCA);
g) análise dinâmica de aplicações (DAST), quando aplicável;
h) detecção de segredos e credenciais expostas;
i) análise de imagens de contêiner e infraestrutura como código;
j) geração ou manutenção de inventário de componentes e SBOM, quando exigido;
k) implantação automatizada e controlada; e
l) observabilidade, resposta a incidentes e retroalimentação do backlog.

4.7 Integração e entrega contínuas

Integração contínua — CI — corresponde à prática de integrar alterações frequentes ao repositório principal mediante validações automatizadas. Entrega ou implantação contínua — CD — corresponde à preparação e, quando autorizado, à promoção controlada de versões entre ambientes.

Os pipelines deverão ser versionados, reproduzíveis e auditáveis. Devem registrar, conforme aplicável, compilação, testes, análises de qualidade e segurança, geração de artefatos, assinatura ou identificação da versão, promoção entre ambientes e resultado da implantação.

A automação não substitui autorizações formais de homologação, implantação, aceite ou recebimento. O pipeline pode comprovar um controle técnico, mas a decisão institucional permanece com o papel competente.

4.8 Quality gates e política de exceções

Quality gates são critérios objetivos que determinam se uma entrega pode avançar no fluxo. Eles deverão ser proporcionais à criticidade e integrados aos gates institucionais do Capítulo 3.

Dimensão	Exemplos de verificação	Resultado esperado
Código	compilação, lint, análise estática, revisão por pares	sem falha bloqueante e com evidências disponíveis
Testes	unitários, integração, regressão e cobertura adequada ao risco	cenários críticos aprovados
Segurança	SAST, SCA, DAST, segredos, contêiner e IaC	sem vulnerabilidade impeditiva não tratada
Arquitetura	aderência a padrões, integrações e requisitos não funcionais	decisões relevantes registradas
Operação	configuração, observabilidade, backup, rollback e capacidade	implantação reproduzível e reversível
Documentação	instruções técnicas, versão, evidências e vínculos	informações suficientes para operar, manter e auditar

Exceções deverão ser raras, justificadas e temporárias. Devem conter risco, impacto, controles compensatórios, responsável, autoridade que aprovou, prazo de regularização e evidência de encerramento. O GovFlow poderá validar campos e regras de exceção, mas não substituir a aceitação formal do risco.

4.9 Princípios de arquitetura de software

A arquitetura deverá apoiar os objetivos institucionais e os atributos de qualidade necessários à solução. Decisões arquiteturais não devem ser tomadas apenas por preferência tecnológica.

a) alinhamento ao negócio e ao valor público;

b) simplicidade compatível com o problema;

c) segurança e privacidade desde a concepção;

d) interoperabilidade e uso de padrões abertos, quando aplicável;

e) modularidade, coesão e baixo acoplamento;

f) observabilidade, operabilidade e capacidade de suporte;

g) manutenibilidade, testabilidade e evolução;

h) resiliência, disponibilidade e continuidade proporcionais à criticidade;

i) portabilidade e redução de dependência tecnológica indevida;

j) gestão responsável de dados; e

k) custo total de propriedade e sustentabilidade ao longo do ciclo de vida.

4.10 Estilos e padrões arquiteturais

A seleção de estilos e padrões deverá considerar o contexto e os requisitos arquiteturalmente relevantes. Nenhum estilo será considerado superior de forma universal.

Opção	Uso adequado	Riscos e cuidados
Monólito modular	soluções com domínio integrado, equipe menor e necessidade de simplicidade operacional	evitar acoplamento excessivo e ausência de fronteiras internas
Arquitetura em camadas	sistemas corporativos com separação clara de responsabilidades	evitar camadas meramente cerimoniais e dependências invertidas
Microsserviços	domínios independentes, escalabilidade seletiva e equipes com maturidade operacional	complexidade distribuída, observabilidade, consistência e custo de operação
Orientada a eventos	integração assíncrona, desacoplamento e processamento de eventos	governança de esquemas, rastreabilidade, idempotência e tratamento de falhas
Hexagonal ou Clean Architecture	necessidade de isolamento do domínio e testabilidade	não transformar abstrações em excesso sem benefício concreto

Padrões de design poderão ser utilizados para resolver problemas recorrentes, desde que sua aplicação seja justificada e não introduza complexidade desnecessária.

4.11 Processo de decisão arquitetural

Decisões arquiteturais relevantes deverão seguir processo explícito: identificar contexto e problema; levantar alternativas; avaliar impactos, riscos e custos; consultar especialistas; decidir; registrar justificativa; e revisar quando as premissas mudarem.

As decisões deverão considerar requisitos não funcionais, dados, integração, segurança, privacidade, infraestrutura, operação, manutenção, contratação, capacidade interna e reversibilidade. Projetos de maior impacto deverão manter registros de decisão arquitetural — ADRs ou equivalente — e modelos no Enterprise Architect, quando aplicável.

O vínculo entre decisão, demanda e requisito deverá ser mantido por referência entre o Enterprise Architect e o Redmine, sem duplicar desnecessariamente o conteúdo.

4.12 Seleção de tecnologias e frameworks

Tecnologias e frameworks deverão ser avaliados por critérios objetivos e por sua aderência à arquitetura institucional. Listas de tecnologias autorizadas ou preferenciais deverão ser mantidas em catálogo versionado e atualizável, evitando tornar o PDS obsoleto.

a) adequação funcional e técnica;
b) maturidade, estabilidade e ciclo de suporte;
c) segurança e histórico de vulnerabilidades;
d) licenciamento, custos e restrições de uso;
e) interoperabilidade e compatibilidade com a plataforma institucional;
f) capacidade da equipe e disponibilidade de profissionais;
g) qualidade da documentação e do ecossistema;
h) desempenho e escalabilidade necessários;
i) facilidade de testes, observabilidade e automação;
j) portabilidade, reversibilidade e risco de aprisionamento tecnológico; e
k) custo total de desenvolvimento, operação, manutenção e evolução.

A matriz de decisão tecnológica deverá registrar critérios, pesos quando aplicáveis, alternativas, evidências, riscos e recomendação. A escolha final deverá ser aprovada pela autoridade técnica competente conforme o Capítulo 9.

4.13 Modernização e sistemas legados

A modernização deverá partir de diagnóstico do sistema, do valor de negócio, dos riscos, da obsolescência, da capacidade de manutenção, das dependências e dos custos. Reescrever integralmente não será a opção padrão.

As estratégias poderão incluir manutenção controlada, atualização de componentes, encapsulamento por APIs, refatoração, modularização, replatforming, rehosting, substituição gradual, estrangulamento do legado ou descontinuação.

A estratégia deverá prever coexistência, migração de dados, compatibilidade, testes, continuidade, reversão, comunicação, capacitação e encerramento seguro do sistema anterior.

4.14 Documentação e governança da arquitetura

A documentação arquitetural deverá ser suficiente para compreender, operar, evoluir e auditar a solução. Deve priorizar modelos úteis e atualizados, evitando produção documental sem uso real.

a) contexto e objetivos da solução;

b) requisitos arquiteturalmente relevantes;

c) visão de componentes, integrações, dados e implantação;

d) decisões arquiteturais e justificativas;

e) riscos, restrições e dívida técnica relevante;

f) padrões e tecnologias adotados;

g) requisitos operacionais, de segurança e observabilidade; e

h) vínculos com demandas, requisitos, repositórios e versões.

O Enterprise Architect será o repositório preferencial para modelos arquiteturais e de processo definidos como aplicáveis. O Redmine manterá os vínculos operacionais e decisórios; o Git/GitLab armazenará documentação versionável próxima ao código; e o GovFlow poderá apoiar sincronização, validação e relatórios.

4.15 Aplicabilidade proporcional das práticas

A profundidade das práticas deverá variar conforme a classificação da iniciativa. A matriz abaixo é orientativa e será detalhada no catálogo institucional de artefatos.

Prática	Demanda simples	Evolução controlada	Projeto corporativo	Sistema crítico
Método de gestão	fluxo simplificado	Kanban, Scrum ou híbrido	abordagem formalmente definida	abordagem formal com governança reforçada
Pipeline CI/CD	quando houver código	recomendado	obrigatório	obrigatório com controles reforçados
Modelagem arquitetural	dispensável ou simplificada	conforme impacto	obrigatória	obrigatória com revisão independente
ADRs	quando houver decisão relevante	recomendado	obrigatório para decisões relevantes	obrigatório e sujeito a revisão
SAST/SCA	conforme risco	recomendado	obrigatório	obrigatório
DAST e testes especializados	conforme exposição	conforme risco	conforme risco	obrigatório conforme plano de segurança
Observabilidade e rollback	básicos	proporcionais	obrigatórios	obrigatórios e testados

A dispensa ou simplificação de uma prática não elimina a necessidade de rastreabilidade, responsabilidade e evidência mínima. Iniciativas classificadas como críticas poderão receber controles adicionais definidos nos Capítulos 7, 10 e 13.

5. Desenvolvimento e Construção de Software

Demanda	Requisito	História	Commit/MR	Pipeline	Release	Homologação	Recebimento

> **LEITURA ORIENTADA:** Este capítulo estabelece os padrões operacionais para transformar itens autorizados do backlog em incrementos de software verificáveis, versionados, testáveis, seguros e rastreáveis. Ele complementa o fluxo institucional definido no Capítulo 3 e as práticas metodológicas, DevSecOps e arquiteturais definidas no Capítulo 4.

As regras aplicam-se ao desenvolvimento interno e à execução contratada. Sua profundidade deverá ser proporcional ao porte, à complexidade, à criticidade, ao risco e à modalidade de execução da iniciativa. O atendimento técnico deste capítulo não substitui a validação funcional, a homologação ou o recebimento contratual previstos nos demais capítulos.

5.1 Condições para início do desenvolvimento

O desenvolvimento somente deverá iniciar quando o item tiver atingido o gate “Pronta para execução”, definido no Capítulo 3, e houver informações suficientes para reduzir ambiguidades e permitir planejamento técnico responsável.

a) demanda, projeto e área demandante identificados;

b) item de backlog, história de usuário, requisito ou defeito formalmente registrado;

c) objetivo, escopo e critérios de aceite compreensíveis e testáveis;

d) prioridade e versão, ciclo ou entrega previstos;

e) dependências, restrições e requisitos não funcionais relevantes identificados;

f) abordagem técnica suficientemente definida para o risco da alteração;

g) estimativa, responsáveis e capacidade de execução avaliados;

h) riscos relevantes e controles de segurança, dados e privacidade identificados;

i) autorização de execução e, quando aplicável, Ordem de Serviço formalizada; e

j) repositório, ambientes e acessos necessários disponíveis.

A ausência de informação essencial deverá resultar em retorno ao refinamento, e não em implementação baseada em pressupostos não registrados. Ajustes menores identificados durante a execução poderão ser esclarecidos e registrados sem reiniciar todo o fluxo, desde que não alterem materialmente o escopo, o custo, o prazo, o risco ou o resultado esperado.

5.2 Refinamento técnico dos itens de backlog

O refinamento técnico transforma a necessidade funcional validada em trabalho implementável. Ele deverá ser realizado pela equipe técnica, com participação do negócio e de especialistas quando necessário, sem transferir à tecnologia a responsabilidade pela decisão funcional.

a) identificar componentes, serviços, integrações e bases de dados afetados;

b) detalhar regras, exceções, cenários alternativos e critérios técnicos;

c) avaliar requisitos de desempenho, disponibilidade, segurança, privacidade, acessibilidade e interoperabilidade;

d) definir estratégia de implementação, migração, compatibilidade e reversão;

e) definir estratégia de testes e evidências;

f) identificar impactos arquiteturais e necessidade de decisão registrada;

g) avaliar observabilidade, logs, métricas e alertas necessários;

h) decompor o item em tarefas tecnicamente coerentes, quando útil; e

i) revisar estimativa, dependências, riscos e capacidade.

Decisões relevantes deverão ser registradas no Redmine, no Enterprise Architect, em ADR ou no repositório técnico correspondente, preservando vínculo com o item de origem.

5.3 Requisitos aplicáveis à implementação

A implementação deverá considerar, conforme aplicável, requisitos funcionais, regras de negócio, critérios de aceite, requisitos não funcionais, restrições técnicas, requisitos de dados, requisitos de segurança e requisitos operacionais.

Elemento	Finalidade	Responsabilidade principal
Requisito funcional	Define comportamento ou capacidade esperada da solução.	Negócio valida; equipe técnica implementa e verifica.
Regra de negócio	Define condição, cálculo, restrição ou política institucional.	Gestor do Negócio aprova.
Critério de aceite	Define evidência objetiva para considerar o comportamento atendido.	Negócio aprova; TI apoia a testabilidade.
Requisito não funcional	Define atributos de qualidade, como desempenho, segurança e disponibilidade.	TI estrutura e valida com as partes competentes.
Restrição técnica	Delimita plataformas, padrões, integrações ou condições de operação.	Autoridade técnica competente.

Elemento	Finalidade	Responsabilidade principal
Requisito de dados	Define origem, qualidade, estrutura, acesso, retenção e proteção.	Negócio, responsáveis pelos dados e TI.
Requisito operacional	Define implantação, monitoramento, backup, suporte e continuidade.	CSTI, CITI e operação, conforme competência.

Descrições vagas, como “melhorar o sistema”, “deixar mais rápido” ou “adequar a segurança”, deverão ser convertidas em condições verificáveis antes da conclusão técnica. Quando a informação não puder ser determinada antecipadamente, a incerteza deverá ser registrada e tratada por experimento, protótipo ou tarefa de investigação.

5.4 Padrões de codificação e organização do código

O código deverá ser legível, coerente, testável, seguro e compatível com a arquitetura aprovada. Padrões específicos de linguagem, framework e plataforma serão mantidos em guias técnicos versionados, referenciados por este PDS, para permitir evolução sem reedição integral do documento.

a) nomes claros e consistentes com o domínio;

b) funções, classes e módulos com responsabilidades coesas;

c) baixo acoplamento e dependências explícitas;

d) tratamento controlado de configurações e parâmetros externos;

e) eliminação de código morto, duplicação injustificada e complexidade acidental;

f) reutilização responsável, sem criar abstrações sem benefício;

g) comentários destinados a explicar decisões ou restrições, e não repetir o código;

h) dependências declaradas e versionadas;

i) aderência às convenções da tecnologia e aos padrões institucionais; e

j) compatibilidade com testes, observabilidade e manutenção.

Desvios de padrão deverão ser tecnicamente justificados. Quando representarem dívida técnica relevante, deverão ser registrados no backlog com risco, impacto e plano de tratamento.

5.5 Segurança na implementação

A implementação deverá incorporar segurança desde a concepção e observar os requisitos e controles definidos no Capítulo 7. A equipe executora é responsável por produzir código seguro e corrigir vulnerabilidades atribuíveis à implementação.

a) validar entradas e controlar formatos, tamanhos e domínios;

b) codificar ou tratar saídas conforme o contexto;

c) utilizar autenticação e autorização compatíveis com o risco;

d) aplicar menor privilégio e segregação de funções;

e) utilizar consultas parametrizadas e mecanismos seguros de persistência;

f) não inserir senhas, tokens, chaves ou segredos no código ou no histórico do repositório;

g) proteger dados pessoais e informações sensíveis em trânsito e em repouso, quando exigido;

h) evitar exposição de informações internas em mensagens de erro e logs;

i) manter dependências e componentes sob controle de versão e análise de vulnerabilidade;

j) aplicar proteções contra classes de vulnerabilidades pertinentes à tecnologia; e

k) registrar eventos de segurança relevantes com integridade e acesso controlado.

A aprovação de uma entrega com vulnerabilidade conhecida somente poderá ocorrer mediante exceção formal, análise do risco, controles compensatórios, prazo de correção e aceitação pela autoridade competente.

5.6 Tratamento de erros, logs e observabilidade

Falhas devem ser tratadas de forma previsível, segura e diagnosticável. Mensagens ao usuário deverão ser compreensíveis e não revelar detalhes internos; informações técnicas necessárias à investigação deverão ser registradas em mecanismos apropriados e protegidos.

a) classificação e tratamento consistente de erros e exceções;

b) identificação ou correlação de requisições, quando aplicável;

c) logs estruturados e com níveis adequados;

d) ausência de dados pessoais, credenciais ou segredos desnecessários nos logs;

e) métricas técnicas e de negócio relevantes;

f) rastreamento distribuído em arquiteturas que o exijam;

g) alertas acionáveis, com responsáveis e canais definidos;

h) retenção, acesso e descarte compatíveis com os normativos; e

i) documentação de diagnóstico e resolução de falhas recorrentes.

Observabilidade deverá ser planejada como parte da entrega. Não será considerada suficiente uma solução que funcione em condições normais, mas não permita detectar, compreender ou tratar falhas relevantes em operação.

5.7 Testabilidade e testes automatizados

O software deverá ser construído de modo a permitir verificação eficiente. Os testes deverão ser selecionados conforme risco, arquitetura, criticidade e impacto da alteração, sem reduzir qualidade a um único percentual de cobertura.

a) testes unitários para regras e componentes isoláveis;
b) testes de integração para interfaces, bancos, filas e serviços;
c) testes de contrato para integrações entre consumidores e provedores, quando aplicável;
d) testes de componente ou sistema para fluxos relevantes;
e) testes de regressão para comportamentos críticos;
f) testes de migração e integridade de dados;
g) testes de segurança e análise automatizada conforme o Capítulo 7;
h) testes de desempenho, carga ou resiliência conforme risco; e
i) uso controlado de dados de teste, mocks, stubs e outros doubles.

Os testes automatizados deverão ser versionados com o código, executáveis de forma repetível e integrados ao pipeline sempre que tecnicamente viável. Cenários críticos sem automação deverão possuir justificativa e estratégia de verificação alternativa.

5.8 Controle de versão e estratégia de branches

O Git/GitLab ou repositório institucional equivalente será a fonte oficial do código-fonte, scripts, configurações versionáveis, testes e documentação técnica próxima ao código. O histórico deverá preservar autoria, integridade e rastreabilidade.

a) branches principais protegidas contra alteração direta não autorizada;
b) integração mediante merge request ou mecanismo equivalente;
c) branches de trabalho vinculadas ao item do Redmine, quando aplicável;
d) tags ou identificadores imutáveis para versões e releases;
e) revisão e controle de permissões;
f) tratamento formal de hotfixes;

g) retenção do histórico conforme política institucional; e

h) proibição de repositórios paralelos não autorizados como fonte oficial.

A estratégia poderá utilizar trunk-based development, GitLab Flow ou outra abordagem aprovada. A escolha deverá considerar frequência de entrega, tamanho da equipe, necessidade de versões simultâneas, criticidade, automação e modelo contratual. O PDS não impõe uma única estratégia para todos os projetos.

5.9 Commits, merge requests e revisão de código

Commits deverão representar alterações coerentes, possuir mensagem clara e manter referência ao item de trabalho sempre que aplicável. Não deverão conter segredos, arquivos indevidos ou alterações não relacionadas sem justificativa.

Merge requests deverão apresentar contexto suficiente para revisão, incluindo referência ao Redmine, resumo da alteração, impactos, testes executados, evidências, riscos e orientações de implantação quando necessárias.

A revisão de código será regra geral antes da integração em branch protegida. Sua profundidade e quantidade de revisores serão proporcionais ao risco, à criticidade, à complexidade e à modalidade de execução.

Aspecto da revisão	Verificações exemplificativas
Correção	aderência ao requisito, tratamento de exceções e efeitos colaterais
Qualidade	legibilidade, coesão, complexidade, duplicação e manutenibilidade
Arquitetura	limites, dependências, integrações e decisões aprovadas
Testes	cobertura dos cenários relevantes e confiabilidade das verificações
Segurança	validação, autorização, segredos, dependências e exposição de dados
Operação	logs, métricas, configuração, migração, implantação e rollback
Documentação	informações necessárias para uso, manutenção e auditoria

Pair programming ou mob programming poderão ser utilizados em tarefas complexas, incidentes críticos, transferência de conhecimento, onboarding, investigação e componentes de alto risco. Essas práticas são recomendadas conforme o contexto, mas não são obrigatórias para toda atividade.

Exceção à revisão prévia somente poderá ocorrer em fluxo emergencial autorizado. Nesse caso, deverá haver revisão posterior, testes mínimos, registro do risco e regularização do processo.

5.10 Integração entre Redmine, Git/GitLab e GovFlow

A rastreabilidade técnica deverá relacionar o registro operacional no Redmine ao histórico do Git/GitLab e às evidências do pipeline. O GovFlow poderá automatizar validações e integrações autorizadas.

Elemento	Fonte oficial	Vínculo esperado
Demanda, requisito ou história	Redmine	identificador utilizado em branches, commits ou merge requests
Código, testes e configuração	Git/GitLab	histórico associado ao item e à versão
Revisão e aprovação técnica	Merge request/GitLab	referência ao item do Redmine e ao pipeline
Pipeline e artefato	CI/CD	commit, tag, versão e resultado das verificações
Modelos e decisões arquiteturais	Enterprise Architect/ADR	referência à demanda ou requisito
Homologação e aceite	Redmine e processo oficial	versão e itens entregues identificados

O GovFlow poderá verificar identificadores, campos obrigatórios, vínculos, status, evidências e consistência entre ferramentas; consolidar relatórios; gerar estruturas padronizadas; e sincronizar informações permitidas. Nenhuma automação poderá homologar, aceitar risco, receber contratualmente ou alterar decisão formal sem regra aprovada e autoridade competente.

5.11 Builds, pacotes e versionamento de releases

Build é o processo de transformar código e dependências em artefato verificável. Release é um conjunto identificado de mudanças preparado para disponibilização. Implantação é a promoção controlada de uma release para determinado ambiente. Esses conceitos não deverão ser utilizados como sinônimos.

Toda release deverá ser identificável e, sempre que tecnicamente possível, reproduzível. Deverá manter relação com:

a) commit ou tag de origem;
b) itens de backlog incluídos;
c) resultados do pipeline e dos testes;
d) dependências e componentes relevantes;
e) artefatos gerados;
f) notas da versão;
g) configuração e migrações aplicáveis; e

h) plano de implantação e reversão, quando necessário.

Artefatos deverão ser armazenados em repositório institucional apropriado, com controle de acesso, retenção, integridade e identificação de versão. Builds manuais não rastreáveis não deverão ser utilizados em produção, salvo contingência formalmente autorizada e posteriormente regularizada.

5.12 Documentação técnica da implementação

A documentação deverá ser suficiente para permitir desenvolvimento, revisão, testes, implantação, operação, manutenção e transferência de conhecimento. A quantidade e o formato serão proporcionais à iniciativa e poderão estar distribuídos entre Redmine, Enterprise Architect, Git/GitLab e repositórios institucionais, desde que haja fonte oficial e vínculos claros.

a) instruções de configuração, build e execução;
b) visão da arquitetura e componentes afetados;
c) APIs, eventos, contratos e integrações;
d) estruturas, migrações e regras relevantes de dados;
e) decisões técnicas e respectivas justificativas;
f) dependências, licenças e requisitos de ambiente;
g) procedimentos de implantação, rollback e troubleshooting;
h) riscos, limitações conhecidas e dívida técnica relevante; e
i) informações de operação, observabilidade e suporte.

A documentação deverá ser atualizada na mesma entrega que altera o comportamento correspondente. Não deverão ser criados documentos paralelos que dupliquem informações estruturadas e mais atuais nas ferramentas oficiais.

5.13 Execução pela fábrica de software

Quando o desenvolvimento for contratado, a fábrica deverá executar somente itens formalmente autorizados e vinculados ao instrumento contratual aplicável, como Ordem de Serviço, backlog aprovado, versão ou pacote de entrega.

a) analisar os itens recebidos e apontar dúvidas, riscos e dependências antes do compromisso;
b) estimar conforme o método contratual e registrar premissas;
c) utilizar repositórios, ambientes, padrões e ferramentas institucionais;

d) manter vínculo entre demanda, código, testes, evidências, versão e produto contratado;

e) realizar implementação, revisão, testes e correções;

f) cumprir os controles de segurança, qualidade e documentação;

g) produzir evidências suficientes para validação técnica, medição e auditoria;

h) apoiar homologação, implantação, correção de pendências e estabilização;

i) transferir conhecimento e evitar dependência indevida do fornecedor; e

j) comunicar impedimentos, desvios e riscos no prazo definido.

A disponibilização de código, isoladamente, não caracteriza entrega concluída. A conclusão dependerá do atendimento aos critérios técnicos, funcionais e contratuais aplicáveis. Produtos incompletos, não rastreáveis, sem testes, sem documentação ou sem evidências poderão ser devolvidos para correção e considerados não aceitos para fins de medição.

5.14 Evidências e critérios de conclusão técnica

A Definition of Done técnica estabelece as condições mínimas para considerar um item tecnicamente concluído e apto a seguir para validação ou homologação. Ela não substitui o aceite funcional nem o recebimento contratual.

Critério	Evidência exemplificativa
Implementação concluída	código integrado na branch prevista e item atualizado
Revisão aprovada	merge request com aprovações e pendências resolvidas
Pipeline aprovado	execução identificada sem falha bloqueante
Testes executados	resultados automatizados e evidências manuais quando aplicáveis
Segurança verificada	resultados dos controles previstos e vulnerabilidades tratadas
Documentação atualizada	arquivos, modelos, instruções ou registros vinculados
Artefato identificado	pacote, imagem, tag ou release reproduzível
Rastreabilidade preservada	vínculos entre Redmine, Git/GitLab, pipeline e versão
Operação preparada	configuração, logs, monitoramento, migração e rollback conforme risco

Critérios adicionais poderão ser definidos por tecnologia, contrato, criticidade ou projeto. O GovFlow poderá verificar automaticamente a presença de evidências e impedir transições quando regras obrigatórias não forem atendidas.

5.15 Exceções e tratamento de urgências

Correções emergenciais, hotfixes e incidentes críticos poderão utilizar fluxo reduzido para preservar a continuidade do serviço, desde que a urgência seja justificada e autorizada.

a) registro da ocorrência e da autoridade que autorizou;

b) identificação do impacto e do risco;

c) alteração mínima necessária;

d) testes proporcionais e verificação de segurança possível;

e) plano de reversão;

f) identificação da versão implantada;

g) monitoramento após a implantação;

h) revisão técnica posterior;

i) regularização dos vínculos, documentação e evidências; e

j) análise de causa e criação de ações preventivas quando aplicável.

Urgência não elimina responsabilidade, rastreabilidade ou prestação de contas. Exceções recorrentes deverão ser analisadas como sinal de fragilidade do processo, da arquitetura, da capacidade ou da gestão operacional.

6. Manutenção, Sustentação e Operação de Software

Detectar	Registrar	Conter	Restaurar	Analisar causa	Corrigir	Prevenir	Aprender

> **LEITURA ORIENTADA:** Este capítulo estabelece o modelo operacional para manter os sistemas da SEMA/MT disponíveis, seguros, estáveis, atualizados e capazes de evoluir após a entrada em produção. Ele complementa o macroprocesso do Capítulo 3 e as práticas técnicas dos Capítulos 4 e 5.

As regras aplicam-se a sistemas mantidos por equipes internas, por fábrica de software, por fornecedores especializados ou por modelos compartilhados. A profundidade dos controles deverá ser proporcional à criticidade, ao risco, ao impacto e ao modelo de suporte de cada solução.

6.1 Objetivos e escopo

A manutenção, a sustentação e a operação deverão assegurar continuidade do serviço, restauração rápida em caso de falha, correção definitiva de causas, evolução controlada, segurança, atualização tecnológica, preservação do conhecimento e rastreabilidade das decisões.

a) manter disponibilidade, desempenho e integridade dos serviços;
b) corrigir defeitos e reduzir reincidências;
c) adaptar soluções a mudanças legais, tecnológicas e operacionais;
d) evoluir funcionalidades de forma priorizada e rastreável;
e) tratar vulnerabilidades, obsolescência e dívida técnica;
f) monitorar sistemas e antecipar falhas;
g) manter documentação, runbooks e conhecimento operacional; e
h) controlar mudanças, versões, ambientes e implantações.

Cada sistema deverá possuir modelo de sustentação definido, indicando responsáveis, horários de atendimento, níveis de serviço, canais, escalonamento, repositórios, ambientes, dependências críticas e procedimentos de continuidade.

6.2 Classificação das demandas em produção

Todo registro relacionado a sistema em produção deverá ser classificado no Redmine ou ferramenta institucional equivalente. A classificação orienta prioridade, fluxo, responsáveis, testes, aprovações e forma de medição.

Classificação	Definição operacional
Incidente	Interrupção, degradação ou comportamento inesperado que afeta um serviço.
Defeito	Falha identificada no produto de software em relação ao comportamento esperado.
Problema	Causa real ou potencial de um ou mais incidentes.
Requisição de serviço	Solicitação padronizada de acesso, informação, configuração ou apoio.
Manutenção corretiva	Alteração destinada a eliminar defeito.
Manutenção adaptativa	Adequação a mudança externa de ambiente, norma, integração ou tecnologia.
Manutenção evolutiva	Ampliação ou modificação de capacidade funcional.
Manutenção perfectiva	Melhoria de desempenho, usabilidade, manutenibilidade ou eficiência.
Manutenção preventiva/técnica	Ação antecipada para reduzir risco, obsolescência ou dívida técnica.
Mudança	Alteração controlada em software, configuração, dados, infraestrutura ou integração.
Hotfix	Correção emergencial destinada a restaurar ou proteger serviço crítico.
Segurança	Tratamento de vulnerabilidade, ameaça ou não conformidade de segurança.

A priorização deverá considerar impacto, urgência, severidade, criticidade do sistema, número de usuários afetados, existência de alternativa, risco legal, ambiental, financeiro ou de segurança e dependências externas. O GovFlow poderá validar campos obrigatórios e apoiar o roteamento, sem substituir a decisão dos responsáveis.

6.3 Manutenção corretiva

A manutenção corretiva elimina falhas funcionais ou técnicas identificadas em produção, homologação ou suporte. O fluxo mínimo deverá contemplar registro, reprodução, classificação, análise de causa, correção, testes, validação, implantação, monitoramento e encerramento.

a) registrar o comportamento observado, ambiente, versão, data, impacto e evidências;
b) reproduzir a falha ou documentar a impossibilidade de reprodução;
c) identificar causa provável e componentes afetados;
d) implementar a correção com rastreabilidade;
e) executar reteste e regressão proporcional;
f) implantar de forma controlada e monitorar o resultado; e
g) registrar causa raiz e ação preventiva quando houver recorrência ou alto impacto.

A correção não será considerada concluída apenas porque o sintoma deixou de ocorrer. É necessário demonstrar que o comportamento esperado foi restaurado e que impactos colaterais relevantes foram verificados.

6.4 Manutenção adaptativa

A manutenção adaptativa adequa o sistema a mudanças externas, como legislação, infraestrutura, sistema operacional, banco de dados, navegador, API, certificado, protocolo, dependência, formato de dados ou política institucional.

A demanda deverá registrar origem da mudança, prazo, sistemas afetados, risco de não adaptação, compatibilidade, estratégia de testes, plano de implantação e eventual período de coexistência. Mudanças previsíveis deverão ser tratadas antecipadamente, evitando conversão desnecessária em incidente emergencial.

6.5 Manutenção evolutiva e perfectiva

A manutenção evolutiva amplia ou modifica funcionalidades. A manutenção perfectiva melhora desempenho, usabilidade, experiência, legibilidade, manutenibilidade ou eficiência sem necessariamente alterar a finalidade principal do sistema.

Alterações funcionais relevantes deverão seguir o fluxo de demanda, requisito, priorização, backlog, desenvolvimento, testes, homologação e aceite definido no Capítulo 3. Melhorias técnicas de baixo risco poderão seguir fluxo simplificado, desde que preservem registro, avaliação de impacto, testes e aprovação aplicável.

6.6 Manutenção preventiva, técnica e de segurança

A manutenção preventiva, técnica e de segurança reduz riscos antes que ocorram falhas ou incidentes. Ela poderá ser originada por monitoramento, auditoria, análise de vulnerabilidade, revisão arquitetural, obsolescência tecnológica ou dívida técnica.

a) atualização de dependências, bibliotecas e frameworks;
b) correção de vulnerabilidades e configurações inseguras;
c) refatoração e redução de complexidade ou dívida técnica;
d) melhoria de testes automatizados e cobertura de cenários críticos;
e) atualização de componentes, certificados e protocolos;
f) melhoria de logs, métricas, alertas e rastreamento;

g) remoção de código, integrações ou recursos obsoletos; e

h) adequação arquitetural e revisão de permissões.

Essas demandas deverão concorrer por capacidade e prioridade de forma transparente. O fato de não produzirem nova funcionalidade visível não elimina seu valor para segurança, continuidade e sustentabilidade.

6.7 Sustentação e suporte contínuo

A sustentação compreende atendimento técnico, apoio a usuários, análise de ocorrências, acompanhamento de produção, gestão de versões, correções, documentação, consultas e apoio às integrações.

Nível	Atuação típica
N1	Registro, confirmação de dados, orientação inicial, solução conhecida e encaminhamento.
N2	Análise funcional ou técnica especializada, configuração e investigação intermediária.
N3	Desenvolvimento, correção estrutural, análise profunda e mudança de software.
N4	Fabricante, fornecedor externo ou especialista de tecnologia, quando aplicável.

O modelo poderá ser ajustado por serviço, mas deverá existir regra clara de escalonamento. Todo encaminhamento deverá preservar contexto, evidências, ações já realizadas e responsável atual, evitando que o usuário tenha de reiniciar o relato.

6.8 Monitoramento, observabilidade e alertas

Sistemas em produção deverão possuir monitoramento e observabilidade proporcionais à criticidade. O objetivo é detectar degradações, apoiar diagnóstico, medir comportamento e antecipar falhas.

a) disponibilidade e saúde de serviços;

b) tempo de resposta, volume, filas e erros;

c) logs estruturados e correlação de eventos;

d) métricas de aplicação, infraestrutura e banco de dados;

e) rastreamento distribuído, quando aplicável;

f) integrações, certificados e dependências externas;

g) capacidade e consumo de recursos; e

h) indicadores de negócio relevantes para operação.

Alertas deverão possuir limiar, criticidade, responsável, canal, escalonamento e procedimento de resposta. Alertas ruidosos, sem responsável ou sem ação definida deverão ser revistos.

6.9 Gestão de incidentes

A gestão de incidentes tem como objetivo restaurar o serviço com segurança e rapidez, reduzindo impacto ao negócio e aos usuários. O fluxo deverá contemplar detecção, registro, classificação, priorização, atribuição, diagnóstico, contenção, restauração, comunicação, validação e encerramento.

Incidentes críticos deverão prever, conforme aplicável, sala de crise, coordenação definida, atualizações periódicas, comunicação institucional, linha do tempo, decisão de rollback e relatório pós-incidente. A restauração temporária poderá ocorrer por solução de contorno, sem dispensar a abertura de problema para tratamento definitivo.

6.10 Gestão de problemas e causa raiz

A gestão de problemas busca identificar e eliminar causas reais ou potenciais de incidentes, reduzir recorrência e registrar conhecimento. Ela não se confunde com a restauração imediata do serviço.

a) consolidar histórico de incidentes relacionados;
b) analisar linha do tempo, mudanças recentes e evidências;
c) formular e testar hipóteses;
d) registrar causa raiz conhecida ou incerteza remanescente;
e) definir solução de contorno e solução definitiva;
f) criar ações preventivas e acompanhar sua conclusão; e
g) atualizar base de conhecimento e runbooks.

Podem ser utilizadas técnicas como 5 Porquês, diagrama de Ishikawa, árvore de falhas, Pareto e análise cronológica, conforme a complexidade.

6.11 Gestão de mudanças

Mudança é qualquer alteração controlada capaz de afetar software, configuração, banco de dados, infraestrutura, integração ou serviço. As mudanças deverão ser classificadas como padrão, normal ou emergencial.

Tipo	Tratamento
Padrão	Repetitiva, de baixo risco e previamente autorizada por procedimento aprovado.
Normal	Exige avaliação de impacto, risco, testes, aprovação e planejamento.
Emergencial	Necessária para restaurar serviço, reduzir dano ou tratar risco imediato, com fluxo acelerado e regularização posterior.

Toda mudança deverá registrar objetivo, escopo, risco, impacto, dependências, janela, responsáveis, testes, comunicação, plano de reversão e verificação pós-implantação. A governança deverá ser proporcional: alterações simples não exigem a mesma instância de aprovação de mudanças críticas.

6.12 Correções emergenciais e hotfixes

Hotfixes poderão seguir fluxo acelerado quando a demora representar risco maior que a execução imediata. Mesmo em emergência deverão ser preservados registro, autorização, rastreabilidade, teste mínimo, revisão possível, plano de rollback e validação pós-implantação.

Após a estabilização, será obrigatório consolidar a correção na linha principal, executar revisão posterior, ampliar testes, atualizar documentação, registrar causa raiz e avaliar ações preventivas. Urgência não significa ausência de controle.

6.13 Testes em manutenção e sustentação

Toda alteração em sistema mantido deverá possuir estratégia de testes proporcional ao risco, ao impacto e à natureza da mudança. Os testes devem demonstrar a correção do comportamento pretendido e reduzir a probabilidade de regressão.

Tipo de teste	Finalidade e aplicação
Unitário	Verifica função, método, classe ou componente isolável. Em correções, deve, quando viável, reproduzir o defeito antes da correção e permanecer no conjunto automatizado.
Integração	Verifica comunicação entre módulos, APIs, serviços, filas, bancos e sistemas externos.
Funcional	Confirma comportamento segundo requisito, regra de negócio ou critério de aceite.
Reteste	Repete o cenário que falhou para confirmar que a correção foi efetiva.
Regressão	Verifica se a alteração não prejudicou funcionalidades existentes ou fluxos relacionados.
Smoke test	Valida rapidamente funções essenciais após implantação.
Aceitação/Homologação	Confirma, pela área de negócio, que a mudança funcional atende ao resultado esperado.

Tipo de teste	Finalidade e aplicação
Desempenho	Avalia tempo de resposta, volume, concorrência, escalabilidade e uso de recursos.
Segurança	Inclui SAST, SCA, DAST, análise de segredos e verificações específicas conforme risco.
Migração e dados	Verifica integridade, completude, consistência, reconciliação e reversibilidade de dados.
Compatibilidade	Avalia navegadores, dispositivos, sistemas operacionais, bancos e versões integradas.
Resiliência/Recuperação	Verifica comportamento diante de falhas, restauração, backup, rollback e continuidade.

Reteste e regressão não são sinônimos: o reteste confirma a correção específica; a regressão procura impactos colaterais. Para defeitos, deverá ser criado, quando tecnicamente aplicável, teste automatizado que reproduza a falha e permaneça como proteção contra recorrência.

As evidências deverão indicar versão, ambiente, data, responsável, dados de entrada, resultado esperado, resultado obtido e vínculo com o item do Redmine. Os testes automatizados deverão ser versionados e integrados ao pipeline sempre que viável.

6.14 Gestão de versões, configuração e ambientes

A sustentação deverá manter controle sobre versões em produção e homologação, dependências, parâmetros, banco de dados, scripts, certificados, variáveis, configurações e infraestrutura. Nenhuma correção deverá depender exclusivamente de alteração manual não registrada.

a) identificar versão e artefato implantados em cada ambiente;
b) versionar scripts e configurações passíveis de versionamento;
c) controlar diferenças autorizadas entre ambientes;
d) proteger segredos e credenciais;
e) registrar migrações e procedimentos de reversão; e
f) manter histórico de mudanças e responsáveis.

6.15 SLA, níveis de serviço e escalonamento

O PDS define os elementos conceituais dos níveis de serviço. Valores específicos deverão ser estabelecidos em contrato, Ordem de Serviço, catálogo de serviços ou plano de sustentação.

a) horário e janela de serviço;

b) severidade e prioridade;

c) tempo de resposta, início de atendimento, restauração e solução;

d) disponibilidade e período de medição;

e) condições de suspensão e exclusões;

f) responsabilidades do usuário, da TI e do fornecedor;

g) escalonamento funcional, técnico e gerencial; e

h) forma de medição, evidência e tratamento de descumprimento.

Severidade deverá considerar impacto e urgência, e não apenas a percepção individual do solicitante. Metas e fórmulas institucionais serão consolidadas no Capítulo 13.

6.16 Atuação da fábrica de software

Quando houver sustentação contratada, a fábrica deverá atuar somente sobre itens autorizados, respeitando contrato, Ordem de Serviço, backlog, SLA, padrões técnicos e repositórios institucionais.

a) analisar e estimar solicitações dentro dos prazos definidos;

b) reproduzir defeitos e registrar diagnóstico;

c) implementar correções e mudanças com rastreabilidade;

d) executar testes e produzir evidências;

e) participar de incidentes críticos e escalonamentos;

f) apoiar implantação, rollback e estabilização;

g) tratar reincidências e não conformidades;

h) atualizar documentação e transferir conhecimento; e

i) fornecer informações para medição, SLA, aceite e eventual glosa.

A CSTI e a fiscalização deverão acompanhar prazo, qualidade, retrabalho, reabertura, reincidência, evidências e aderência contratual. A indisponibilidade de conhecimento no fornecedor não poderá justificar ausência de documentação ou dependência institucional.

6.17 Conhecimento, documentação e continuidade

A operação deverá manter base de conhecimento e documentação suficiente para atendimento, recuperação e transferência de responsabilidade.

a) runbooks e procedimentos operacionais;

b) manuais e orientações de suporte;

c) histórico de incidentes, problemas e soluções de contorno;

d) decisões técnicas e arquiteturais;

e) instruções de backup, restauração, rollback e recuperação;

f) dependências, integrações e contatos de escalonamento;

g) limitações conhecidas e riscos operacionais; e

h) procedimentos de continuidade e contingência.

O conhecimento não poderá permanecer exclusivamente com uma pessoa, equipe ou fornecedor. Mudanças relevantes deverão atualizar a documentação correspondente na mesma entrega.

6.18 Encerramento, reabertura e lições aprendidas

Um item somente será encerrado quando a solução ou restauração tiver sido validada, os testes e evidências estiverem registrados, o ambiente estiver estável, as partes interessadas tiverem sido comunicadas e a documentação aplicável estiver atualizada.

A reabertura deverá ocorrer quando o problema reaparecer, a correção for incompleta, o critério não tiver sido atendido, houver regressão ou a implantação tiver sido revertida. Incidentes relevantes e mudanças críticas deverão gerar lições aprendidas e ações de melhoria acompanhadas até a conclusão.

7. Conformidade, Segurança e Proteção de Dados

Unitários	Integração	SAST	SCA	Secrets	DAST	Contêiner/IaC	SBOM/Pentest

> **LEITURA ORIENTADA:** Este capítulo estabelece os controles, verificações, evidências, responsabilidades e critérios de decisão aplicáveis à segurança da informação, à segurança de software, à proteção de dados pessoais e à conformidade das iniciativas de software da SEMA/MT. Ele complementa os princípios DevSecOps do Capítulo 4, as práticas de construção do Capítulo 5, a operação do Capítulo 6 e a divisão de responsabilidades do Capítulo 9.

Os controles deverão ser aplicados de forma proporcional ao risco, à criticidade, à exposição, aos dados tratados e ao impacto potencial da solução. Segurança e privacidade não constituem etapas isoladas ao final do desenvolvimento: devem ser consideradas desde o registro da demanda até a operação, manutenção e descontinuação.

7.1 Objetivos e princípios

A segurança e a proteção de dados deverão preservar confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, privacidade e continuidade, sem impedir a entrega de valor público. A aplicação deste capítulo observará os seguintes princípios:

a) segurança desde a concepção (Security by Design);

b) privacidade desde a concepção e por padrão (Privacy by Design e Privacy by Default);

c) defesa em profundidade e redução da superfície de ataque;

d) menor privilégio, necessidade de saber e segregação de funções;

e) minimização de dados e limitação da finalidade;

f) rastreabilidade e responsabilidade demonstrável;

g) proteção proporcional ao risco e à criticidade;

h) falha segura e recuperação controlada;

i) melhoria contínua baseada em evidências; e

j) responsabilidade compartilhada entre negócio, tecnologia, infraestrutura, governança e fornecedores.

Ferramentas e automações podem identificar falhas, bloquear gates e consolidar evidências, mas não substituem decisões formais, aceite de risco ou responsabilidades institucionais.

7.2 Classificação de criticidade e risco

Toda iniciativa deverá ser classificada quanto à criticidade e ao risco antes da execução e revista quando houver mudança relevante. A classificação orientará controles mínimos, testes, aprovações, periodicidade de avaliações, necessidade de modelagem de ameaças, pentest e avaliação de impacto à proteção de dados.

Nível	Caracterização geral	Tratamento esperado
Baixo	Impacto limitado, baixa exposição e ausência de dados ou operações críticas.	Controles básicos, revisão proporcional e testes essenciais.
Moderado	Impacto relevante, integrações ou tratamento de dados pessoais em escala limitada.	Controles ampliados, scans automatizados e análise de risco documentada.
Alto	Serviço importante, exposição externa, dados sensíveis ou impacto institucional elevado.	Modelagem de ameaças, testes aprofundados, gates reforçados e aprovação específica.
Crítico	Risco ambiental, social, legal, financeiro ou operacional muito elevado; indisponibilidade ou comprometimento pode causar dano grave.	Controles máximos, avaliações especializadas, contingência, monitoramento contínuo e aceite formal de risco residual.

A classificação deverá considerar impacto ambiental e ao cidadão, disponibilidade, exposição à internet, volume e natureza dos dados, integrações, privilégios, dependência externa, obrigação legal, impacto financeiro e potencial de dano.

7.3 Segurança e privacidade desde a concepção

Desde o registro da demanda deverão ser identificados, conforme aplicável, os dados tratados, usuários e perfis, integrações, requisitos de disponibilidade, ameaças, requisitos legais, trilhas de auditoria, retenção, descarte, continuidade, exposição externa e necessidades de autenticação e autorização.

A Definition of Ready deverá verificar se os requisitos relevantes de segurança e privacidade estão suficientemente definidos. Lacunas críticas deverão impedir o início da execução ou ser tratadas por decisão formal com riscos e ações registradas.

7.4 Modelagem de ameaças e avaliação de riscos

Iniciativas de maior criticidade ou risco deverão realizar modelagem de ameaças e avaliação estruturada dos riscos de segurança. Poderão ser utilizadas técnicas como STRIDE, diagramas de fluxo de dados, árvores de ataque, misuse cases, abuse cases ou abordagem equivalente.

a) identificar ativos, usuários, agentes, integrações e fronteiras de confiança;

b) mapear ameaças, vulnerabilidades e cenários de abuso;

c) estimar probabilidade, impacto e exposição;

d) definir controles preventivos, detectivos, corretivos e compensatórios;

e) registrar risco residual e autoridade responsável por sua aceitação; e

f) revisar a análise diante de mudanças arquiteturais, incidentes ou novas ameaças.

Quando aplicável, os modelos arquiteturais e de ameaça deverão ser mantidos no Enterprise Architect e vinculados à demanda no Redmine.

7.5 Gestão de identidades, autenticação e autorização

Os sistemas deverão adotar controles de identidade e acesso compatíveis com o risco, incluindo:

a) identificação individual de usuários e rastreabilidade de ações;

b) proibição de contas compartilhadas, salvo exceção justificada e controlada;

c) autenticação forte e MFA para perfis privilegiados ou cenários de maior risco;

d) autorização baseada em papéis, atributos ou política equivalente;

e) princípio do menor privilégio e segregação de funções;

f) revisão periódica, bloqueio e revogação de acessos;

g) gestão específica de contas técnicas, serviços e robôs;

h) proteção de sessão, expiração e mecanismos contra uso indevido; e

i) logs de autenticação, autorização e alterações relevantes.

7.6 Proteção de dados, criptografia e gestão de segredos

A proteção dos dados deverá considerar classificação, finalidade, contexto de uso e potencial de dano. Conforme o risco, deverão ser aplicados:

a) criptografia em trânsito e em repouso;

b) proteção de backups e mídias;

c) gestão, rotação e segregação de chaves;

d) proibição de credenciais, tokens e segredos no código-fonte;

e) uso de cofres de segredos ou mecanismos equivalentes;

f) mascaramento, pseudonimização ou anonimização quando apropriado;

g) restrição de dados pessoais em logs, ambientes de teste e relatórios;

h) retenção, arquivamento e descarte seguros; e

i) proteção das configurações e variáveis sensíveis.

7.7 Segurança de código, dependências e cadeia de fornecimento

A construção e a entrega deverão controlar riscos provenientes do código próprio, de componentes de terceiros e da cadeia de fornecimento de software.

a) aplicar práticas de codificação segura e revisão de mudanças sensíveis;

b) controlar dependências diretas e transitivas, versões e procedência;

c) avaliar vulnerabilidades conhecidas, obsolescência e licenciamento;

d) proteger repositórios, branches, pipelines, runners e artefatos;

e) analisar imagens de contêiner e infraestrutura como código;

f) gerar SBOM quando exigido pela criticidade, contrato ou padrão institucional;

g) garantir reprodutibilidade, integridade e proveniência de builds quando aplicável; e

h) corrigir ou mitigar componentes vulneráveis antes da liberação.

7.8 Testes e verificações de segurança

Os testes de segurança deverão ser selecionados segundo a tecnologia, a criticidade, o risco e a exposição. Eles complementam os testes unitários, de integração, funcionais, de regressão, desempenho e resiliência previstos nos Capítulos 5 e 6.

Verificação	Finalidade
SAST	Analisar código ou artefatos sem executar a aplicação, identificando padrões inseguros e vulnerabilidades potenciais.
SCA	Avaliar bibliotecas, frameworks e dependências quanto a vulnerabilidades, obsolescência e licenciamento.
DAST	Avaliar a aplicação em execução, incluindo entradas, sessões, autenticação, autorização e exposição.
Secrets scanning	Detectar senhas, tokens, chaves, certificados e outros segredos indevidamente versionados.
Scan de contêiner	Avaliar imagem-base, pacotes, usuário de execução, permissões, portas e vulnerabilidades.
Scan de IaC	Avaliar configurações de infraestrutura, rede, armazenamento, identidades, criptografia e exposição.
Testes de autorização	Confirmar que cada perfil acessa apenas recursos e operações permitidos.
Testes unitários de segurança	Verificar regras de validação, autorização, proteção de dados, falha segura e ausência de exposição.
Testes de integração de segurança	Verificar controles nas comunicações entre APIs, serviços, bancos, filas e sistemas externos.

Verificação	Finalidade
Pentest	Avaliação especializada e complementar da possibilidade de exploração real de vulnerabilidades.
Reteste de segurança	Confirmar que vulnerabilidades corrigidas foram eliminadas e não podem ser contornadas.

O pentest não se confunde com scanner automatizado. Sua exigência será determinada por criticidade, exposição, mudança arquitetural relevante, risco, obrigação institucional ou contratual. Não será fixada periodicidade universal para todos os sistemas.

7.9 Gestão de vulnerabilidades

Toda vulnerabilidade identificada deverá seguir fluxo formal de tratamento: identificação, registro, validação, classificação, análise de exposição, priorização, atribuição, correção ou mitigação, reteste, aceite de risco ou encerramento e monitoramento.

A prioridade não dependerá exclusivamente de uma pontuação automática. Deverão ser considerados exploração ativa, exposição, criticidade do ativo, dados afetados, facilidade de exploração, impacto institucional, controles compensatórios e disponibilidade de correção.

Prazos específicos deverão constar em política, SLA, contrato ou catálogo institucional. Vulnerabilidades não corrigidas somente poderão avançar mediante exceção ou aceite formal de risco, conforme o item 7.17.

7.10 Proteção de dados pessoais e bases legais

Toda operação de tratamento de dados pessoais deverá identificar finalidade, categorias de dados e titulares, operações realizadas, agentes de tratamento, compartilhamentos, base legal, retenção, medidas de segurança e riscos.

O consentimento não será presumido como base legal padrão. A hipótese aplicável deverá ser definida conforme a finalidade e o contexto, especialmente quando o tratamento estiver relacionado ao cumprimento de obrigação legal ou regulatória, à execução de políticas públicas ou ao exercício das competências institucionais.

CPF, endereço e outros identificadores são dados pessoais e exigem proteção adequada ao contexto. Dados pessoais sensíveis correspondem às categorias específicas

previstas na legislação. A criticidade do tratamento dependerá também do volume, da combinação de informações e do potencial de dano.

7.11 Mapeamento, inventário e fluxo de dados pessoais

As soluções deverão manter, conforme aplicabilidade, inventário ou registro das operações de tratamento, contemplando origem, coleta, transformação, armazenamento, uso, compartilhamento, transferência, arquivamento e eliminação.

a) dados e categorias de titulares;
b) finalidade e base legal;
c) sistemas, integrações e destinatários;
d) responsáveis e operadores;
e) retenção e descarte;
f) medidas de segurança e acessos;
g) transferências e compartilhamentos; e
h) riscos e controles.

O inventário poderá ser complementado por catálogo de dados, diagrama de fluxo, modelo no Enterprise Architect e referências no Redmine, preservando fonte oficial e rastreabilidade.

7.12 Direitos dos titulares e funcionalidades de atendimento

Os sistemas deverão apoiar, conforme a hipótese legal e a aplicabilidade, o atendimento aos direitos dos titulares, incluindo confirmação de tratamento, acesso, correção, informação sobre compartilhamento, bloqueio, anonimização ou eliminação nas hipóteses cabíveis, portabilidade quando aplicável, revogação de consentimento, oposição e revisão de decisões automatizadas pertinentes.

O PDS não presume eliminação irrestrita. Obrigações legais, interesse público, arquivo, exercício de direitos e demais hipóteses aplicáveis podem exigir conservação. As respostas deverão ser registradas, seguras, autenticadas e rastreáveis.

7.13 Relatório de Impacto à Proteção de Dados Pessoais - RIPD

O RIPD será elaborado quando exigido pela autoridade competente, por norma institucional ou quando a avaliação indicar tratamento com alto risco aos direitos e às liberdades dos titulares. Não será obrigatório indistintamente para todos os sistemas.

A triagem deverá considerar, entre outros fatores, dados sensíveis, crianças e adolescentes, larga escala, monitoramento sistemático, tecnologias emergentes, decisões automatizadas, cruzamento de bases e impacto relevante.

Quando aplicável, o RIPD deverá registrar descrição do tratamento, finalidade, necessidade, proporcionalidade, riscos, controles, risco residual, responsáveis, aprovação e critérios de revisão.

7.14 Incidentes de segurança e violações de dados pessoais

Incidente de segurança é evento que afeta ou pode afetar confidencialidade, integridade, disponibilidade ou autenticidade. Quando envolver dados pessoais, deverá haver avaliação específica do risco ou dano relevante aos titulares e das obrigações de comunicação vigentes.

a) detectar, registrar, classificar e conter;
b) preservar evidências e manter linha do tempo;
c) comunicar internamente os responsáveis;
d) avaliar dados, titulares, extensão, impacto e risco;
e) decidir sobre comunicações obrigatórias;
f) corrigir, recuperar e monitorar;
g) registrar medidas, decisões e justificativas; e
h) produzir lições aprendidas e ações preventivas.

Os prazos e critérios legais vigentes deverão ser observados no momento do incidente. O PDS não cria prazo paralelo ou conflitante com a regulamentação aplicável.

7.15 Segurança de ambientes, infraestrutura e operação

Os ambientes e a infraestrutura deverão aplicar hardening, segregação, controle de rede, atualização, gestão de configuração, backup, recuperação, monitoramento, proteção

de banco de dados, certificados, identidades privilegiadas, continuidade e capacidade, conforme criticidade.

a) separar desenvolvimento, testes, homologação e produção;
b) restringir acessos administrativos e registrar operações privilegiadas;
c) manter correções e atualizações de segurança;
d) proteger backups e testar restauração;
e) monitorar eventos, disponibilidade, capacidade e configurações;
f) controlar certificados, chaves e credenciais;
g) manter planos de continuidade, recuperação e rollback; e
h) revisar configurações e exceções periodicamente.

7.16 Requisitos para fornecedores e fábrica de software

Contratos, Ordens de Serviço e instrumentos correlatos deverão incorporar requisitos de segurança e proteção de dados proporcionais ao objeto e ao risco.

a) confidencialidade, controle de acesso e responsabilização;
b) desenvolvimento seguro, testes e tratamento de vulnerabilidades;
c) uso de repositórios, ambientes e credenciais institucionais;
d) gestão de componentes, dependências e SBOM quando aplicável;
e) produção e entrega de evidências;
f) comunicação tempestiva de incidentes e cooperação na resposta;
g) proteção, devolução ou eliminação de dados ao término;
h) transferência de conhecimento e documentação;
i) requisitos para subcontratação e cadeia de fornecimento; e
j) auditoria e verificação de conformidade, conforme o instrumento.

Dados reais não deverão ser utilizados em desenvolvimento ou testes sem necessidade, autorização e controles adequados. A fábrica deverá corrigir vulnerabilidades e não conformidades de sua responsabilidade dentro dos prazos estabelecidos.

7.17 Evidências, gates e exceções de segurança

Os gates do processo deverão verificar, conforme aplicabilidade, requisitos de segurança, análise de risco, modelagem de ameaças, resultados de SAST, SCA, DAST e

demais verificações, testes, vulnerabilidades abertas, documentação, autorizações, risco residual e plano de tratamento.

Gate	Evidências esperadas
Requisitos	Dados, identidades, autorização, privacidade, riscos e requisitos de segurança definidos.
Código	Revisão aprovada, SAST, SCA, secrets scan e testes unitários de segurança aplicáveis.
Pacote	Dependências, imagem, IaC, SBOM e integridade do artefato quando exigidos.
Homologação	DAST, testes de autorização, vulnerabilidades tratadas e evidências de privacidade.
Produção	Risco residual, exceções, hardening, backup, rollback, monitoramento e aprovações.

Uma vulnerabilidade poderá bloquear a entrega, ser corrigida, receber mitigação temporária, ser objeto de exceção ou ter risco formalmente aceito. A exceção deverá registrar justificativa, risco, prazo, controle compensatório, responsável, aprovador e data de revisão. Ferramentas não aceitam risco; a autoridade competente o faz.

7.18 Governança, responsabilidades e atuação do encarregado

As responsabilidades seguem a segregação estabelecida no Capítulo 9:

Participante	Responsabilidade principal
CPQSI	Governança, políticas, conformidade, acompanhamento de riscos, indicadores e avaliação do processo.
CSTI	Segurança de software, requisitos, validação técnica, acompanhamento da fábrica e tratamento de vulnerabilidades de aplicação.
CITI	Segurança de infraestrutura, ambientes, redes, bancos, identidade técnica, backup e continuidade.
Área demandante	Finalidade, necessidade dos dados, regras de negócio, validação e homologação funcional.
Fábrica/fornecedor	Implementação segura, testes, correções, documentação e evidências.
Encarregado	Orientação, comunicação, canal com titulares e autoridade, apoio à governança e demais atribuições legais e regulamentares.

O encarregado não será tratado como desenvolvedor, executor exclusivo dos controles, aprovador de arquitetura ou responsável único pela conformidade. Cada unidade e fornecedor responde pelas atividades sob sua competência.

7.19 Indicadores e melhoria contínua

O Capítulo 13 consolidará fórmulas, metas, fontes, periodicidade e responsáveis. Este capítulo estabelece as famílias mínimas de indicadores:

a) vulnerabilidades por severidade, exposição, idade e situação;

b) tempo de tratamento e reincidência;

c) cobertura e resultado dos scans e testes;

d) sistemas com inventário de dados e avaliações de impacto;

e) incidentes, impacto, resposta e recorrência;

f) exceções e riscos residuais abertos;

g) conformidade dos gates;

h) capacitação e aderência de fornecedores; e

i) evolução da maturidade de segurança e privacidade.

Os resultados deverão retroalimentar o backlog de melhoria, os padrões técnicos, os planos de capacitação, a arquitetura, os contratos e a revisão periódica do PDS.

8. Governança de TI, Portfólio e Gestão de Dados

Governança: avaliar e direcionar	Gestão: planejar e coordenar	Operação: executar e evidenciar

LEITURA ORIENTADA: As responsabilidades são complementares e devem respeitar as competências institucionais.

A governança do Processo de Desenvolvimento de Software - PDS assegura que as iniciativas de software da SEMA/MT sejam avaliadas, direcionadas, priorizadas e monitoradas segundo objetivos institucionais, valor público, riscos, capacidade de execução e resultados. Este capítulo estabelece o modelo de direção e controle do PDS, complementando o fluxo operacional do Capítulo 3, os papéis do Capítulo 9 e o catálogo de métricas do Capítulo 13.

8.1 Objetivos e princípios de governança

A governança do PDS tem por objetivos alinhar as iniciativas de software à estratégia institucional; assegurar clareza decisória; otimizar recursos, riscos e benefícios; monitorar o desempenho; garantir transparência e responsabilização; e promover melhoria contínua.

a) alinhamento estratégico e geração de valor público;
b) transparência, prestação de contas e rastreabilidade das decisões;
c) responsabilização compatível com as competências regimentais;
d) otimização de riscos, recursos, capacidade e investimentos;
e) proporcionalidade dos controles ao porte, à criticidade e ao risco;
f) sustentabilidade técnica, econômica, operacional e institucional;
g) decisão baseada em evidências e dados confiáveis; e
h) melhoria contínua orientada por resultados e lições aprendidas.

A governança deverá evitar tanto decisões técnicas desconectadas das necessidades institucionais quanto decisões funcionais que desconsiderem viabilidade, arquitetura, segurança, dados, capacidade e sustentabilidade.

8.2 Distinção entre governança, gestão e operação

Governança, gestão e operação são dimensões complementares, mas não equivalentes. A autoridade e a responsabilidade exercidas em cada dimensão deverão ser explicitadas nas decisões e registros do PDS.

Nível	Função predominante	Exemplos no PDS
Governança	Avaliar, direcionar, priorizar e monitorar.	Aprovar diretrizes, decidir prioridades, aceitar riscos, acompanhar resultados e deliberar sobre exceções relevantes.
Gestão	Planejar, coordenar, acompanhar e tratar desvios.	Organizar portfólio, capacidade, contratos, riscos, cronogramas, dependências e planos de ação.
Operação	Executar, registrar, testar, entregar e sustentar.	Analisar demandas, desenvolver, testar, implantar, operar, monitorar e produzir evidências.

Uma mesma unidade poderá participar de mais de uma dimensão, desde que a autoridade exercida em cada decisão esteja clara e sejam preservadas a segregação de funções e as competências institucionais.

8.3 Estrutura decisória do PDS

A estrutura decisória do PDS observará o Regimento Interno, as designações formais e os instrumentos aplicáveis. Conforme a matéria e o impacto, poderão participar a Alta Administração, a STI, instâncias colegiadas existentes, CPQSI, CSTI, CITI, áreas demandantes, responsáveis por arquitetura, segurança, dados e operação, além da fiscalização e da gestão contratual.

O Capítulo 9 define as responsabilidades e autoridades. Este capítulo disciplina como essas instâncias utilizam informações do portfólio, riscos, capacidade, arquitetura, contratos, dados e indicadores para decidir.

Não serão criados comitês ou níveis de aprovação apenas por conveniência documental. A formalidade deverá ser proporcional ao impacto da decisão, sem eliminar controles obrigatórios ou autoridades legalmente competentes.

8.4 Governança do portfólio de demandas e produtos

O portfólio institucional deverá consolidar iniciativas de novos produtos, evolução, manutenção, sustentação, modernização, segurança, dívida técnica, dados, inteligência artificial, integrações, infraestrutura associada ao software e descontinuação.

Informação mínima	Finalidade
Responsável e área patrocinadora	Identificar autoridade funcional e ponto de decisão.
Problema, necessidade e valor esperado	Justificar a iniciativa e o resultado público pretendido.
Situação, prioridade e dependências	Permitir ordenação e coordenação do fluxo.
Risco e criticidade	Definir controles, aprovações e urgência.
Estimativa, capacidade e fonte de recursos	Avaliar viabilidade e momento de execução.
Modalidade de execução	Distinguir equipe interna, fábrica, contratação específica ou solução adquirida.
Resultados e indicadores esperados	Permitir avaliação posterior do valor entregue.

O Redmine constituirá a fonte operacional para demandas, estados, responsáveis, prioridades, versões e evidências. O GovFlow poderá consolidar e validar os dados do portfólio, produzir painéis e apoiar alertas, sem substituir a autoridade das instâncias decisórias.

8.5 Priorização institucional e alocação de capacidade

A priorização deverá considerar obrigação legal ou regulatória, risco, impacto ambiental, impacto ao cidadão, valor público, urgência, criticidade, dependências, esforço, custo, alinhamento estratégico, segurança, dívida técnica e disponibilidade contratual.

A decisão de prioridade deverá ser registrada com critérios, justificativa, responsáveis e data. Alterações significativas de prioridade deverão preservar o histórico e avaliar impactos sobre iniciativas em andamento.

A capacidade deverá ser tratada como recurso finito. O planejamento deverá equilibrar, conforme o contexto institucional:

a) novos produtos e funcionalidades;

b) manutenção e sustentação;

c) segurança e conformidade;

d) modernização e redução de obsolescência;

e) dívida técnica e arquitetural; e

f) atividades de dados, integração e melhoria operacional.

A reserva ou distribuição de capacidade deverá ser revista periodicamente. O PDS não fixa percentuais universais, pois a composição depende do portfólio, dos riscos, dos contratos e das prioridades vigentes.

8.6 Governança de riscos, conformidade e exceções

A governança deverá acompanhar riscos de portfólio, projetos, arquitetura, segurança, dados, operação, contratação, dependência tecnológica e continuidade. Os riscos relevantes deverão possuir responsável, avaliação, resposta, prazo e evidências de acompanhamento.

Exceções a padrões, gates, controles ou artefatos somente poderão ser concedidas mediante registro formal contendo:

a) regra ou controle objeto da exceção;
b) justificativa e contexto;
c) risco e impacto;
d) controles compensatórios;
e) responsável pela regularização;
f) autoridade aprovadora;
g) prazo e data de revisão; e
h) plano de tratamento ou encerramento.

A aceitação de risco deverá ser realizada por autoridade competente. Ferramentas e automações poderão registrar ou bloquear o fluxo, mas não poderão aceitar riscos em nome da instituição.

8.7 Governança da arquitetura e das decisões tecnológicas

A governança da arquitetura deverá assegurar coerência entre processos, aplicações, dados, integrações, infraestrutura, segurança e objetivos institucionais. Decisões relevantes deverão ser justificadas, versionadas e vinculadas às demandas e requisitos que as originaram.

Serão governados, conforme aplicável: princípios arquiteturais, padrões, tecnologias homologadas, decisões arquiteturais, ADRs, baselines, integrações, requisitos não funcionais, obsolescência, dívida arquitetural, modernização e exceções.

O Enterprise Architect poderá atuar como repositório institucional dos modelos, baselines e rastreabilidade técnica. Decisões de baixo impacto poderão seguir padrões previamente aprovados, sem necessidade de deliberação colegiada específica.

8.8 Governança das ferramentas, registros e automações

As ferramentas que operacionalizam o PDS deverão possuir administração funcional, técnica e de segurança claramente atribuída. Mudanças relevantes em configurações, workflows, permissões, integrações e automações deverão ser controladas.

A governança abrangerá, no mínimo:

a) trackers, status, campos, perfis e workflows do Redmine;
b) regras, templates, integrações, credenciais e versões do GovFlow;
c) modelos, permissões e baselines do Enterprise Architect;
d) grupos, repositórios, branches, pipelines, runners e permissões do Git/GitLab;
e) logs, trilhas de auditoria, backup, recuperação e continuidade das ferramentas; e
f) documentação e testes das mudanças de configuração.

Mudanças relevantes deverão seguir solicitação, análise de impacto, validação, teste, aprovação, implantação e documentação. O GovFlow não poderá criar ou alterar regras institucionais sem aprovação formal.

8.9 Governança de fornecedores, contratos e Ordens de Serviço

A governança contratual deverá integrar informações técnicas, administrativas, financeiras e de desempenho. O acompanhamento da fábrica não se limitará à contagem de entregas ou consumo contratual, devendo avaliar qualidade, prazo, segurança, rastreabilidade, documentação, transferência de conhecimento e valor entregue.

Deverão ser monitorados, conforme aplicável:

a) vigência, saldo e capacidade contratual;
b) Ordens de Serviço, escopo, produtos, prazos e responsáveis;
c) níveis de serviço e indicadores contratuais;
d) retrabalho, reincidência, defeitos reabertos e não conformidades;
e) evidências, medição, glosas e recebimentos;
f) riscos, dependência do fornecedor e continuidade; e
g) transferência e preservação do conhecimento institucional.

Painéis gerenciais poderão combinar dados do Redmine, GovFlow, Git/GitLab, ferramentas de CI/CD e registros contratuais, desde que as fontes e regras de consolidação sejam documentadas.

8.10 Governança de dados

Os dados produzidos, tratados ou compartilhados pelos sistemas deverão ser governados como ativos institucionais. A governança de dados deverá assegurar finalidade, responsabilidade, qualidade, integridade, segurança, disponibilidade, interoperabilidade, rastreabilidade, minimização, preservação e descarte adequado.

As decisões de dados deverão ser tomadas em conjunto pelas áreas de negócio e pelas unidades técnicas competentes. A TI é custodiante de muitos ativos e plataformas, mas não é proprietária exclusiva do significado, da finalidade ou das regras de negócio dos dados.

8.11 Papéis na gestão e curadoria de dados

Papel	Responsabilidade predominante
Proprietário do dado	Autoridade de negócio sobre o domínio, finalidade, regras, acesso e qualidade esperada.
Gestor ou responsável pelo dado	Coordena a aplicação das decisões, controles e prioridades do domínio.
Curador de dados	Atua na definição, metadados, qualidade, consistência e resolução de problemas.
Custodiante técnico	Mantém armazenamento, disponibilidade, backup, proteção e controles técnicos.
Produtor de dados	Origina ou registra dados segundo regras definidas.
Consumidor de dados	Utiliza dados em processos, serviços, análises ou decisões, observando as regras de uso.

A designação desses papéis deverá considerar os domínios e processos institucionais. Eles não serão atribuídos automaticamente a uma única unidade de tecnologia.

8.12 Qualidade, metadados, linhagem e interoperabilidade

A qualidade dos dados deverá ser avaliada segundo dimensões adequadas ao uso, como completude, validade, consistência, unicidade, atualidade, precisão, conformidade e integridade referencial.

Os sistemas e produtos de dados deverão documentar, conforme aplicável, conceito, domínio, origem, produtor, responsável, classificação, formato, regras, transformações, relacionamentos e usos relevantes.

A linhagem deverá permitir identificar de onde o dado veio, como foi transformado, onde foi armazenado e onde é utilizado. A interoperabilidade deverá utilizar padrões, contratos e identificadores consistentes, evitando integrações informais e duplicação descontrolada.

8.13 Ciclo de vida, retenção e descarte de dados

O ciclo de vida dos dados compreenderá criação ou coleta, validação, uso, compartilhamento, armazenamento, atualização, arquivamento, retenção e eliminação. Os requisitos deverão ser definidos desde a concepção da solução e revistos durante sua operação e descontinuação.

Os prazos de retenção e as formas de descarte deverão considerar legislação, necessidades administrativas, valor histórico, segurança, privacidade, auditoria, continuidade e requisitos do domínio. A eliminação deverá ser segura, verificável e compatível com backups e réplicas, quando aplicável.

8.14 Uso de dados, analytics e inteligência artificial

Iniciativas de analytics, ciência de dados e inteligência artificial deverão observar finalidade clara, qualidade e representatividade dos dados, origem e licitude, documentação, controle de acesso, versionamento, rastreabilidade, avaliação de desempenho, segurança e privacidade.

Conforme o risco e o impacto, também deverão ser avaliados vieses, explicabilidade, supervisão humana, reprodutibilidade, monitoramento de degradação, controle de modelos e possibilidade de contestação ou revisão das decisões apoiadas por algoritmos.

Os detalhes técnicos e critérios especializados poderão ser mantidos em guias versionados, desde que referenciados pelo PDS e submetidos à governança institucional.

8.15 Referenciais de governança

O PDS utiliza como referências, conforme aplicável, COBIT, ITIL, normas ISO relacionadas, DAMA-DMBOK, planejamento estratégico, Regimento Interno, políticas estaduais e normativos institucionais.

A utilização desses referenciais será seletiva e proporcional. O PDS não declara conformidade integral com um framework ou norma sem avaliação específica de aderência, evidências e aprovação institucional.

Do COBIT, serão especialmente considerados os princípios de alinhamento estratégico, entrega de benefícios, otimização de riscos e recursos, monitoramento, responsabilização, gestão de fornecedores, qualidade, segurança e continuidade.

8.16 Governança dos indicadores e resultados

Indicadores deverão apoiar perguntas de gestão e decisões concretas. O catálogo detalhado de métricas, fórmulas, metas e periodicidades será mantido no Capítulo 13 ou em catálogo institucional versionado.

Elemento obrigatório	Descrição
Nome e objetivo	Identificação clara e finalidade gerencial.
Pergunta de gestão	Decisão ou problema que o indicador ajuda a avaliar.
Fórmula e fonte	Regra de cálculo e sistemas de origem.
Periodicidade e responsável	Frequência, produtor e responsável pela qualidade.
Meta, faixa ou referência	Parâmetro de interpretação, quando aplicável.
Limitações	Restrições, vieses e condições de uso.
Ação esperada	Providência a ser considerada diante do resultado.

Indicadores sem decisão associada, fonte confiável ou interpretação documentada não deverão ser mantidos apenas para composição de painéis.

8.17 Avaliação de maturidade e melhoria contínua

A maturidade do PDS deverá ser avaliada periodicamente, considerando capacidade e resultados, e não apenas quantidade de documentos. A avaliação poderá abranger processo, pessoas, ferramentas, automação, requisitos, arquitetura, qualidade, segurança, dados, contratos, métricas e operação.

Nível conceitual	Caracterização
Inicial	Práticas dependentes de pessoas, pouco padronizadas e com evidências limitadas.
Definido	Processos, papéis e critérios documentados e aplicados de forma consistente.
Gerenciado	Acompanhamento sistemático de capacidade, riscos, qualidade e desempenho.
Medido	Decisões apoiadas por dados confiáveis, metas e análise de tendências.
Otimizado	Melhoria contínua, automação responsável e adaptação baseada em resultados.

A avaliação deverá produzir plano de melhoria priorizado, com responsáveis, prazos, benefícios esperados e acompanhamento. A evolução poderá ocorrer de forma distinta entre dimensões e produtos.

8.18 Transparência, prestação de contas e auditoria

A governança do PDS deverá preservar histórico de decisões, autoria, evidências, relatórios, trilhas de auditoria, riscos, exceções e resultados. O acesso às informações deverá observar transparência, necessidade de conhecimento, proteção de dados e segurança.

A prestação de contas deverá permitir compreender o que foi priorizado, executado, entregue, recebido, adiado, cancelado ou excepcionalizado, bem como as justificativas e os resultados associados.

As avaliações e auditorias deverão considerar tanto a conformidade com o processo quanto sua efetividade, evitando que o cumprimento meramente formal de documentos substitua a análise de qualidade, risco e valor público.

Os achados deverão gerar ações de melhoria rastreáveis, acompanhadas até sua conclusão ou aceitação formal do risco correspondente.


SEMA
Secretaria
de Estado de
Meio Ambiente
Governo de
Mato
Grosso
Governança, Portfólio, Dados e Decisão
Direcionamento institucional, priorização, gestão de dados e apoio à tomada de decisão no ciclo de vida de software.
PDS v2.0
5 PILARES do PDS
1 GOVERNANÇA
Estabelece diretrizes, papéis e responsabilidades para decisões alinhadas à estratégia institucional.
2 PORTFÓLIO
Prioriza e balanceia iniciativas de software com base em valor, risco, capacidade e dependências.
3 DADOS
Garante qualidade, segurança, integração e uso estratégico dos dados ao longo do ciclo de vida de software.
4 DECISÃO
Apoia a tomada de decisão com informações confiáveis, indicadores e inteligência institucional.
5 CICLO DE VIDA
Assegura práticas modernas em todas as fases do ciclo de vida de software de forma contínua e colaborativa.
MICROFLUXO do Ciclo
1. DEMANDA
Identificação de necessidades e oportunidades.
2. ANÁLISE
Avaliação de valor, viabilidade, riscos e dependências.
3. PRIORIZAÇÃO
Seleção das iniciativas com base em critérios e capacidade.
4. EXECUÇÃO
Desenvolvimento com qualidade, segurança e colaboração.
5. MONITORAMENTO
Acompanhamento de entregas, indicadores e desempenho.
6. RESULTADOS
Geração de valor, aprendizado e melhoria contínua.
PRINCÍPIOS que orientam
Valor Público e Impacto
Transparência e Prestação de Contas
Segurança e Privacidade
Colaboração e Integração
Eficiência e Sustentabilidade
Aprendizado e Melhoria Contínua
FERRAMENTAS de apoio
Catálogo de Sistemas e Serviços
Painel de Portfólio e Indicadores
Repositório de Dados e Metadados
Gestão de Demandas e Prioridades
Frameworks e Boas Práticas
Capacitação e Comunidades de Prática

9. Papéis e Responsabilidades

LEITURA ORIENTADA: Este capítulo estabelece as responsabilidades, autoridades e relações de participação aplicáveis ao Processo de Desenvolvimento de Software da SEMA/MT. Seu propósito é assegurar que cada atividade possua executor, responsável institucional, aprovador e participantes claramente identificados, evitando sobreposição, lacunas e conflitos de competência.

As atribuições previstas neste capítulo complementam o Regimento Interno, os atos de designação, os instrumentos de contratação e os demais normativos aplicáveis. Em caso de conflito, prevalecem as competências legais e regimentais e as responsabilidades formalmente estabelecidas no processo administrativo ou no contrato.

9.1 Princípios de atribuição e segregação de responsabilidades

- A unidade organizacional não se confunde com o papel exercido no processo. Uma mesma unidade poderá desempenhar papéis distintos, e um papel poderá ser exercido por pessoas de unidades diferentes, conforme a iniciativa e a designação formal.
- Ferramentas e automações registram, validam ou encaminham atividades, mas não substituem a responsabilidade e a autoridade institucional de quem decide, aprova, homologa, aceita ou recebe.
- As responsabilidades de especificar, executar, revisar, validar, homologar, fiscalizar e receber deverão ser segregadas de forma compatível com a criticidade, o risco e a modalidade de execução.
- A área de negócio responde pela necessidade, pelas regras funcionais e pela homologação; a TI responde pela análise, pela solução técnica, pela qualidade técnica e pela coordenação do ciclo de software.
- A responsabilidade contratual é distinta da responsabilidade técnica. A validação técnica não equivale, por si só, ao recebimento contratual definitivo.
- Toda designação deverá ser registrada no Redmine ou no sistema administrativo competente, com vínculo à demanda, ao projeto, à Ordem de Serviço ou ao contrato correspondente.
- As responsabilidades e os artefatos serão aplicados proporcionalmente ao porte, à complexidade, à criticidade e aos riscos da iniciativa.

9.2 Estrutura de papéis do PDS

Os papéis do PDS são organizados em quatro grupos complementares:

- papéis institucionais e de governança, relacionados à direção, priorização, método, conformidade e resolução de conflitos;
- papéis de negócio, relacionados à necessidade, ao valor público, às regras funcionais, à validação e à homologação;
- papéis técnicos e operacionais, relacionados à análise, arquitetura, desenvolvimento, testes, infraestrutura, implantação, operação e suporte;
- papéis contratuais, relacionados à autorização, fiscalização, medição, recebimento, gestão e responsabilização do fornecedor.

Os papéis ágeis, como Responsável pelo Produto, Facilitador do Fluxo ou Scrum Master, serão designados conforme a iniciativa e não alteram as competências regimentais das unidades. Não se adota equivalência automática entre CSTI e Product Owner, nem entre CPQSI e Scrum Master.

9.3 Área demandante, Gestor do Negócio e usuários-chave

9.3.1 Área demandante

- registrar formalmente a necessidade, o problema ou a oportunidade;
- apresentar justificativa, resultados esperados, impactos, urgência e vínculos estratégicos ou legais;
- designar o Gestor do Negócio e indicar usuários-chave e homologadores;
- fornecer informações, regras, documentos, dados e acesso aos especialistas do domínio;
- participar do refinamento, da validação dos requisitos, da homologação e da avaliação dos resultados;
- assegurar disponibilidade dos representantes do negócio durante o ciclo da demanda.

9.3.2 Gestor do Negócio

- representar funcionalmente a área demandante;
- detalhar a necessidade, o benefício esperado e as regras de negócio;
- validar histórias de usuário, requisitos, critérios de aceitação, protótipos e fluxos;
- participar da priorização e comunicar mudanças de necessidade;
- coordenar a homologação funcional e registrar o resultado;

- confirmar o atendimento ao escopo funcional e ao valor esperado;
- registrar pendências, restrições e riscos funcionais.

9.3.3 Usuários-chave e homologadores

- contribuir com conhecimento operacional e cenários reais de uso;
- validar fluxos, terminologia, dados e regras específicas;
- executar os roteiros de homologação na versão e no ambiente indicados;
- registrar evidências, resultados, defeitos e observações no Redmine;
- não aprovar tecnicamente arquitetura, segurança ou infraestrutura, salvo quando formalmente designados para função técnica.

9.4 Governança e direção institucional

9.4.1 Superintendência de Tecnologia da Informação - STI

- coordenar institucionalmente o PDS e patrocinar sua melhoria contínua;
- aprovar diretrizes, padrões e modelos de governança de software no âmbito de sua competência;
- deliberar ou encaminhar prioridades, conflitos de capacidade e exceções relevantes;
- acompanhar portfólio, riscos, indicadores e resultados das iniciativas;
- articular as unidades de tecnologia, áreas demandantes, instâncias estratégicas e gestão contratual;
- definir autoridades técnicas e instâncias de escalonamento quando necessário.

9.4.2 CPQSI - governança do processo, qualidade e segurança da informação

- manter, avaliar e propor evolução do método e dos controles do PDS;
- definir ou apoiar padrões de qualidade, segurança, conformidade e gestão de riscos;
- acompanhar indicadores, auditorias, exceções e planos de melhoria;
- orientar a adoção metodológica e apoiar capacitações;
- avaliar a aderência do processo, sem assumir automaticamente a execução operacional das cerimônias ágeis;
- não homologar em nome da área de negócio nem substituir a validação técnica da CSTI ou a fiscalização contratual.

9.4.3 Instâncias estratégicas e unidades de assessoramento

O NGER, o CGE, o Gabinete, a Unidade de Assessoria e outras instâncias participarão quando a iniciativa exigir alinhamento estratégico, decisão de portfólio, patrocínio, avaliação de resultados, resolução de conflitos institucionais ou manifestação especializada. Sua participação não é automática em todas as demandas e deverá observar suas competências formais.

9.5 Coordenação, análise e gestão técnica

9.5.1 Coordenadoria de Sistemas de Tecnologia da Informação - CSTI

- realizar a triagem e a análise técnica inicial das demandas;
- conduzir ou coordenar a elicitação e a estruturação de requisitos, histórias de usuário e critérios técnicos;
- avaliar viabilidade, dependências, integrações, impactos e riscos técnicos;
- organizar e manter o backlog técnico e a rastreabilidade no Redmine;
- coordenar a análise de solução, arquitetura, estimativas e planejamento da execução;
- acompanhar a equipe interna ou a fábrica contratada durante o desenvolvimento;
- validar tecnicamente código, testes, documentação, segurança, evidências e entregas;
- coordenar a preparação para homologação, implantação, sustentação e evolução;
- emitir ou subsidiar pareceres técnicos, sem substituir o recebimento contratual de competência dos agentes designados.

A CSTI responde institucionalmente pela coordenação e execução do processo de software, mas a implementação material poderá ser realizada por equipe interna, fábrica contratada ou modelo compartilhado.

9.5.2 Analista de requisitos ou de negócio

- planejar e realizar elicitação;
- analisar, modelar e documentar requisitos e regras de negócio;
- escrever histórias de usuário e critérios de aceitação;
- manter rastreabilidade entre demanda, requisitos, testes e entregas;
- apoiar validações e controle de mudanças;
- assegurar que a aprovação funcional seja realizada pelo Gestor do Negócio.

9.5.3 Responsável pelo Produto ou Backlog

- organizar, ordenar e manter o backlog;
- garantir clareza, granularidade e vínculo dos itens;
- preparar refinamentos e coordenar dependências;
- aplicar as decisões de priorização tomadas pelas instâncias competentes;
- promover visibilidade do fluxo e das versões;
- atuar em colaboração com o Gestor do Negócio e a CSTI.

9.5.4 Arquiteto ou responsável técnico

- avaliar e documentar a arquitetura e suas decisões relevantes;
- analisar requisitos não funcionais, integrações, dados, segurança e impactos;
- assegurar aderência aos padrões e à arquitetura corporativa;
- manter modelos e baselines no Enterprise Architect, quando aplicável;
- participar de análise de riscos, modernização e evolução tecnológica.

9.5.5 Líder técnico

- orientar a execução técnica e apoiar estimativas;
- revisar soluções, código e decisões de implementação;
- acompanhar impedimentos e dependências técnicas;
- verificar aderência aos padrões e à Definition of Done técnica;
- apoiar a transferência de conhecimento e a manutenção da documentação.

9.6 Infraestrutura, operação e suporte

9.6.1 Coordenadoria de Infraestrutura de Tecnologia da Informação - CITI

- avaliar requisitos de infraestrutura, capacidade, rede, banco de dados e plataforma;
- prover e administrar ambientes de desenvolvimento, homologação e produção conforme suas competências;
- assegurar controles de acesso, backup, monitoramento, continuidade e segurança técnica da infraestrutura;
- apoiar a preparação e a execução da implantação, incluindo contingência e rollback;
- registrar evidências operacionais e tratar incidentes de infraestrutura;
- participar do time de execução quando sua especialidade for necessária, sem ser considerada integrante fixa do Squad de desenvolvimento.

9.6.2 Gerência de Atendimento e Suporte Técnico

- registrar e classificar incidentes, solicitações e feedback dos usuários;
- aplicar procedimentos de atendimento e escalonamento;
- fornecer informações para manutenção, priorização e melhoria dos sistemas;
- participar da transição para operação e da comunicação com usuários;
- manter rastreabilidade entre atendimento, problema, mudança e demanda de evolução.

9.7 Segurança, privacidade, dados e conformidade

- A CPQSI atua na governança, nas políticas, na conformidade, na avaliação do processo e no acompanhamento de riscos.
- A CSTI atua na segurança de software, incluindo requisitos, arquitetura, validação técnica, acompanhamento de análises e tratamento de vulnerabilidades de aplicação.
- A CITI atua na segurança da infraestrutura, ambientes, redes, bancos, identidades técnicas, registros, backup e continuidade.
- A fábrica contratada implementa codificação segura, executa os controles previstos, corrige vulnerabilidades, atualiza dependências e fornece evidências.
- O Encarregado pelo Tratamento de Dados Pessoais e as áreas competentes de privacidade exercem suas atribuições legais e institucionais, sem assumir automaticamente a execução técnica do software.
- Os proprietários, gestores ou curadores de dados, quando designados, respondem pela definição semântica, qualidade, acesso, compartilhamento, retenção e uso adequado dos dados de seu domínio.
- A aceitação de risco residual deverá ser realizada pela autoridade competente conforme a natureza, o impacto e a criticidade do risco.

9.8 Equipes internas e fábrica contratada

9.8.1 Equipe interna de execução

- executar análise, arquitetura, desenvolvimento, testes, revisão, documentação e implantação conforme a composição e a capacidade definidas para a iniciativa;
- registrar atividades, código, testes, evidências e decisões nos repositórios oficiais;
- observar os mesmos critérios de qualidade, segurança, rastreabilidade e aceite aplicáveis à execução contratada.

9.8.2 Fábrica de software contratada

Quando acionada por instrumento formal, a fábrica será responsável pela execução dos produtos contratados, observando o PDS, o contrato, a Ordem de Serviço, o backlog aprovado, os critérios de aceitação e os padrões institucionais.

- apoiar tecnicamente o refinamento quando solicitado, sem substituir a aprovação funcional do negócio;
- elaborar e justificar estimativas;
- desenvolver, versionar, integrar, testar, corrigir e documentar;
- produzir relatórios, evidências, pacotes de entrega e registros exigidos;
- corrigir não conformidades, defeitos e vulnerabilidades atribuíveis à entrega;
- garantir transferência de conhecimento e atualização documental;
- cumprir níveis de serviço, prazos, perfis profissionais e demais obrigações contratuais.

9.8.3 Preposto da contratada

- atuar como interface formal entre contratada, fiscalização e equipes da SEMA/MT;
- coordenar a equipe e consolidar estimativas, entregas e comunicações;
- gerenciar impedimentos e providenciar correções;
- assegurar cumprimento dos registros, prazos e obrigações contratuais.

9.8.4 Qualidade e especialistas da contratada

- O profissional de qualidade ou QA planeja e executa testes, registra defeitos, regressões e evidências.
- Especialistas de arquitetura, banco de dados, DevOps, segurança, UX, dados ou outras áreas serão mobilizados conforme a necessidade e o instrumento contratual.
- A atuação de especialistas da contratada não substitui a validação e a autoridade técnica institucional da SEMA/MT.

9.9 Fiscalização e gestão contratual

9.9.1 Fiscal técnico

- acompanhar tecnicamente a execução da Ordem de Serviço;
- verificar aderência ao escopo, aos requisitos, critérios, padrões e produtos contratados;
- analisar evidências, estimativas, medições e ocorrências técnicas;
- registrar determinações, pendências, não conformidades e recomendações;

- emitir parecer técnico e recomendar aceite, correção, glosa ou outras providências, conforme sua competência.

9.9.2 Fiscal requisitante

- acompanhar o atendimento à necessidade institucional;
- considerar a manifestação do Gestor do Negócio e da área demandante;
- verificar a aderência funcional no âmbito de sua designação;
- subsidiar o recebimento e a avaliação do resultado contratado.

9.9.3 Fiscal administrativo

- verificar obrigações administrativas, documentais, trabalhistas, fiscais e demais exigências de sua competência;
- acompanhar prazos, registros e regularidade administrativa;
- comunicar ocorrências e subsidiar providências contratuais.

9.9.4 Gestor do contrato

- coordenar a gestão contratual e articular os fiscais;
- consolidar informações, riscos, saldo, vigência e desempenho;
- formalizar ou encaminhar decisões e providências de sua competência;
- coordenar os procedimentos de medição, recebimento, glosa, sanção e faturamento, quando aplicáveis;
- assegurar que nenhuma execução contratual seja iniciada sem instrumento formal válido.

9.10 Validação, homologação, aceite e recebimento

Etapa	Responsável principal	Objeto e resultado
Validação de requisitos	Gestor do Negócio	Confirma que histórias, regras, requisitos e critérios representam a necessidade institucional.
Validação técnica	CSTI e/ou Fiscal Técnico	Verifica arquitetura, código, testes, segurança, documentação, evidências e conformidade técnica.
Homologação funcional	Área demandante, Gestor do Negócio e homologadores	Executa cenários e confirma o comportamento funcional no ambiente e na versão indicados.
Aceite funcional	Gestor do Negócio ou autoridade funcional designada	Declara que a entrega atende ao escopo funcional e registra ressalvas ou pendências.
Recebimento provisório	Agente definido no contrato ou ato de designação	Formaliza o recebimento inicial dos produtos para verificação.
Recebimento definitivo	Agente ou comissão definidos nos instrumentos aplicáveis	Reconhece a conformidade após verificações técnicas, funcionais e contratuais.

Etapa	Responsável principal	Objeto e resultado
Autorização de faturamento	Autoridade competente	Autoriza o prosseguimento do pagamento após medição, glosas e recebimentos aplicáveis.

A conclusão de uma etapa não substitui as demais. A aprovação do pipeline, por exemplo, não equivale à homologação funcional; a homologação não equivale ao recebimento definitivo; e o registro no Redmine não substitui o termo formal exigido no processo administrativo.

9.11 Administração das ferramentas e repositórios

Para cada ferramenta institucional deverão ser designadas, no mínimo, as responsabilidades de administração funcional, administração técnica, segurança, continuidade e qualidade dos dados.

Ferramenta ou repositório	Responsabilidades mínimas
Redmine	Parametrização do processo, trackers, status, campos, papéis, permissões, qualidade cadastral, auditoria e suporte.
GovFlow	Regras declarativas, automações, integrações, credenciais, versionamento, observabilidade, validação e manutenção.
Enterprise Architect	Padrões de modelagem, repositório, baselines, permissões, integração e rastreabilidade arquitetural.
Git/GitLab	Grupos, projetos, permissões, branches, merge requests, pipelines, runners, retenção, segurança e disponibilidade.
Ambientes e plataformas	Acessos, capacidade, configuração, backup, monitoramento, continuidade, implantação e operação.

A designação nominal das unidades e dos administradores será detalhada no Capítulo 10 e em procedimentos operacionais. Credenciais pessoais não deverão ser compartilhadas, e as contas técnicas deverão possuir proprietário, finalidade, escopo e processo de revisão.

9.12 Matriz RACI do ciclo de vida

A matriz abaixo estabelece a referência geral. Matrizes específicas poderão detalhar projetos, contratos ou iniciativas críticas. Legenda: R - executa; A - responde e aprova; C - consultado; I - informado.

Atividade	R	A	C	I
Registrar demanda	Área demandante	Gestor do Negócio	CSTI	STI/partes interessadas
Realizar triagem	CSTI	CSTI	Área demandante, CITI	CPQSI
Elicitar e estruturar requisitos	Analista/CSTI	CSTI	Gestor do Negócio, usuários-chave	CPQSI
Validar requisitos funcionais	Gestor do Negócio	Gestor do Negócio	CSTI, usuários-chave	Partes interessadas
Analisar arquitetura e viabilidade técnica	CSTI/Arquiteto	Autoridade técnica definida	CITI, CPQSI, fábrica	Gestor do Negócio
Priorizar demanda	Responsável pelo Backlog	Instância competente	Gestor do Negócio, CSTI, STI	Fábrica e interessados
Estimar execução contratada	Fábrica	Preposto da contratada	CSTI, Fiscal Técnico	Gestor do Contrato
Autorizar Ordem de Serviço	Gestão contratual	Autoridade competente	CSTI, fiscais, demandante	Contratada
Desenvolver e testar	Equipe interna ou fábrica	Responsável pela execução	CSTI, CITI	Negócio e fiscalização
Validar tecnicamente	CSTI/Fiscal Técnico	Autoridade técnica ou Fiscal Técnico	CITI, CPQSI, fábrica	Gestor do Negócio
Homologar funcionalmente	Homologadores	Gestor do Negócio	CSTI, fábrica	Fiscalização
Implantar	CSTI/CITI/fábrica	Responsável técnico-operacional	Negócio, segurança, fiscalização	Usuários e suporte
Emitir parecer técnico	CSTI/Fiscal Técnico	Fiscal Técnico ou autoridade definida	CITI, Gestor do Negócio	Gestão contratual
Receber contratualmente	Agentes designados	Autoridade definida	Fiscalização, CSTI, negócio	Contratada
Auditar o processo	CPQSI/controle competente	Autoridade de governança	CSTI, CITI, fiscalização	STI e envolvidos

9.13 Matriz de autoridade decisória

Decisão	Autoridade principal	Condição ou evidência
Confirmar necessidade e benefício	Gestor do Negócio	Registro formal da demanda.
Aceitar ou devolver demanda na triagem	CSTI	Critérios de completude e competência.
Aprovar requisitos funcionais	Gestor do Negócio	Histórias, regras, critérios e protótipos.
Aprovar solução técnica	Autoridade técnica definida pela STI	Arquitetura, integrações e requisitos não funcionais.
Priorizar institucionalmente	Instância competente de priorização	Critérios de valor, risco, urgência, capacidade e estratégia.
Aprovar estimativa técnica	CSTI e/ou Fiscal Técnico	Coerência técnica e contratual da estimativa.
Autorizar execução contratual	Autoridade competente	Ordem de Serviço ou instrumento equivalente.
Aprovar tecnicamente a entrega	CSTI e/ou Fiscal Técnico	Evidências e critérios técnicos.
Homologar funcionalmente	Gestor do Negócio	Resultado dos cenários de homologação.
Autorizar implantação	Autoridades técnica e operacional definidas	Gates, plano, segurança, contingência e janela.
Receber contratualmente	Agentes definidos nos instrumentos aplicáveis	Termos e verificações requeridos.
Aprovar exceção metodológica	Autoridade de governança definida	Justificativa, risco e prazo de regularização.
Aceitar risco residual	Autoridade competente conforme criticidade	Risco documentado, controles e impacto.

9.14 Escalonamento, conflitos, impedimentos e exceções

- Impedimentos operacionais deverão ser registrados no Redmine e tratados inicialmente pelos responsáveis diretos.
- Conflitos funcionais serão escalados ao Gestor do Negócio e à autoridade da área demandante.
- Conflitos técnicos serão escalados à CSTI e, quando necessário, à STI ou à autoridade técnica designada.
- Conflitos contratuais serão tratados pela fiscalização e pela gestão contratual nos sistemas administrativos competentes.
- Conflitos de prioridade, capacidade ou valor institucional serão encaminhados à instância de priorização competente.
- Exceções ao PDS deverão possuir justificativa, análise de risco, autoridade aprovadora, prazo, controles compensatórios e registro rastreável.

• Nenhuma exceção poderá afastar obrigação legal, regimental ou contratual.

9.15 Modelo de interação institucional

O modelo de interação do PDS adota o seguinte encadeamento: a área demandante registra e qualifica a necessidade; a CSTI realiza triagem, análise e estruturação; as instâncias competentes priorizam; a equipe interna ou a fábrica executa; a CSTI e os agentes técnicos validam; a área demandante homologa; a infraestrutura coordena ou apoia a implantação; e a fiscalização e a gestão contratual realizam os atos de recebimento de sua competência.

O Redmine manterá os registros operacionais e a rastreabilidade do fluxo. O GovFlow apoiará validações, automações e integrações. O Enterprise Architect manterá os modelos arquiteturais aplicáveis. Git/GitLab e as ferramentas de CI/CD manterão código, revisões, testes e evidências técnicas. Os atos administrativos e contratuais permanecerão nos sistemas oficiais correspondentes, vinculados à demanda ou à Ordem de Serviço.

Diagramas oficiais do modelo de interação poderão ser mantidos nos anexos ou no repositório institucional de arquitetura. Código-fonte de diagramas, como Mermaid, deverá permanecer em repositório versionado, e não no corpo principal deste PDS.

SEMA Secretaria de Estado de Meio Ambiente | Governo de Mato Grosso

Papéis e Responsabilidades

PDS v2.0

Atores, atribuições e interações no Processo de Desenvolvimento de Software

1 Área Demandante / Unidade Finalística

identifica a necessidade, define regras de negócio, valida requisitos, homologa a solução e apoia o aceite funcional.

2 Gestor do Negócio

representa o negócio, prioriza demandas, esclarece requisitos, define valor esperado e acompanha a entrega.

3 CSTI

analisa tecnicamente a demanda, apoia requisitos, coordena fluxo técnico, valida arquitetura, testes e evidências.

4 CPQSI

acompanha qualidade do processo, conformidade, padrões, riscos, indicadores e melhoria contínua.

5 CITI

provê infraestrutura, ambientes, publicação, operação técnica e suporte à implantação.

6 Fábrica de Software / Contratada

implementa a solução, produz código e artefatos, executa testes, corrige falhas e entrega evidências.

7 Fiscal Técnico / Fiscal Requisitante

acompanha execução, verifica conformidade, registra medições, analisa entregas, homologação, SLA e recebimentos.

8 Governança / Gestão

define diretrizes, aprova prioridades, acompanha resultados, trata exceções e assegura alinhamento institucional.

Responsabilidades-chave por etapa

1 Demanda	2 Análise	3 Requisitos	4 Execução	5 Testes e Validação	6 Homologação e Recebimento	7 Implantação e Sustentação
Área Demandante + Gestor do Negócio	Gestor do Negócio + CSTI	Área Demandante + Gestor do Negócio + CSTI	Fábrica de Software / Contratada + CSTI	CSTI + Fábrica + Área Demandante	Área Demandante + Fiscal + CSTI	CITI + Fábrica + CSTI + Fiscal

Princípios de atuação

- Segregação de responsabilidades
- Rastreabilidade
- Colaboração entre negócio e TI
- Qualidade e segurança por padrão
- Evidências e conformidade
- Melhoria contínua

Os papéis podem atuar de forma colaborativa, mas as decisões formais e as evidências devem permanecer claramente atribuídas e registradas.


Fluxo Integrado de Desenvolvimento, Implantação e Sustentação
Visão institucional das interações entre áreas no ciclo do PDS
NGER
UPPE
STI
CSTI
CITI
CPQSI
Unidades Finalísticas (SGDD, SPGAI, SRMA, SMCB, SF, SEAAC, SMIS, SGF, SGRH, DUD)
1 Planejamento
2 Desenvolvimento
3 Validação/ Qualidade
4 Implantação
5 Homologação
6 Sustentação
1 Demandas e Priorização
2 Análise de Viabilidade e Planejamento
3 Arquitetura da Solução e Plano do Projeto
4 Estimativas e Alocação de Recursos
5 Análise de Segurança e Conformidade
6 Plano de Testes e Qualidade
7 Especificação da Demanda e Requisitos
Loop de Desenvolvimento
8 Desenvolvimento (Construção da Solução)
9 Ambiente de Desenvolvimento e Infraestrutura
10 Revisão de Código e Boas Práticas
11 Testes Unitários e Integração Contínua
12 Acompanhamento e Feedback
13 Build de Validação
14 Ambiente de Validação
15 Testes de Segurança e Conformidade
16 Testes Funcionais e Não Funcionais
17 Validação com Usuários
18 Preparação da Implantação
19 Ambiente de Pré-Produção
20 Checklist de Segurança
21 Plano de Implantação
22 Treinamento e Comunicação
23 Deploy para Homologação
24 Ambiente de Homologação
25 Validação de Segurança Final
26 Execução do Plano de Testes
27 Homologação Formal
28 Deploy em Produção
29 Ambiente de Produção
30 Monitoramento de Segurança
31 Monitoramento de Qualidade (SLAs)
32 Operação e Suporte ao Usuário
Loop de Sustentação
Fluxo principal
Sequência normal do processo
Fluxo de retorno/relatório
Feedback, relatórios e aprovações
Loop de desenvolvimento e sustentação
Processos iterativos e contínuos

10. Ferramentas, Plataformas e Integrações do PDS

Redmine	GovFlow	EA	Git/GitLab	CI/CD	OpenShift	Observabilidade

> **LEITURA ORIENTADA:** Este capítulo define o ecossistema de ferramentas, plataformas e integrações que operacionaliza o Processo de Desenvolvimento de Software - PDS da SEMA/MT. As ferramentas apoiam o processo, mas não substituem competências, responsabilidades, aprovações ou decisões institucionais.

10.0 Visão integrada do ecossistema de ferramentas

O ecossistema tecnológico do PDS distribui responsabilidades entre plataformas especializadas e mantém o GovFlow como camada de orquestração e validação. Cada conjunto de informação possui fonte oficial, evitando duplicidade, divergência e perda de rastreabilidade.

Princípio de governança: integrações e automações apoiam o trabalho, mas não alteram competências institucionais nem substituem decisões humanas, homologações, aceites ou recebimentos formais.


SEMA
SECRETARIA DE ESTADO DE MEIO AMBIENTE
GOVERNO DE MATO GROSSO
ECOSSISTEMA INTEGRADO DE FERRAMENTAS DO PDS
PDS v2.0
Fontes oficiais, automação, rastreabilidade e integração entre gestão, arquitetura, código, entrega e operação
RM
Redmine
Demandas, backlog, requisitos, tarefas, riscos, homologação e decisões.
EA
Enterprise Architect
Processos, BPMN, arquitetura, requisitos complexos, dados e integrações.
GT
Git / GitLab
Código-fonte, branches, merge requests, pipelines, tags e releases.
GF
GovFlow
Orquestração, automação e validação
• regras do PDS
• integrações entre plataformas
• trilhas, alertas e consolidação
Rastreabilidade ponta a ponta • fontes oficiais • integração controlada
ADM
Sistemas Administrativos
Processos oficiais, contratação, OS, recebimentos, faturamento e documentos.
CI
CI/CD e DevSecOps
Builds, testes unitários e de integração, SAST, SCA, DAST, SBOM e artefatos.
OS
OpenShift / Ambientes
Execução, contêineres, deploy, configuração, escalabilidade e rollback.
OBS
Observabilidade
Logs, métricas, traces, alertas e painéis operacionais.

10.1 Objetivos e princípios

O ecossistema tecnológico do PDS deverá assegurar fonte oficial da informação, integração, rastreabilidade, interoperabilidade, automação responsável, segurança, auditabilidade, continuidade, portabilidade e evolução controlada.

a) cada tipo de informação deverá possuir fonte oficial definida;

b) registros não serão duplicados sem finalidade e responsabilidade claras;

c) integrações deverão preservar autoria, histórico e rastreabilidade;

d) automações não substituirão manifestações formais de autoridades competentes;

e) soluções deverão evitar dependência tecnológica desnecessária e permitir evolução;

f) ferramentas críticas deverão possuir administração, segurança e continuidade definidas; e

g) configurações, integrações e mudanças deverão ser versionadas e documentadas.

10.2 Arquitetura do ecossistema de ferramentas

O ecossistema do PDS será organizado em camadas complementares. A adoção de uma ferramenta em determinada camada não impede o uso de outra solução homologada, desde que sejam preservadas as funções, os controles e as fontes oficiais definidas neste capítulo.

Camada	Finalidade predominante	Componentes institucionais
Negócio e processo	Registrar demandas, backlog, decisões, aprovações, evidências e estados.	Redmine, GovFlow, ferramentas de atendimento e sistemas administrativos oficiais.
Modelagem e arquitetura	Representar processos, requisitos complexos, arquitetura, dados e integrações.	Enterprise Architect e repositórios arquiteturais aprovados.
Desenvolvimento e entrega	Versionar código, infraestrutura como código, documentação, pipelines e artefatos.	Git/GitLab e ferramentas de CI/CD.
Execução	Hospedar aplicações, serviços, contêineres, bancos e componentes técnicos.	OpenShift e demais plataformas homologadas.
Segurança e qualidade	Executar testes, análises, scans, gates e geração de evidências.	Ferramentas DevSecOps integradas aos pipelines.
Observabilidade e operação	Coletar logs, métricas, rastreamento, alertas e painéis.	Plataformas de monitoramento e observabilidade.

10.3 Redmine como plataforma operacional do PDS

O Redmine será a plataforma operacional e a fonte oficial dos registros do fluxo do PDS, conforme parametrização institucional. Deverá concentrar informações suficientes para demonstrar quem solicitou, analisou, decidiu, executou, validou, homologou e recebeu cada entrega.

Deverão ser registrados, conforme aplicável:

a) demanda, área demandante, Gestor do Negócio e responsáveis;
b) classificação, prioridade, criticidade, riscos e dependências;
c) épicos, funcionalidades, histórias de usuário, requisitos e critérios de aceite;
d) tarefas, subtarefas, defeitos, incidentes, problemas e mudanças;
e) versões, releases, ambientes, homologações e aceitações;
f) evidências, pareceres, termos, referências contratuais e decisões; e
g) relações entre itens e histórico de transições.

A configuração institucional deverá abranger trackers, status, workflows, campos personalizados, papéis, permissões, projetos, categorias, versões, relações, notificações e relatórios. Alterações relevantes deverão seguir o processo de governança definido neste capítulo.

10.4 GovFlow como camada de orquestração e automação

O GovFlow atuará como camada de orquestração, automação, integração e validação das regras do PDS. Sua arquitetura declarativa poderá padronizar projetos, recursos, workflows, trackers, papéis, prioridades, campos e status, reduzindo divergências entre configuração e processo institucional.

O GovFlow poderá, conforme autorização e configuração:

a) validar preenchimento e consistência de dados obrigatórios;
b) criar ou atualizar estruturas padronizadas;
c) verificar condições de gates e transições;
d) gerar documentos, relatórios e painéis;
e) consolidar indicadores e alertas;
f) integrar Redmine, Enterprise Architect, Git/GitLab e outros serviços;
g) executar health checks e registrar logs de execução; e

h) sincronizar informações cuja autoridade e precedência estejam definidas.

O GovFlow não poderá homologar, aceitar risco, autorizar contratação, receber entrega ou substituir decisão humana formal. Bloqueios e transições automáticas deverão possuir regra documentada, responsável e trilha de auditoria.

10.5 Enterprise Architect como repositório de arquitetura e modelagem

O Enterprise Architect será o repositório institucional preferencial para arquitetura, processos e modelagem técnica quando a complexidade, a criticidade ou o impacto justificarem sua utilização.

Poderão ser mantidos no Enterprise Architect: BPMN, UML, casos de uso, requisitos complexos, componentes, integrações, modelos de dados, diagramas de implantação, baselines, decisões arquiteturais e vínculos de rastreabilidade.

O uso será proporcional. Demandas simples não exigirão modelagem extensa; projetos corporativos, sistemas críticos, modernizações, integrações relevantes e mudanças arquiteturais deverão manter documentação compatível com o risco e a necessidade de manutenção.

O Redmine deverá conter identificadores ou referências que permitam localizar os modelos, pacotes, requisitos, baselines e decisões correspondentes.

10.6 Git/GitLab como plataforma de código e entrega técnica

O Git/GitLab será a fonte oficial para código-fonte, infraestrutura como código, scripts, pipelines, documentação versionável, branches, commits, merge requests, tags, releases e pacotes técnicos.

A administração deverá contemplar grupos, projetos, permissões, proteção de branches, regras de revisão, runners, retenção, backup, segurança, integração com o Redmine e preservação das evidências de pipeline.

As alterações deverão ser vinculadas aos itens correspondentes do Redmine por identificadores consistentes, conforme as regras do Capítulo 5.

10.7 Pipelines de CI/CD e ferramentas DevSecOps

Os pipelines deverão automatizar, conforme aplicável, etapas de build, testes, análises de qualidade e segurança, empacotamento, publicação e implantação. A sequência poderá variar segundo a tecnologia, o risco e a modalidade da iniciativa.

A cadeia técnica poderá incluir:

a) compilação e build reproduzível;

b) testes unitários, de integração e funcionais automatizados;

c) SAST, SCA, DAST e secrets scan;

d) scan de contêiner e infraestrutura como código;

e) geração de SBOM e evidências de proveniência;

f) publicação de artefatos e imagens;

g) implantação automatizada em ambientes autorizados; e

h) coleta de resultados para gates, homologação e auditoria.

As ferramentas específicas serão mantidas no catálogo técnico institucional, permitindo atualização sem reescrever o PDS. A substituição de uma ferramenta não poderá reduzir controles obrigatórios sem análise e aprovação.

10.8 OpenShift, contêineres e ambientes de execução

O OpenShift e demais plataformas conteinerizadas homologadas poderão suportar os ambientes de desenvolvimento, teste, homologação e produção. A adoção de outra plataforma dependerá de avaliação técnica e governança compatíveis.

A administração deverá controlar namespaces, recursos, imagens, configurações, secrets, deployments, escalabilidade, disponibilidade, logs, backup, rollback, monitoramento e segregação entre ambientes.

É vedado utilizar produção como ambiente habitual de teste, compartilhar credenciais entre ambientes, executar implantação sem rastreabilidade ou manter configurações manuais não documentadas como única fonte de operação.

10.9 Observabilidade, monitoramento e operação

As plataformas de observabilidade deverão apoiar a operação por meio de logs estruturados, métricas técnicas e de negócio, rastreamento distribuído, alertas, painéis e correlação de eventos.

A configuração deverá considerar criticidade, retenção, proteção de dados, acesso, responsáveis, limiares, canais de alerta, escalonamento e integração com a gestão de incidentes. Os registros deverão permitir relacionar eventos operacionais à versão e à mudança que os originou.

10.10 Ferramentas de atendimento e gestão de serviços

As ferramentas de atendimento e gestão de serviços poderão apoiar suporte, incidentes, requisições, catálogo de serviços, base de conhecimento, comunicação com usuários, escalonamento e níveis de serviço.

Esta seção substitui o placeholder anteriormente denominado “SAC”. A ferramenta nominal será registrada no catálogo institucional quando formalmente definida. A integração com o Redmine deverá evitar duplicidade e estabelecer claramente qual sistema é a fonte oficial de cada tipo de registro.

10.11 Documentos e sistemas administrativos oficiais

Processos administrativos, contratações, contratos, Ordens de Serviço, recebimentos, faturamento e comunicações oficiais permanecerão nos sistemas administrativos competentes.

O Redmine deverá manter referências, números, links, situação e evidências operacionais suficientes para garantir rastreabilidade, sem substituir o processo administrativo oficial nem criar cópias paralelas sem controle.

10.12 Integração e rastreabilidade entre as ferramentas

A rastreabilidade ponta a ponta deverá permitir relacionar demanda, requisito, modelo, item de backlog, código, pipeline, pacote, versão, homologação, termo e recebimento.

Elemento	Identificador ou vínculo esperado
Demanda e backlog	ID do Redmine e relações entre épico, história, tarefa, defeito ou mudança.
Arquitetura e requisitos complexos	Pacote, elemento, baseline ou referência do Enterprise Architect.
Código	Branch, commit e merge request vinculados ao item do Redmine.
Pipeline e artefato	ID da execução, resultado, pacote, imagem, tag ou checksum.
Versão e homologação	Versão do Redmine, ambiente, itens homologados e evidências.
Execução contratual	Número da OS, produtos, medição, parecer e termos de recebimento.

As integrações deverão documentar direção do fluxo, precedência, campos sincronizados, tratamento de erro, autenticação, logs e responsabilidade. Dados não poderão ser sobrescritos automaticamente quando houver conflito de autoridade entre fontes.

10.13 Administração, perfis e responsabilidades

Responsabilidade	Atribuição predominante
Proprietário funcional	Define finalidade institucional, regras de uso, prioridades e requisitos funcionais da ferramenta.
Administrador funcional	Configura workflows, campos, perfis, templates e regras operacionais aprovadas.
Administrador técnico	Mantém instalação, infraestrutura, banco, atualização, backup, desempenho e disponibilidade.
Administrador de segurança	Controla acessos privilegiados, credenciais, logs, revisões e requisitos de segurança.
Usuário responsável	Registra informações corretas, preserva evidências e utiliza a ferramenta segundo o PDS.

A designação nominal e institucional será mantida no catálogo, nas normas operacionais ou nos atos administrativos correspondentes.

10.14 Segurança, credenciais e contas técnicas

As ferramentas deverão utilizar contas individuais, autenticação compatível com o risco, menor privilégio e revisão periódica de acessos. Contas técnicas deverão possuir finalidade, proprietário, escopo, mecanismo de rotação e registro de uso.

a) credenciais, tokens, chaves e certificados não poderão ser armazenados em código ou documentação aberta;

b) segredos deverão ser mantidos em cofres ou mecanismos equivalentes;

c) contas compartilhadas serão vedadas, salvo exceção formalmente justificada;

d) integrações por API deverão possuir escopo mínimo, logs e política de revogação;

e) desligamentos e mudanças de função deverão provocar revisão ou revogação tempestiva; e

f) acessos privilegiados deverão ser monitorados e revisados.

10.15 Disponibilidade, backup, recuperação e continuidade

Cada ferramenta crítica deverá possuir responsável, classificação de criticidade, monitoramento, backup, restauração testada, documentação, plano de continuidade e inventário de dependências.

Quando aplicável, deverão ser definidos RTO e RPO, procedimentos de recuperação, contatos de escalonamento, alternativas temporárias e critérios de retorno à operação. A existência de backup sem teste de restauração não será considerada evidência suficiente de continuidade.

10.16 Gestão de configuração e mudanças nas ferramentas

Alterações em trackers, status, workflows, campos, plugins, integrações, permissões, versões, automações e infraestrutura deverão seguir fluxo controlado:

1. solicitação e justificativa;
2. análise técnica, funcional e de segurança;
3. avaliação de impacto e dependências;
4. teste em ambiente adequado;
5. aprovação pela autoridade competente;
6. implantação controlada;
7. validação e monitoramento; e
8. atualização de documentação e catálogo.

Mudanças emergenciais poderão seguir fluxo acelerado, mas deverão ser regularizadas e documentadas após a estabilização.

10.17 Atualização, obsolescência e descontinuação

Ferramentas e plataformas deverão ser avaliadas quanto a suporte, segurança, compatibilidade, custo, adoção, dependências e capacidade de evolução. A descontinuação poderá ocorrer por fim de suporte, risco, custo excessivo, incompatibilidade, baixa adoção, dependência crítica ou existência de solução institucional superior.

O plano de descontinuação deverá contemplar inventário, exportação, migração, preservação de histórico, validação, comunicação, revogação de acessos e desligamento seguro.

10.18 Critérios para adoção de novas ferramentas

A adoção de novas ferramentas deverá ser precedida de avaliação de necessidade, aderência funcional e técnica, segurança, interoperabilidade, licenciamento, custo total, suporte, comunidade, capacidade interna, portabilidade, proteção de dados, continuidade, reversibilidade e risco de dependência tecnológica.

Ferramentas gratuitas ou de código aberto poderão reduzir custos de licenciamento, mas exigem avaliação de implantação, operação, atualização, suporte, capacitação e continuidade. A ausência de preço de licença não equivale à ausência de custo institucional.

10.19 Catálogo institucional de ferramentas

Será mantido catálogo institucional atualizável contendo, no mínimo: nome, finalidade, proprietário, administradores, versão, ambientes, criticidade, usuários, integrações, dados tratados, suporte, licenciamento, backup, monitoramento, situação e plano de evolução.

O catálogo poderá ser atualizado sem reedição integral do PDS, desde que não altere fontes oficiais, responsabilidades, controles ou decisões institucionais aprovadas.

Informação	Conteúdo esperado
Identificação	Nome, versão, finalidade e situação no ciclo de vida.
Responsabilidade	Proprietário funcional e administradores funcional, técnico e de segurança.
Arquitetura	Ambientes, infraestrutura, integrações e dependências.
Segurança e dados	Criticidade, dados tratados, perfis, autenticação e registros.
Operação	Backup, monitoramento, suporte, continuidade e contatos.
Evolução	Licenciamento, roadmap, riscos, atualização, migração ou descontinuação.

10.20 Tratamento do Camunda

O Camunda não constitui ferramenta obrigatória do PDS. Poderá ser mantido no catálogo como motor BPMN existente, componente legado, solução opcional ou tecnologia em transição, conforme avaliação arquitetural e plano institucional. A modelagem de processos e o cumprimento das regras do PDS não dependerão exclusivamente desse produto.

11. Gestão de Riscos, Oportunidades e Exceções

Identificar	Analisar	Priorizar	Responder	Monitorar	Escalar	Aceitar risco residual	Revisar

> **LEITURA ORIENTADA:** A gestão de riscos integra todas as etapas do Processo de Desenvolvimento de Software da SEMA/MT. Seu propósito é apoiar decisões, proteger a continuidade dos serviços, reduzir incertezas, tornar exceções transparentes e ampliar a capacidade institucional de antecipar ameaças e aproveitar oportunidades. O tratamento de riscos não se limita ao início de projetos: deve ocorrer desde o registro da demanda até a operação, sustentação, evolução e descontinuação da solução.

11.1 Objetivos e princípios

A gestão de riscos do PDS observará os princípios de continuidade, proporcionalidade, rastreabilidade, responsabilidade definida, atualização permanente, decisão baseada em evidências e escalonamento conforme criticidade. Seus objetivos são:

- apoiar a priorização e a alocação de capacidade e recursos;
- antecipar impactos sobre prazos, custos, qualidade, segurança, dados, contratos e continuidade;
- definir respostas, contingências e autoridades responsáveis;
- registrar e controlar riscos residuais e exceções;
- identificar oportunidades de automação, reutilização, modernização e melhoria;
- produzir conhecimento institucional a partir de riscos materializados e lições aprendidas.

11.2 Conceitos e classificações

Termo	Definição no PDS
Risco	Evento futuro e incerto que pode afetar objetivos, entregas, serviços ou resultados.
Ameaça	Risco com potencial de efeito negativo.
Oportunidade	Risco com potencial de efeito positivo.
Problema	Condição existente que já produz ou pode produzir impacto.
Incidente	Evento ocorrido que interrompe, degrada ou ameaça um serviço.
Impedimento	Obstáculo atual que dificulta ou bloqueia a execução.
Premissa	Condição considerada verdadeira para fins de planejamento.
Restrição	Limitação que condiciona a solução ou a execução.
Risco inerente	Nível de risco antes da aplicação dos controles.
Risco residual	Nível remanescente após controles, mitigação e contingência.

A classificação correta evita que riscos futuros sejam tratados como incidentes já ocorridos, ou que problemas atuais permaneçam ocultos em registros genéricos.

11.3 Categorias de riscos do PDS

Os riscos poderão receber uma ou mais categorias, conforme sua natureza e seus efeitos:

- estratégico e institucional;
- negócio, valor público e reputação;
- escopo, requisitos, prazo e custo;
- capacidade, pessoas e conhecimento;
- fornecedor, contrato e dependência externa;
- arquitetura, tecnologia, integração e obsolescência;
- dados, privacidade e segurança;
- qualidade, testes e implantação;
- operação, disponibilidade e continuidade;
- legal, regulatório, ambiental e financeiro;
- mudança organizacional e adoção da solução.

11.4 Identificação contínua de riscos e oportunidades

A identificação ocorrerá de forma contínua nos gates e nas atividades de triagem, requisitos, arquitetura, estimativa, contratação, desenvolvimento, testes, homologação, implantação, operação, auditoria e encerramento. Poderão ser utilizadas entrevistas, workshops, análise de premissas e dependências, retrospectivas, indicadores, incidentes, modelagem de ameaças, auditorias, lições aprendidas e avaliação de fornecedores.

Todo participante do PDS poderá registrar risco ou oportunidade. O proprietário do risco e o responsável pelas ações deverão, entretanto, ser formalmente definidos.

11.5 Registro e rastreabilidade

O Redmine será a fonte oficial dos registros operacionais de risco. Cada registro deverá conter, conforme aplicável:

- identificador, título e descrição;
- categoria, causa, evento e consequência;

- probabilidade, impacto e nível;
- proprietário do risco e responsável pela ação;
- resposta planejada, prazo, gatilho e contingência;
- controles existentes e evidências;
- risco inerente e risco residual;
- autoridade de aceite e data de revisão;
- vínculos com demanda, projeto, produto, Ordem de Serviço, arquitetura, incidente, vulnerabilidade ou mudança.

O GovFlow poderá validar campos obrigatórios, calcular classificações aprovadas, alertar revisões vencidas, consolidar relatórios e apoiar o escalonamento. A automação não substituirá o julgamento nem a autoridade institucional.

11.6 Análise qualitativa

A análise qualitativa considerará probabilidade e impacto e poderá incorporar urgência, proximidade, detectabilidade, velocidade de materialização, reversibilidade, exposição e capacidade de resposta. A escala institucional deverá ser simples o suficiente para uso cotidiano e suficientemente clara para permitir comparação e escalonamento.

11.7 Análise quantitativa, quando aplicável

Riscos relevantes poderão receber análise quantitativa, incluindo impacto financeiro, atraso provável, indisponibilidade, perda de capacidade, exposição contratual, cenários, reservas e análise de sensibilidade. A análise quantitativa será proporcional ao porte e à criticidade da iniciativa e não será exigida para demandas simples sem benefício decisório.

11.8 Priorização e matriz de riscos

A classificação institucional utilizará níveis como baixo, moderado, alto e crítico. A matriz definitiva e seus limiares serão mantidos em procedimento ou catálogo versionado. Como referência conceitual:

Probabilidade	Impacto baixo	Impacto moderado	Impacto alto	Impacto crítico
Rara	Baixo	Baixo	Moderado	Alto
Possível	Baixo	Moderado	Alto	Crítico
Provável	Moderado	Alto	Alto	Crítico
Quase certa	Alto	Alto	Crítico	Crítico

A matriz de riscos não substitui os métodos de priorização do backlog. Probabilidade e impacto classificam riscos; WSJF, MoSCoW, GUT e outros métodos apoiam decisões distintas, conforme definido no Capítulo 3.

11.9 Planejamento das respostas

Para ameaças, poderão ser adotadas as seguintes respostas:

- evitar: eliminar a causa, o escopo ou a condição de exposição;
- mitigar: reduzir a probabilidade ou o impacto;
- transferir ou compartilhar: distribuir responsabilidades ou impactos, sem eliminar a responsabilidade institucional;
- aceitar: assumir conscientemente o risco, com ou sem reserva;
- escalar: encaminhar a decisão à autoridade com competência e recursos.

Para oportunidades, poderão ser adotadas estratégias de explorar, melhorar, compartilhar ou aceitar.

11.10 Ações preventivas, contingências e gatilhos

Riscos relevantes deverão possuir, conforme aplicável, ação preventiva, responsável, prazo, indicador, gatilho de materialização, plano de contingência, comunicação, reserva e estratégia de recuperação. O gatilho deverá ser observável e permitir resposta antes que o impacto se torne irreversível.

11.11 Risco inerente e risco residual

O risco inerente será avaliado antes dos controles. Após a aplicação das medidas preventivas, mitigadoras e contingenciais, deverá ser calculado ou classificado o risco residual. Essa avaliação será obrigatória antes de decisões críticas, como implantação em produção, aceite de exceção, uso de dados de alto risco, encerramento de vulnerabilidade ou contratação com dependência relevante.

11.12 Aceite de risco e autoridade decisória

O aceite de risco deverá registrar descrição, justificativa, controles existentes, risco residual, prazo, proprietário, autoridade competente, data de revisão e plano de

regularização, quando aplicável. A autoridade será definida conforme criticidade, impacto, competência, natureza do risco, contrato e Regimento Interno.

Ferramentas, desenvolvedores, fornecedores e equipes operacionais não poderão aceitar risco institucional em nome da SEMA/MT sem delegação formal.

11.13 Gestão de riscos em projetos e produtos

A gestão deverá distinguir riscos da iniciativa e riscos do produto. Riscos da iniciativa relacionam-se a escopo, prazo, custo, capacidade e execução. Riscos do produto relacionam-se à arquitetura, operação, segurança, dados, manutenção e continuidade. O encerramento do projeto não encerra automaticamente os riscos do produto em operação.

11.14 Gestão de riscos da fábrica e dos contratos

A execução contratada deverá considerar, entre outros, riscos de atraso, baixa produtividade, estimativa inadequada, retrabalho, reincidência de defeitos, indisponibilidade de especialistas, concentração de conhecimento, acesso indevido, uso inadequado de dados, saldo ou vigência insuficientes, dependência do fornecedor, licenciamento, propriedade intelectual, transferência de conhecimento e continuidade após o contrato.

Os riscos relevantes deverão ser vinculados às Ordens de Serviço e acompanhados pela CSTI, fiscalização e gestão contratual, conforme suas competências.

11.15 Riscos de arquitetura, tecnologia e obsolescência

Deverão ser avaliados riscos de dependência tecnológica, fim de suporte, acoplamento excessivo, baixa escalabilidade, ausência de observabilidade, dívida arquitetural, integração frágil, licenciamento, aprisionamento tecnológico, impossibilidade de migração e insuficiência de conhecimento interno. ADRs, modelos do Enterprise Architect e o catálogo de tecnologias deverão apoiar a análise e a rastreabilidade.

11.16 Riscos de segurança, privacidade e dados

Os riscos de segurança, privacidade e dados serão integrados ao registro corporativo, incluindo ameaça, vulnerabilidade, exposição, perda, alteração, indisponibilidade, vazamento, retenção inadequada, compartilhamento indevido, qualidade

insuficiente, vieses e decisões automatizadas. Os controles e testes técnicos permanecem disciplinados no Capítulo 7.

11.17 Riscos de implantação, operação e continuidade

Planos de implantação e operação deverão considerar indisponibilidade, falha de migração, rollback inviável, perda de dados, incompatibilidade, janela insuficiente, configuração manual, ausência de backup, monitoramento inadequado, falha de capacidade, certificados, integrações externas e dependências críticas. Os riscos relevantes deverão possuir contingência e critérios claros de interrupção ou reversão.

11.18 Gestão de oportunidades

O PDS também registrará oportunidades que possam ampliar valor público, qualidade, eficiência ou sustentabilidade. Exemplos incluem reutilização de componentes, automação de validações, redução de licenciamento, melhoria de desempenho, modernização antecipada, integração de bases e redução do tempo de atendimento. A oportunidade deverá possuir responsável, benefício esperado, ação e prazo de avaliação.

11.19 Exceções, desvios e não conformidades

Toda exceção relevante de processo, arquitetura, segurança, qualidade, ferramenta ou implantação deverá gerar ou atualizar um risco formal. O registro deverá conter justificativa, prazo, responsável, controle compensatório, autoridade aprovadora e data de revisão.

Não conformidades deverão produzir registro, análise, correção, ação preventiva, acompanhamento e evidência de encerramento.

11.20 Monitoramento, revisão e escalonamento

Os riscos serão revisados nos gates, nos ciclos de acompanhamento, após mudanças, incidentes e auditorias, antes da implantação e do recebimento, quando um gatilho ocorrer ou quando vencer a data de revisão. Riscos críticos deverão ser escalonados imediatamente à autoridade competente. Alterações de probabilidade, impacto, controle ou contexto deverão atualizar o registro e a resposta planejada.

11.21 Indicadores e relatórios de risco

A governança acompanhará famílias de indicadores como quantidade de riscos por nível, riscos sem proprietário, ações vencidas, tempo de tratamento, riscos materializados, reincidência, eficácia das respostas, riscos residuais críticos, exceções abertas, riscos contratuais e oportunidades realizadas. Fórmulas, metas, fontes e periodicidades serão consolidadas no Capítulo 13.

11.22 Encerramento, materialização e lições aprendidas

Um risco poderá ser encerrado quando deixar de ser aplicável, terminar o período de exposição, for concluído o tratamento, o risco residual for aceito, a oportunidade for realizada ou a iniciativa for cancelada. Quando o evento ocorrer, o registro deverá ser convertido ou vinculado a incidente, problema, mudança ou ação corretiva, preservando a rastreabilidade.

As lições aprendidas deverão retroalimentar requisitos, arquitetura, testes, contratos, procedimentos, indicadores e o próprio PDS, evitando a repetição de falhas e ampliando a maturidade institucional.

12. Capacitação e Gestão do Conhecimento

LEITURA ORIENTADA: Este capítulo estabelece o modelo institucional para desenvolver, manter e comprovar as competências necessárias à aplicação do Processo de Desenvolvimento de Software da SEMA/MT. A capacitação deverá ser contínua, orientada pelos papéis exercidos e vinculada à prática, de modo que o PDS seja efetivamente executado e não apenas conhecido em nível conceitual.

12.1 Objetivos e princípios

A capacitação e a gestão do conhecimento deverão apoiar a qualidade das entregas, a segurança, a continuidade dos serviços, a autonomia institucional e a redução de retrabalho e dependência de fornecedores. As ações deverão observar os seguintes princípios:

- aprendizagem orientada ao papel e às responsabilidades exercidas;
- aplicação prática em situações compatíveis com a realidade institucional;
- proporcionalidade entre criticidade da função e profundidade da formação;
- atualização periódica diante de mudanças de processo, tecnologia, contrato ou norma;
- acessibilidade dos materiais e diversidade de formatos de aprendizagem;
- avaliação da aprendizagem e de sua aplicação no trabalho;
- reutilização, versionamento e preservação do conhecimento institucional;
- transferência sistemática de conhecimento entre equipes internas e fornecedores;
- registro das ações, participantes, resultados e evidências.

12.2 Governança da capacitação

A governança da capacitação deverá definir a unidade coordenadora, os responsáveis pelos conteúdos, os públicos, as prioridades, os recursos, os mecanismos de avaliação e o repositório oficial de materiais. A CPQSI poderá coordenar a dimensão metodológica e de governança do PDS, com participação da CSTI, CITI, áreas demandantes, gestão e fiscalização contratual, encarregado pelo tratamento de dados pessoais e demais especialistas conforme o tema.

A aprovação de conteúdos técnicos deverá contar com especialistas do domínio. A unidade coordenadora não substituirá as responsabilidades dos proprietários dos processos, das ferramentas ou dos controles abordados.

12.3 Levantamento das necessidades de competência

O levantamento das necessidades deverá ocorrer, no mínimo, durante o planejamento anual e sempre que houver mudança relevante. Deverá considerar:

- papéis e responsabilidades efetivamente exercidos;
- competências requeridas e nível atual de domínio;
- lacunas identificadas em auditorias, incidentes, retrabalho, indicadores ou avaliações;
- implantação de novas ferramentas, tecnologias, processos ou contratos;
- alterações legais, regulatórias, arquiteturais ou de segurança;
- entrada, movimentação ou saída de profissionais;
- criticidade dos sistemas e riscos associados às atividades;
- necessidade de continuidade e redução de concentração de conhecimento.

O plano de capacitação não deverá ser formado apenas a partir da oferta disponível de cursos. As ações deverão responder a lacunas verificadas e a resultados esperados.

12.4 Trilhas de aprendizagem por papel

A capacitação deverá ser organizada em trilhas cumulativas, permitindo formação básica comum e aprofundamento conforme o papel.

Trilha	Público principal	Resultados esperados
Fundamentos do PDS	Todos os participantes	Compreender fluxo, papéis, registros, gates, evidências e responsabilidades.
Gestão da demanda e produto	Áreas demandantes, gestores do negócio, analistas e CSTI	Registrar necessidades, definir valor, priorizar, validar requisitos e homologar resultados.
Requisitos e arquitetura	Analistas, arquitetos e equipes técnicas	Modelar processos, requisitos, integrações, dados e decisões arquiteturais com rastreabilidade.
Desenvolvimento e entrega	Desenvolvedores e fábrica	Aplicar padrões de código, Git, revisão, CI/CD, documentação e Definition of Done.
Testes e qualidade	QA, desenvolvedores, CSTI e homologadores	Planejar, executar, automatizar e evidenciar testes proporcionais ao risco.
Segurança, privacidade e DevSecOps	Equipes técnicas, CITI, CPQSI e fábrica	Aplicar controles, scans, tratamento de vulnerabilidades e proteção de dados.
Fiscalização e gestão contratual	Fiscais e gestores de contrato	Acompanhar OS, evidências, SLA, medição, glosa, recebimento e riscos.
Sustentação e operação	Suporte, CSTI, CITI e fábrica	Tratar incidentes, problemas, mudanças, observabilidade e continuidade.
Dados, analytics e IA	Negócio, equipes de dados e governança	Assegurar qualidade, rastreabilidade, ética, segurança e monitoramento de dados e modelos.
Ferramentas institucionais	Usuários, administradores e responsáveis	Utilizar e administrar Redmine, GovFlow, EA, Git/GitLab, OpenShift e observabilidade.

12.5 Capacitação das áreas demandantes e dos gestores do negócio

As áreas demandantes e os gestores do negócio deverão ser preparados para participar ativamente do ciclo do produto. A formação deverá abranger:

- registro do problema, da necessidade e do resultado público esperado;
- identificação de usuários, processos, dados, restrições e impactos;
- participação na elicitação e validação de requisitos;
- formulação e leitura de histórias de usuário e critérios de aceite;
- priorização, tratamento de dependências e avaliação de valor;
- preparação e execução da homologação;
- registro de evidências, pendências e decisões;
- distinção entre defeito, ajuste de escopo e nova evolução;
- aceite funcional e responsabilidades após a implantação.

12.6 Capacitação de analistas, arquitetos e equipes técnicas

A formação técnica deverá abranger análise de requisitos, BPMN, UML, arquitetura, requisitos não funcionais, integrações, modelagem de dados, estimativas, rastreabilidade, decisões arquiteturais, análise de impacto e manutenção da documentação. O uso do Enterprise Architect deverá ser ensinado de forma proporcional à complexidade da iniciativa, evitando modelagem meramente burocrática.

12.7 Capacitação em testes e qualidade de software

A trilha de testes deverá combinar fundamentos, planejamento, execução prática, automação e produção de evidências. O conteúdo mínimo deverá contemplar:

Dimensão	Conteúdos mínimos
Fundamentos	Erro, defeito, falha e incidente; verificação e validação; estratégia de testes; pirâmide de testes; critérios de entrada e saída; risco baseado em testes.
Níveis e tipos	Unitário, componente, integração, contrato, sistema, funcional, aceitação, reteste, regressão, smoke, exploratório, usabilidade, acessibilidade, desempenho, carga, estresse, volume, segurança, compatibilidade, migração, resiliência e recuperação.
Automação	Seleção de cenários, dados de teste, estabilidade, execução no pipeline, manutenção e análise.
Evidências	Rastreabilidade com requisitos e critérios de aceite, ambiente, versão, resultado esperado, resultado obtido, registros e anexos.
Homologação	Preparação de cenários, classificação de pendências, homologação parcial, aprovação, reprovação e aceite funcional.

12.7.1 Prática de testes unitários

A capacitação em testes unitários deverá ensinar isolamento da unidade, organização dos testes, dados de teste, uso criterioso de mocks, stubs e fakes, comportamento esperado, determinismo, legibilidade, manutenção e integração ao pipeline. Deverá enfatizar que cobertura elevada não garante, isoladamente, qualidade dos testes.

Na correção de defeitos, os profissionais deverão ser orientados a reproduzir a falha por teste automatizado quando tecnicamente viável, implementar a correção e preservar o teste como proteção contra regressão.

12.8 Capacitação em segurança, privacidade e DevSecOps

A formação deverá contemplar Security by Design, Privacy by Design, modelagem de ameaças, codificação segura, autenticação e autorização, proteção de segredos, SAST, SCA, DAST, scans de contêiner e infraestrutura como código, SBOM, gestão de vulnerabilidades, resposta a incidentes, bases legais, direitos dos titulares, RIPD e aceite de risco. O conteúdo deverá ser ajustado ao papel: desenvolvedores precisam saber implementar controles; gestores e autoridades precisam saber interpretar riscos e tomar decisões.

12.9 Capacitação em dados, analytics e inteligência artificial

A trilha deverá tratar de governança e qualidade de dados, metadados, linhagem, classificação, privacidade, preparação de dados, versionamento, reprodutibilidade, vieses, avaliação de modelos, explicabilidade proporcional ao risco, supervisão humana, segurança, monitoramento e documentação. Projetos de IA deverão incluir aprendizagem sobre limitações dos modelos e uso responsável dos resultados.

12.10 Capacitação da fiscalização e da gestão contratual

Fiscais e gestores de contrato deverão receber formação específica sobre papéis e segregação de responsabilidades, planejamento e autorização de Ordens de Serviço, acompanhamento de escopo, prazos, capacidade e riscos, análise de evidências, medição, SLA, glosas, recebimentos provisório e definitivo, comunicação com o preposto, não

conformidades, propriedade dos ativos, transferência de conhecimento e encerramento contratual.

12.11 Capacitação da fábrica e dos fornecedores

Antes de atuar em atividades do PDS, profissionais da fábrica e fornecedores deverão conhecer as regras aplicáveis ao seu escopo, incluindo fluxo do Redmine, validações do GovFlow, padrões de arquitetura e Git, Definition of Ready, Definition of Done, testes, qualidade, segurança, homologação, evidências, documentação, acesso e confidencialidade. A capacitação institucional não elimina a obrigação contratual do fornecedor de disponibilizar profissionais qualificados.

A substituição de profissionais críticos deverá ser acompanhada de transferência de conhecimento e verificação de prontidão, sem prejuízo das obrigações e dos prazos contratuais.

12.12 Capacitação nas ferramentas institucionais

Ferramenta ou plataforma	Conteúdos por perfil
Redmine	Demandas, classificação, backlog, workflows, relações, versões, riscos, evidências, homologação, relatórios e administração funcional.
GovFlow	Validações, automações, integrações, regras declarativas, health checks, logs, análise de falhas e administração.
Enterprise Architect	BPMN, UML, arquitetura, dados, baselines, decisões e rastreabilidade.
Git/GitLab	Repositórios, branches, commits, merge requests, revisão, pipelines, tags, releases e segurança.
CI/CD e DevSecOps	Build, testes, scans, artefatos, gates, implantação, rollback e interpretação dos resultados.
OpenShift e observabilidade	Ambientes, deploy, configuração, secrets, logs, métricas, alertas, troubleshooting e continuidade.

12.13 Integração e formação inicial

Todo novo participante deverá receber onboarding proporcional ao papel antes de executar atividades críticas de forma autônoma. O onboarding deverá incluir visão geral do PDS, responsabilidades, acessos, segurança, proteção de dados, fluxo de trabalho, ferramentas, documentação, canais de suporte, atividade prática e avaliação mínima de prontidão.

A concessão de acesso técnico não deverá ser confundida com habilitação para exercer decisões, aprovações ou funções institucionais.

12.14 Formação prática, laboratórios e projetos-piloto

As ações deverão priorizar aprendizagem prática por meio de oficinas, laboratórios, simulações, casos reais, exercícios no Redmine, modelagem no Enterprise Architect, pipelines demonstrativos, análise de incidentes, homologação simulada, projetos-piloto, revisão conjunta de artefatos e aprendizagem em pares. Conteúdos expositivos deverão ser combinados com tarefas que demonstrem capacidade de aplicação.

12.15 Documentação, manuais e base de conhecimento

A base de conhecimento deverá reunir, conforme aplicável, manual do PDS, guias rápidos, procedimentos, tutoriais, vídeos, perguntas frequentes, exemplos, modelos, checklists, runbooks, orientações de troubleshooting e decisões recorrentes.

Cada material deverá possuir título, responsável, versão, data de publicação ou revisão, público, escopo, validade, relação com a versão do PDS e localização oficial. Materiais obsoletos deverão ser identificados, arquivados ou retirados de uso, preservando-se o histórico quando necessário.

12.16 Comunidades de prática e compartilhamento

Poderão ser instituídas comunidades de prática para requisitos, arquitetura, desenvolvimento, testes, segurança, dados, DevOps, gestão de produtos e fiscalização. Essas comunidades deverão compartilhar problemas e soluções, revisar padrões, divulgar lições aprendidas, construir ativos reutilizáveis e reduzir soluções isoladas, sem substituir as autoridades formais de decisão.

12.17 Mentoria, acompanhamento e transferência de conhecimento

A transferência de conhecimento deverá ocorrer entre equipes internas, entre especialistas, entre SEMA/MT e fornecedores e nos momentos de entrada, saída ou substituição de profissionais. Poderão ser utilizados mentoria, shadowing, sessões técnicas, documentação, revisão conjunta, operação assistida, laboratórios e gravações autorizadas.

Tecnologias e sistemas críticos deverão possuir, sempre que possível, mais de uma pessoa interna capaz de compreender sua arquitetura, operação e principais procedimentos de recuperação.

12.18 Avaliação da aprendizagem e da aplicação prática

A eficácia da capacitação deverá ser avaliada por mecanismos proporcionais, tais como testes de conhecimento, exercícios práticos, análise de artefatos, execução supervisionada, observação no trabalho, auditorias posteriores, feedback e indicadores de erro ou retrabalho. A presença em curso, isoladamente, não comprova competência para executar uma atividade crítica.

Quando a avaliação indicar lacuna relevante, deverão ser planejadas ações de reforço, acompanhamento ou restrição temporária de autonomia, conforme o risco da função.

12.19 Atualização contínua e reciclagem

A reciclagem deverá ocorrer quando houver nova versão do PDS, mudança relevante de ferramenta ou workflow, atualização normativa, incidente significativo, conclusão de auditoria, adoção de tecnologia, novo contrato, mudança de função ou lacuna identificada. Conteúdos sujeitos a rápida obsolescência deverão possuir revisão mais frequente.

12.20 Registros, evidências e indicadores

As ações deverão registrar participantes, papel, conteúdo, duração, modalidade, instrutor, avaliação, resultado, evidência, trilha concluída e validade quando aplicável. Os registros deverão respeitar a proteção de dados pessoais e a política institucional de retenção.

As famílias de indicadores poderão abranger cobertura de capacitação, conclusão por trilha, desempenho, aplicação prática, redução de erros, reincidência, satisfação, tempo de onboarding, atualização dos materiais e lacunas abertas. Fórmulas, fontes e metas serão definidas no Capítulo 13 ou em catálogo institucional de indicadores.

12.21 Plano anual de capacitação do PDS

O plano anual deverá ser elaborado a partir das necessidades identificadas e conter, no mínimo:

- objetivos e resultados esperados;
- públicos e trilhas prioritárias;
- competências e lacunas atendidas;
- ações, modalidades e carga horária estimada;
- calendário e responsáveis;
- recursos e dependências;
- critérios de participação e priorização;
- métodos de avaliação;
- indicadores e evidências;
- plano de atualização dos materiais.

O planejamento anual deverá admitir ações extraordinárias em resposta a incidentes, mudanças normativas, implantação de ferramentas, novos contratos ou riscos emergentes. Ao final do ciclo, os resultados deverão ser avaliados e utilizados no planejamento seguinte.

13. Métricas e Avaliação de Desempenho

LEITURA ORIENTADA: Este capítulo estabelece o modelo institucional de medição do Processo de Desenvolvimento de Software da SEMA/MT. Seu objetivo é transformar registros operacionais em informações confiáveis para decisão, melhoria contínua, prestação de contas, gestão contratual e avaliação de valor público. Métricas não deverão ser produzidas como finalidade em si mesmas: cada indicador deverá responder a uma pergunta de gestão e estar associado a uma ação possível.

13.1 Objetivos e princípios de medição

A medição deverá apoiar o planejamento, a priorização, a previsibilidade, a qualidade, a segurança, a gestão de riscos, a operação, a fiscalização contratual e a avaliação dos benefícios entregues. O modelo observará os seguintes princípios:

- relevância para uma decisão ou objetivo institucional;
- definição clara e interpretação compartilhada;
- rastreabilidade até a fonte e os registros de origem;
- qualidade, consistência e atualidade dos dados;
- comparabilidade apenas entre contextos equivalentes;
- proporcionalidade entre custo de medição e benefício decisório;
- segmentação adequada por tipo, criticidade, equipe, produto ou período;
- combinação de indicadores de resultado, fluxo, qualidade, risco e valor;
- proteção contra uso isolado, punitivo ou manipulável;
- revisão periódica diante de mudanças no processo, nas ferramentas ou na estratégia.

13.2 Modelo de medição do PDS

Elemento	Definição	Exemplo
Medida	Valor observado diretamente na fonte.	Quantidade de incidentes abertos no período.
Métrica	Valor calculado a partir de uma ou mais medidas.	Percentual de incidentes solucionados dentro do SLA.
Indicador	Métrica interpretada em contexto para apoiar decisão.	Tendência de cumprimento do SLA por serviço e severidade.
Meta ou faixa	Resultado desejado, limite ou intervalo de referência.	Faixa de atenção quando o cumprimento ficar abaixo do limite aprovado.
Alerta	Condição que exige avaliação ou ação.	Risco crítico sem responsável ou vulnerabilidade vencida.

O modelo deverá combinar indicadores antecedentes, que sinalizam condições capazes de influenciar resultados futuros, e indicadores de resultado, que demonstram efeitos já produzidos. Nenhum conjunto reduzido de métricas deverá ser tratado como explicação universal do desempenho do PDS.

13.3 Governança dos indicadores

Cada indicador institucional deverá possuir ficha controlada, contendo no mínimo:

- nome, código e versão;
- objetivo e pergunta de gestão;
- definição, escopo e exclusões;
- fórmula, unidade e regras de cálculo;
- fonte primária e eventuais fontes auxiliares;
- responsável pelo dado e responsável pela análise;
- periodicidade de atualização e de revisão;
- segmentações e filtros permitidos;
- linha de base, meta, faixa ou limite, quando aplicável;
- forma correta de interpretação e limitações;
- ação esperada diante de desvios;
- data de aprovação e próxima revisão.

A criação, alteração ou retirada de indicadores deverá ser aprovada pela instância responsável pela governança do PDS ou do domínio medido. Mudanças de fórmula deverão preservar a comparabilidade histórica ou declarar explicitamente a quebra de série.

13.4 Qualidade e confiabilidade dos dados

Antes de utilizar um indicador para decisão, deverá ser avaliada a qualidade dos dados de origem. Serão consideradas, conforme aplicável, completude, validade, consistência, unicidade, atualidade, integridade, rastreabilidade e estabilidade da regra de cálculo.

O Redmine será a fonte operacional dos registros do fluxo; Git/GitLab, pipelines, OpenShift, observabilidade, Enterprise Architect, GovFlow e sistemas administrativos oficiais fornecerão evidências complementares conforme sua responsabilidade. O GovFlow

poderá validar campos obrigatórios, datas incompatíveis, vínculos ausentes, duplicidades e outras inconsistências, sem alterar registros ou decisões sem autorização.

Quando os dados não forem suficientemente confiáveis, o painel deverá sinalizar a limitação. A ausência ou baixa qualidade do dado não deverá ser ocultada por estimativas não identificadas.

13.5 Indicadores de demanda e portfólio

Família	Indicadores exemplificativos	Decisões apoiadas
Entrada e qualificação	Demandas recebidas, qualificadas, devolvidas, rejeitadas, canceladas e tempo de triagem.	Ajustar canais, critérios de entrada e capacidade de análise.
Fila e envelhecimento	Idade da demanda, tempo sem atualização, demanda reprimida e itens bloqueados.	Repriorizar, escalonar dependências e evitar acúmulo invisível.
Composição do portfólio	Distribuição por área, criticidade, valor, obrigação legal, tipo de iniciativa e risco.	Balancear o portfólio e demonstrar alinhamento institucional.
Capacidade comprometida	Percentual destinado a novos produtos, evolução, sustentação, segurança e dívida técnica.	Evitar consumo integral da capacidade por uma única natureza.
Benefícios previstos	Iniciativas com objetivo, indicador de benefício, responsável e linha de base definidos.	Avaliar se projetos estão preparados para produzir e medir valor.

13.6 Indicadores de fluxo e prazo

O fluxo deverá ser medido por etapa, distinguindo tempo de execução, espera, bloqueio e retrabalho. Poderão ser acompanhados lead time, cycle time, tempo de triagem, refinamento, desenvolvimento, teste, homologação, aceite, implantação e encerramento.

A análise não deverá depender apenas da média. Sempre que o volume permitir, deverão ser utilizados mediana, percentis, distribuição, amplitude e segmentação por tipo, complexidade e criticidade. Itens emergenciais ou atípicos deverão ser identificados para não distorcer indevidamente a série.

Indicador	Interpretação principal
Lead time	Tempo total entre a entrada definida e a entrega ou encerramento.
Cycle time	Tempo entre o início efetivo do trabalho e sua conclusão.
Tempo de espera	Período em que o item não recebe trabalho ativo.
Tempo bloqueado	Período impedido por dependência, decisão, acesso, ambiente ou terceiro.
Throughput	Quantidade concluída em uma janela, considerada junto com o perfil dos itens.
Aging	Tempo dos itens ainda em andamento ou fila.
Previsibilidade	Diferença entre prazo planejado e realizado, com análise das causas.

13.7 Indicadores de produtividade e capacidade

A avaliação de capacidade deverá considerar planejamento e realização, trabalho em andamento, throughput, interrupções, retrabalho, disponibilidade de perfis críticos e consumo contratual. Quantidade de linhas de código não deverá ser adotada como indicador de produtividade, e equipes distintas não deverão ser comparadas apenas pela contagem de histórias ou tarefas.

Indicadores de utilização deverão ser interpretados com cautela: utilização próxima de cem por cento tende a reduzir a capacidade de absorver urgências, tratar incidentes, aprender e melhorar o processo. A análise deverá buscar equilíbrio entre fluxo, qualidade e sustentabilidade da equipe.

13.8 Indicadores de requisitos e backlog

- percentual de itens aderentes à Definition of Ready;
- histórias sem critérios de aceite ou sem responsável de negócio;
- alterações de requisitos após início da execução;
- itens reabertos, rejeitados ou devolvidos por informação insuficiente;
- backlog envelhecido e itens sem revisão;
- dependências não resolvidas;
- mudanças de escopo e suas causas;
- cobertura de rastreabilidade entre demanda, requisito, arquitetura, código, teste, homologação e entrega.

Os indicadores deverão apoiar melhoria da qualidade do refinamento, e não desencorajar mudanças legítimas decorrentes de aprendizagem. Mudanças deverão ser analisadas pelo impacto e pela causa, distinguindo evolução consciente de instabilidade recorrente.

13.9 Indicadores de desenvolvimento e entrega

Dimensão	Indicadores exemplificativos
Integração e revisão	Frequência de commits e integrações, tempo de merge request, revisões pendentes e taxa de devolução.
Pipeline	Taxa de sucesso, duração, falhas por etapa, tempo de recuperação e instabilidade.
Entrega	Frequência de release e deploy, tempo entre mudança e produção e entregas concluídas.
Mudança	Percentual de mudanças emergenciais, rollbacks, falhas pós-implantação e retrabalho.
Documentação	Entregas com documentação técnica, operacional e de usuário atualizada.

Métricas associadas ao modelo DORA poderão ser usadas como referência, desde que adaptadas ao contexto institucional e combinadas com qualidade, risco, satisfação e valor. A busca por frequência de entrega não deverá reduzir controles necessários nem incentivar fragmentação artificial.

13.10 Indicadores de testes e qualidade

A avaliação de testes e qualidade deverá cobrir planejamento, cobertura, execução, defeitos, regressão e homologação.

Grupo	Indicadores exemplificativos	Cuidados de interpretação
Cobertura	Cobertura de testes unitários, requisitos, critérios de aceite, automação e criticidade.	Cobertura de código elevada não comprova, isoladamente, qualidade dos testes.
Execução	Taxa de sucesso, duração, testes instáveis, falhas de ambiente e cenários não executados.	Falha de ambiente deve ser separada de falha funcional.
Defeitos	Quantidade por severidade e fase, densidade, reabertura, reincidência, idade e tempo de correção.	Contagem bruta deve ser contextualizada por tamanho, risco e período.
Escape	Defeitos encontrados em homologação ou produção que poderiam ter sido detectados antes.	Deve orientar melhoria de prevenção e detecção, não culpabilização isolada.
Regressão	Defeitos recorrentes, correções sem teste de proteção e falhas após alteração.	Avaliar manutenção da suíte e causa técnica.
Homologação	Ciclos, aprovação na primeira submissão, tempo da área, pendências e aceite parcial.	Separar indisponibilidade do homologador de defeito da solução.

A efetividade dos testes poderá ser avaliada pela proporção de defeitos relevantes detectados antes da produção, pela redução de reincidência e pela capacidade da suíte de apoiar mudanças com segurança. Testes unitários deverão ser avaliados também por legibilidade, estabilidade, isolamento e proteção de regras críticas.

13.11 Indicadores de segurança e privacidade

- vulnerabilidades por severidade, ativo, origem e idade;
- tempo de triagem, tratamento, correção e reteste;
- vulnerabilidades críticas ou altas em produção;
- reincidência e vulnerabilidades reabertas;
- cobertura e resultados de SAST, SCA, DAST, secrets scan, contêiner e IaC;
- dependências e imagens obsoletas;
- exceções de segurança, prazo e risco residual;

- incidentes de segurança e incidentes envolvendo dados pessoais;
- sistemas com inventário de dados, análise de base legal e RIPD quando aplicável;
- revisões de acesso privilegiado e conformidade dos gates.

A severidade técnica deverá ser combinada com exposição, criticidade do ativo, dados tratados, exploração conhecida e controles compensatórios. Indicadores de segurança não deverão incentivar ocultação ou reclassificação artificial de vulnerabilidades.

13.12 Indicadores de implantação e releases

- implantações realizadas, bem-sucedidas, canceladas e revertidas;
- taxa de falha de mudança;
- tempo de implantação e de restauração;
- indisponibilidade causada por mudança;
- mudanças emergenciais e fora da janela;
- releases sem evidências completas, plano de rollback ou monitoramento;
- falhas de configuração, migração e compatibilidade;
- percentual de implantações automatizadas e rastreáveis.

A simples conclusão do deploy não será suficiente para considerar a implantação bem-sucedida. O período de observação, os indicadores de saúde, a validação funcional e a ausência de impacto relevante deverão compor a avaliação.

13.13 Indicadores de operação, manutenção e sustentação

Dimensão	Indicadores exemplificativos
Disponibilidade e desempenho	Disponibilidade, latência, erros, saturação, capacidade e cumprimento de objetivos de serviço.
Sustentação	Chamados, tempo de atendimento, tempo de solução, backlog, envelhecimento e cumprimento de SLA.
Manutenção	Distribuição entre corretiva, adaptativa, evolutiva, preventiva, técnica e segurança.
Prevenção	Atualizações, obsolescência tratada, manutenção preventiva e dívida técnica reduzida.
Observabilidade	Cobertura de logs, métricas, traces, alertas úteis e tempo de detecção.

Indicadores operacionais deverão ser segmentados por serviço, severidade, componente e período. Alarmes sem ação, duplicados ou excessivamente sensíveis deverão ser tratados como problema de qualidade da observabilidade.

13.14 Indicadores de incidentes e problemas

- incidentes por severidade, serviço, origem e recorrência;
- tempo médio ou percentis de reconhecimento, atendimento, restauração e solução;
- incidentes relacionados a mudanças;
- problemas sem causa raiz ou plano de ação;
- erros conhecidos e ações corretivas vencidas;
- incidentes reabertos e reincidentes;
- eficácia de contingências e comunicação;
- tempo entre materialização do risco e registro do incidente.

MTTA, MTTR e outras médias deverão ser acompanhadas de distribuição e severidade. Incidentes críticos não deverão ser diluídos estatisticamente em grande volume de ocorrências simples.

13.15 Indicadores de riscos e exceções

- riscos por nível, categoria, produto e proprietário;
- riscos sem responsável, sem ação ou com revisão vencida;
- riscos materializados e impacto produzido;
- riscos residuais altos ou críticos aceitos;
- eficácia das respostas e contingências;
- exceções abertas, vencidas, regularizadas e reincidentes;
- tempo de regularização;
- riscos da fábrica, do contrato e de dependência tecnológica;
- oportunidades identificadas e benefícios realizados.

O indicador deverá distinguir quantidade de riscos de exposição efetiva. Reduzir a quantidade por exclusão ou reclassificação não representa, necessariamente, redução de risco.

13.16 Indicadores de dados e inteligência artificial

Domínio	Indicadores exemplificativos
Qualidade de dados	Completude, consistência, validade, atualidade, unicidade, precisão e integridade referencial.
Governança	Domínios com proprietário e curador, metadados, classificação e linhagem documentados.
Operação de dados	Falhas de carga, tempo de processamento, dados rejeitados, incidentes e tempo de correção.
Modelos de IA	Precisão, recall, F1, falsos positivos e negativos, latência, estabilidade e disponibilidade.
Monitoramento de IA	Drift de dados e conceito, degradação, vieses, explicabilidade, intervenção humana e versões em produção.
Reprodutibilidade	Dados, código, parâmetros, ambiente e artefatos necessários para reproduzir resultados.

As métricas de modelos deverão ser selecionadas de acordo com o problema, o custo dos erros e o perfil dos dados. Acurácia isolada poderá ser inadequada, especialmente em bases desbalanceadas. Modelos de maior impacto deverão incluir avaliação de grupos, riscos, supervisão humana e critérios de suspensão ou rollback.

13.17 Indicadores da fábrica e dos contratos

- entregas previstas, realizadas, aceitas, rejeitadas e reabertas;
- pontualidade, variação de prazo e causas;
- consumo, saldo e previsão das Ordens de Serviço;
- cumprimento de SLA e níveis de serviço;
- retrabalho, reincidência e defeitos por severidade;
- tempo de correção e resposta do fornecedor;
- glosas, não conformidades e pendências de recebimento;
- documentação, evidências e ativos entregues;
- transferência de conhecimento e dependência de profissionais-chave;
- conformidade de segurança, acesso e proteção de dados.

Indicadores gerenciais não substituirão regras de medição, aceite, glosa ou recebimento estabelecidas no contrato e na legislação. Sua função será ampliar a transparência e apoiar ações preventivas e decisões da fiscalização e gestão contratual.

13.18 Indicadores de capacitação e conhecimento

- cobertura das trilhas por papel;

- conclusão e desempenho nas avaliações;
- aplicação prática e prontidão para funções críticas;
- tempo de onboarding;
- lacunas de competência abertas e tratadas;
- materiais atualizados, vencidos ou sem responsável;
- transferências de conhecimento realizadas;
- concentração de conhecimento em pessoas ou fornecedores;
- redução de erros, retrabalho ou incidentes após a capacitação.

13.19 Indicadores de satisfação e valor público

A avaliação deverá ir além da entrega técnica e verificar uso, satisfação, resultado e benefício. Poderão ser utilizados:

- satisfação dos usuários e das áreas demandantes;
- adoção, usuários ativos e taxa de uso das funcionalidades relevantes;
- redução de tempo, etapas, deslocamentos ou trabalho manual;
- redução de erros e retrabalho no processo de negócio;
- melhoria de transparência, controle e qualidade da decisão;
- economia, custo evitado ou melhor uso de recursos;
- melhoria ambiental ou regulatória relacionada ao objetivo da solução;
- benefícios previstos, realizados e não realizados;
- motivos de baixa adoção ou descontinuação.

A entrada em produção não será considerada, isoladamente, evidência de sucesso. O gestor do negócio deverá participar da definição e da avaliação dos indicadores de benefício.

13.20 Metas, limites e faixas de desempenho

Metas e limites deverão ser aprovados com base em linha de base, contexto, risco, capacidade e objetivo. Sempre que adequado, poderão ser utilizadas faixas como dentro do esperado, atenção, crítico, não aplicável e dados insuficientes.

Valores específicos, metas contratuais e limiares sujeitos a atualização deverão permanecer em catálogo de indicadores, plano de medição, contrato, SLA ou documento operacional versionado, evitando congelamento inadequado no corpo permanente do PDS.

Metas deverão ser revisadas quando incentivarem comportamento disfuncional ou deixarem de apoiar decisão.

13.21 Painéis, relatórios e ciclos de análise

Nível	Periodicidade indicativa	Foco
Operacional	Contínua, diária ou semanal	Fluxo, impedimentos, incidentes, pipelines, testes e ações imediatas.
Tático	Semanal ou mensal	Capacidade, portfólio, qualidade, riscos, contratos e tendências.
Estratégico	Mensal, trimestral ou conforme governança	Valor, benefícios, riscos relevantes, investimentos e direcionamento.

Os painéis poderão ser consolidados pelo GovFlow a partir de fontes autorizadas. Cada ciclo de análise deverá produzir, quando necessário, decisão, responsável, prazo e acompanhamento. Painéis sem rotina de análise e ação deverão ser revistos ou descontinuados.

13.22 Uso responsável das métricas

As métricas deverão orientar melhoria do sistema de trabalho e não servir, isoladamente, para culpabilizar pessoas. São práticas inadequadas:

- comparar equipes ou produtos sem considerar contexto, complexidade e risco;
- usar quantidade de tarefas, commits ou linhas de código como avaliação individual simplista;
- premiar velocidade em detrimento de qualidade, segurança ou documentação;
- incentivar divisão artificial de itens para aumentar contagens;
- ocultar, adiar ou reclassificar defeitos, riscos e vulnerabilidades para melhorar o painel;
- interpretar médias sem distribuição, severidade ou volume;
- manter indicadores sem pergunta de gestão ou ação associada.

Indicadores deverão ser analisados em conjunto. Melhora aparente em prazo acompanhada de aumento de defeitos, incidentes ou retrabalho não deverá ser interpretada como ganho sustentável.

13.23 Revisão e evolução do catálogo de indicadores

O catálogo deverá ser revisado quando houver alteração do PDS, mudança de ferramenta ou fonte, novo contrato, mudança estratégica, baixa qualidade dos dados,

indicador sem uso, comportamento disfuncional, nova obrigação ou necessidade decisória. A revisão deverá avaliar custo de coleta, confiabilidade, utilização, impacto e redundância.

Indicadores retirados deverão ser arquivados com sua definição e período de validade. Séries históricas relevantes deverão ser preservadas, observadas as regras de segurança, privacidade e retenção.

14. Considerações Finais

14.1 Síntese institucional do PDS

LEITURA ORIENTADA: O Processo de Desenvolvimento de Software da SEMA/MT consolida um modelo institucional integrado para conceber, priorizar, contratar, desenvolver, testar, homologar, implantar, operar, manter, evoluir e descontinuar soluções digitais. O PDS organiza a participação das áreas de negócio, das unidades de tecnologia, das instâncias de governança, da fiscalização e gestão contratual, da fábrica de software e dos demais fornecedores, preservando a competência decisória de cada participante e a rastreabilidade de todo o ciclo de vida.

O processo aplica-se, de forma proporcional, ao desenvolvimento interno ou contratado, às evoluções, manutenções, sustentações, modernizações, integrações, iniciativas de dados e inteligência artificial, automações, componentes de infraestrutura relacionados ao software e atividades de descontinuação. Sua finalidade não é ampliar burocracia, mas reduzir ambiguidades, tornar decisões verificáveis, elevar a qualidade, proteger a continuidade dos serviços e assegurar que os investimentos em tecnologia produzam valor público.

O fluxo institucional parte do registro formal da demanda, passa por análise, refinamento, priorização, planejamento, desenvolvimento, testes, validação técnica, homologação de negócio, aceite, recebimento, implantação e acompanhamento operacional. Redmine, GovFlow, Enterprise Architect, Git/GitLab, pipelines de CI/CD, OpenShift e demais ferramentas homologadas apoiam esse fluxo, sem substituir autoridades, responsabilidades ou atos administrativos.

14.2 Princípios consolidados

A aplicação e a evolução do PDS deverão observar, de maneira conjunta, os seguintes princípios:

- foco em valor público, resultados institucionais e benefícios verificáveis;
- alinhamento com o planejamento estratégico, as políticas ambientais e as prioridades da SEMA/MT;
- participação efetiva da área demandante e do Gestor do Negócio;
- responsabilidades, autoridades e segregação de funções claramente definidas;
- rastreabilidade entre demanda, requisito, arquitetura, backlog, código, teste, release, homologação, aceite e recebimento;

- aplicação proporcional à criticidade, complexidade, risco, impacto, exposição e modalidade de execução;
- qualidade, segurança, privacidade e proteção de dados incorporadas desde a concepção;
- automação responsável, auditável e sujeita à governança;
- gestão contínua de riscos, oportunidades, exceções, dívida técnica e obsolescência;
- transparência, evidências, prestação de contas e preservação do histórico;
- continuidade, sustentabilidade, portabilidade e redução de dependências indevidas;
- aprendizagem institucional, capacitação e melhoria contínua baseada em resultados.

14.3 Aplicação obrigatória e proporcional

O PDS deverá ser observado pelas áreas demandantes, gestores do negócio, unidades da STI, CPQSI, CSTI, CITI, responsáveis por arquitetura, segurança e dados, fiscais, gestores contratuais, fábrica de software, fornecedores e demais participantes das iniciativas abrangidas. A observância do processo deverá constar, quando cabível, nos instrumentos de planejamento, contratação, Ordens de Serviço, planos de trabalho, termos de referência, procedimentos e orientações internas.

A obrigatoriedade não significa aplicação idêntica a qualquer situação. A profundidade dos artefatos, das análises, dos testes, das aprovações e das evidências deverá ser ajustada conforme criticidade, complexidade, risco, impacto institucional, dados tratados, exposição externa, custo, prazo, tamanho da mudança e modalidade de execução. Correções simples e de baixo risco poderão utilizar fluxo simplificado; sistemas corporativos críticos, integrações relevantes, tratamentos de dados sensíveis, soluções expostas à internet ou mudanças arquiteturais significativas deverão observar controles ampliados.

A simplificação deverá ser consciente e rastreável. A ausência de determinado artefato ou gate deverá decorrer de regra de proporcionalidade, decisão documentada ou exceção formal, e não de omissão, conveniência ou desconhecimento do processo.

14.4 Integração entre negócio, TI e fornecedores

A efetividade do PDS depende da atuação coordenada entre negócio, tecnologia, governança e fornecedores. Nenhuma dessas partes deverá conduzir isoladamente todas as decisões da iniciativa.

- As áreas de negócio definem necessidades, objetivos, regras, prioridades, critérios de aceite e benefícios esperados, participam da validação dos requisitos e realizam a homologação funcional;
- As unidades de tecnologia analisam viabilidade, estruturam a solução, orientam arquitetura e segurança, coordenam ou executam o desenvolvimento, validam tecnicamente e apoiam implantação e sustentação;
- As instâncias de governança avaliam alinhamento, valor, riscos, capacidade, conformidade, resultados e necessidade de escalonamento;
- A fábrica e os fornecedores executam as obrigações contratadas, mantêm profissionais qualificados, produzem artefatos, realizam testes, corrigem falhas, documentam e apresentam evidências;
- A fiscalização e a gestão contratual acompanham obrigações, desempenho, medição, qualidade, não conformidades, glosas, recebimentos e demais atos previstos no contrato.

A integração deverá ocorrer por meio de registros oficiais, reuniões objetivas, decisões documentadas, critérios claros e referências cruzadas entre as ferramentas. Comunicações informais poderão agilizar o trabalho, mas não deverão substituir os registros necessários para aprovação, homologação, aceite, risco, mudança, recebimento ou auditoria.

14.5 Responsabilidade pelas decisões

As decisões do PDS deverão ser tomadas por pessoas ou instâncias com competência compatível com sua natureza. Em especial:

- ferramentas, scripts, pipelines e automações não aprovam demandas, não homologam resultados, não aceitam riscos institucionais e não autorizam recebimentos;
- fornecedores e desenvolvedores não poderão aceitar risco institucional em nome da SEMA/MT;
- a área demandante não deverá aprovar isoladamente questões técnicas críticas, de arquitetura, segurança, infraestrutura ou conformidade;
- a equipe técnica não deverá homologar regras de negócio em nome dos usuários responsáveis;
- o encarregado pelo tratamento de dados pessoais não deverá ser tratado como executor exclusivo de todos os controles de privacidade;
- a fiscalização contratual não substitui a homologação funcional da área de negócio;
- a homologação funcional não substitui a validação técnica, o aceite formal ou o recebimento contratual;

- o recebimento provisório ou definitivo deverá observar competências, evidências e condições previstas nos instrumentos aplicáveis.

Quando uma decisão exigir competências distintas, deverá ser adotada aprovação conjunta ou sequência de validações, preservando a responsabilidade de cada participante.

14.6 Implantação progressiva do PDS

A implantação do PDS deverá ocorrer de forma planejada, progressiva e mensurável. A simples publicação do documento não caracteriza implantação efetiva. Recomenda-se a adoção das seguintes fases:

Fase 1 - Preparação. Estabelecer as condições institucionais para o início, incluindo aprovação e publicação, responsáveis designados, comunicação, plano de capacitação, catálogo inicial e cronograma de implantação.

Fase 2 - Adequação das ferramentas. Configurar workflows, trackers, campos, perfis, templates, integrações, repositórios, pipelines, permissões, painéis e documentação necessários ao processo.

Fase 3 - Projeto-piloto. Aplicar o PDS em iniciativa representativa e acompanhada, produzindo registros completos, evidências dos gates, indicadores iniciais, lições aprendidas e ajustes priorizados.

Fase 4 - Expansão controlada. Ampliar o uso para novos projetos, produtos e contratos, com onboarding das equipes, migração progressiva, tratamento de exceções e monitoramento de aderência e qualidade.

Fase 5 - Estabilização e evolução. Consolidar o modelo por meio de auditorias, avaliação de maturidade, melhoria das automações, atualização dos materiais, gestão dos indicadores e plano contínuo de evolução.

O cronograma, os responsáveis, as prioridades e os critérios de passagem entre fases deverão ser definidos em plano de implantação aprovado. A expansão deverá considerar capacidade das equipes, maturidade das ferramentas, riscos, disponibilidade contratual e necessidade de continuidade das entregas em andamento.

14.7 Regras de transição

A transição para o novo PDS deverá preservar a continuidade dos serviços e evitar retrabalho sem benefício. Projetos e demandas iniciados após a data de vigência deverão adotar o processo conforme sua aplicabilidade. Iniciativas em andamento deverão passar por avaliação de aderência, com definição do que será mantido, regularizado, migrado, simplificado ou excepcionalmente dispensado.

Não será necessário reconstruir retroativamente todos os artefatos de uma iniciativa quando o custo superar o benefício. Contudo, lacunas que afetem segurança, legalidade, rastreabilidade, qualidade, continuidade, homologação, aceite, propriedade dos ativos, transferência de conhecimento ou recebimento deverão ser tratadas prioritariamente.

Durante a transição, deverão ser preservados documentos, decisões, modelos, código, evidências, históricos, dados, riscos e vínculos relevantes. Migrações entre ferramentas deverão ser planejadas e validadas para evitar perda de informação ou ruptura da rastreabilidade.

14.8 Projetos, produtos e contratos em andamento

Cada iniciativa em andamento deverá ser avaliada e classificada, de forma proporcional, em uma das condições abaixo:

Aderente. A iniciativa já observa os controles essenciais do PDS; deverá manter o fluxo e corrigir apenas lacunas pontuais.

Parcialmente aderente. A iniciativa atende parte relevante do processo, mas possui lacunas; deverá adotar plano de adequação priorizado por risco e benefício.

Em transição. A iniciativa necessita migrar fluxos, registros, ferramentas ou responsabilidades; deverá possuir cronograma, responsáveis, controles temporários e marco de conclusão.

Exceção temporária. A iniciativa não consegue cumprir determinada prática no prazo de implantação; deverá registrar risco, justificativa, controle compensatório, autoridade, prazo e regularização.

Em descontinuação. O produto ou a iniciativa será encerrado ou substituído; deverão ser aplicados controles de preservação, migração, segurança, comunicação e desligamento.

Contratos vigentes deverão ser analisados antes da inclusão de novas obrigações. O PDS não altera automaticamente escopo, preço, prazo, critérios de medição ou responsabilidades contratuais. Adequações poderão exigir Ordem de Serviço, termo aditivo, instrumento complementar, negociação, planejamento de transição ou aplicação apenas aos novos ciclos, conforme análise jurídica, administrativa e técnica.

14.9 Configuração e adequação das ferramentas

A implantação operacional dependerá da configuração controlada das ferramentas e plataformas. Deverão ser avaliados e ajustados, conforme aplicável:

- projetos, trackers, tipos de item, status, workflows, papéis, permissões, campos personalizados, categorias, versões e relações no Redmine;
- regras declarativas, validações, integrações, automações, logs, relatórios e health checks no GovFlow;
- repositórios, pacotes, baselines, modelos e vínculos no Enterprise Architect;
- grupos, projetos, branches, merge requests, runners, pipelines, pacotes, releases e permissões no Git/GitLab;
- ambientes, namespaces, imagens, secrets, recursos, observabilidade, backup e recuperação no OpenShift e plataformas relacionadas;
- catálogos, painéis, bases de conhecimento, formulários e sistemas administrativos utilizados no ciclo.

Toda alteração relevante de configuração deverá seguir o processo de gestão de mudanças definido no Capítulo 10. Ambientes de homologação deverão ser utilizados para validar workflows, integrações, permissões e automações antes da implantação em produção.

14.10 Gestão das exceções durante a implantação

Exceções transitórias poderão ser necessárias durante a implantação, mas deverão possuir prazo e governança. Cada exceção relevante deverá registrar, no mínimo, objeto, motivo, escopo, risco, impacto, controle compensatório, responsável, autoridade aprovadora, data de início, prazo de validade, condição de revisão e plano de regularização.

Exceções vencidas deverão ser escalonadas. A renovação não deverá ser automática e exigirá nova análise do risco, da capacidade e das alternativas. Exceções

reiteradas poderão indicar inadequação do processo, limitação estrutural, problema contratual ou necessidade de atualização do PDS.

14.11 Governança da evolução do PDS

A manutenção do PDS deverá possuir responsável institucional definido. Caberá à governança do processo receber propostas, avaliar impactos, consultar áreas, analisar métricas, consolidar lições aprendidas, acompanhar mudanças legais e tecnológicas, preparar versões, coordenar aprovações e comunicar alterações.

Propostas de mudança deverão apresentar problema, justificativa, impacto, alternativas, benefícios, riscos, áreas afetadas, necessidade de capacitação, alteração de ferramentas e plano de transição. Mudanças relevantes não deverão ser incorporadas de forma informal ou silenciosa.

Procedimentos, catálogos e guias complementares poderão evoluir com maior frequência do que o corpo principal, desde que sua governança, versionamento, compatibilidade e autoridade estejam definidos.

14.12 Revisão ordinária e extraordinária

O PDS deverá ser submetido a revisões ordinárias em periodicidade definida pela SEMA/MT, considerando indicadores, auditorias, maturidade, resultados, dificuldades de aplicação e evolução institucional. A periodicidade específica poderá ser estabelecida em ato ou plano complementar para permitir ajustes sem reedição desnecessária deste documento.

Revisões extraordinárias poderão ocorrer diante de alteração legal ou regimental, nova política, novo contrato, incidente relevante, auditoria, mudança tecnológica, descontinuação de ferramenta, risco emergente, baixa eficácia, reorganização institucional ou mudança estratégica. A urgência não elimina a necessidade de registro, aprovação e comunicação.

14.13 Controle de versão e histórico de alterações

Cada versão do PDS deverá registrar número, data, responsável pela elaboração, autoridade aprovadora, capítulos e anexos alterados, resumo das mudanças, justificativa,

impactos, data de vigência e documentos relacionados. Alterações substanciais deverão indicar ações de transição e capacitação.

Versões anteriores deverão ser preservadas em repositório oficial, com identificação de sua vigência. O histórico deverá permitir compreender qual regra se aplicava a cada período, projeto, contrato ou decisão relevante. Minutas, versões de trabalho e versões aprovadas deverão ser claramente diferenciadas.

14.14 Comunicação e publicação

A aprovação e as alterações relevantes deverão ser comunicadas aos públicos afetados por meios institucionais adequados, incluindo publicação, avisos, reuniões, guias de mudança, capacitações, base de conhecimento e atualização dos modelos e ferramentas.

A comunicação deverá explicar o que mudou, quem é afetado, quando a regra entra em vigor, quais ações são necessárias, quais materiais foram atualizados e onde obter suporte. Mudanças que alterem responsabilidades, gates, critérios de aceite, segurança, ferramentas ou obrigações contratuais exigirão atenção especial.

14.15 Prevalência normativa e compatibilidade documental

O PDS complementa, mas não substitui, a legislação, o Regimento Interno, as políticas institucionais, os atos administrativos, os contratos, termos de referência, acordos, normas de segurança, proteção de dados, gestão documental e demais instrumentos aplicáveis. Também não cria, por si só, competência ou obrigação contratual não prevista em instrumento válido.

Em caso de conflito ou incompatibilidade, deverá ser aplicado o instrumento juridicamente superior ou mais específico, sem prejuízo do registro da divergência e do encaminhamento para correção. A unidade responsável deverá avaliar se o PDS, o procedimento complementar, a configuração da ferramenta ou o instrumento relacionado necessita atualização.

Referências a frameworks, normas técnicas e boas práticas deverão ser interpretadas como orientação institucional compatível com o contexto da SEMA/MT, salvo quando houver adoção formal ou exigência legal ou contratual expressa.

14.16 Critérios de efetividade da implantação

A implantação deverá ser considerada efetiva quando houver evidências de aplicação real e melhoria do sistema de trabalho. Entre os sinais esperados estão:

- demandas registradas, qualificadas e priorizadas com critérios transparentes;
- responsáveis, decisões, riscos, requisitos, critérios de aceite e dependências claramente identificados;
- rastreabilidade entre os registros de negócio, arquitetura, código, testes, releases e recebimentos;
- uso consistente dos workflows, gates, templates, ferramentas e evidências;
- capacitação e prontidão dos participantes para seus papéis;
- testes, segurança, homologação e aceite realizados de forma verificável;
- redução de retrabalho, falhas evitáveis, atrasos sem explicação e decisões informais;
- melhoria da previsibilidade, da qualidade, da continuidade e do tratamento de riscos;
- indicadores analisados e convertidos em decisões, responsáveis e ações;
- benefícios, satisfação, adoção e valor público avaliados após a entrega.

A conformidade documental isolada não será suficiente. A avaliação deverá considerar eficácia, resultados, qualidade das evidências, adequação ao risco e capacidade de aprendizado institucional.

14.17 Compromisso com valor público e melhoria contínua

O sucesso do PDS será medido pela capacidade de produzir soluções úteis, seguras, sustentáveis e alinhadas às políticas públicas. O processo deverá contribuir para melhorar serviços ambientais, fiscalização, monitoramento, transparência, atendimento ao cidadão, integração de informações, qualidade das decisões, continuidade operacional e uso responsável dos recursos públicos.

A melhoria contínua deverá utilizar métricas, auditorias, incidentes, defeitos, riscos, retrospectivas, avaliações de usuários, desempenho contratual, lições aprendidas e evolução tecnológica. A busca por velocidade não deverá comprometer qualidade, segurança, proteção de dados, acessibilidade, documentação ou sustentabilidade.

Artefatos, tickets, diagramas, pipelines e relatórios são meios. O resultado esperado é a entrega de valor público com responsabilidade, previsibilidade, confiança e capacidade de evolução.

14.18 Disposições finais

Os casos omissos deverão ser encaminhados às unidades e instâncias competentes, considerando natureza, risco, impacto e responsabilidades estabelecidas. Documentos complementares poderão detalhar procedimentos, matrizes, catálogos, formulários, checklists, templates, critérios de proporcionalidade e parâmetros operacionais, desde que sejam compatíveis com este PDS.

A entrada em vigor ocorrerá conforme o ato de aprovação e publicação. A aplicação deverá ser acompanhada, avaliada e aperfeiçoada de forma contínua. Alterações no PDS, em seus anexos e em documentos complementares deverão observar governança, controle de versão, comunicação, capacitação e preservação do histórico.

Com a adoção deste processo, a SEMA/MT estabelece uma base comum para integrar estratégia, negócio, tecnologia, dados, segurança, contratação e operação, promovendo entregas mais consistentes e decisões mais transparentes ao longo de todo o ciclo de vida das soluções digitais.

15. Anexos, Modelos e Instrumentos Operacionais

LEITURA ORIENTADA: Este capítulo organiza os instrumentos que apoiam a execução, o controle, a comprovação e a melhoria do Processo de Desenvolvimento de Software da SEMA/MT. Os modelos devem ser aplicados com proporcionalidade, conforme a criticidade, o risco, a complexidade, a modalidade de execução e as obrigações administrativas ou contratuais da iniciativa.

15.1 Finalidade e classificação dos anexos

Os anexos transformam as diretrizes do PDS em instrumentos de trabalho. Eles não substituem sistemas oficiais, atos administrativos, contratos, termos de referência ou documentos exigidos pela legislação. Quando houver instrumento oficial específico, o modelo deste capítulo atua como checklist, referência de conteúdo ou complemento operacional.

Categoria	Características	Exemplos
I - Anexos normativos	Integram o PDS e mudam com nova versão formal.	Glossário, macrofluxo, matriz de fontes oficiais.
II - Modelos controlados	Podem evoluir mediante procedimento de governança e controle de versão.	Planos, checklists, termos, relatórios e registros.
III - Catálogos dinâmicos	Atualização mais frequente, sem alterar princípios do PDS.	Ferramentas, campos, metas, tecnologias, contatos e versões.

15.2 Regras de utilização e preenchimento

- Utilizar somente os campos aplicáveis e registrar justificativa quando um item relevante não for utilizado.
- Preservar identificadores, autoria, data, versão, vínculos e evidências.
- Evitar duplicar informações já mantidas em fonte oficial; preferir referência cruzada.
- Registrar decisões, ressalvas, riscos residuais, exceções e autoridades responsáveis.
- Proteger dados pessoais, credenciais, segredos e informações classificadas.
- Manter linguagem objetiva, verificável e coerente com o estado real da iniciativa.

15.3 Governança e atualização dos modelos

Cada instrumento deverá possuir código, versão, responsável funcional, responsável técnico quando aplicável, data de vigência, repositório oficial e histórico de alterações. Mudanças que alterem responsabilidades, gates, critérios de aceite, obrigações contratuais ou controles de segurança dependem de aprovação da instância competente.

15.4 Catálogo de instrumentos do PDS

Código	Instrumento	Categoria
A	Glossário do PDS	Normativo
B	Visão consolidada do ciclo do PDS	Normativo
C	Matriz das fontes oficiais	Normativo
D	Formulário de abertura de demanda	Controlado
E	Análise preliminar da demanda	Controlado
F	Documento de visão do produto	Controlado
G	Registro de priorização	Controlado
H	História de usuário e critérios de aceite	Controlado
I	Especificação de requisito	Controlado
J	Checklist da Definition of Ready	Controlado
K	Plano de ciclo de execução	Controlado
L	Ordem de Serviço e plano de execução	Controlado
M	Relatório de acompanhamento da fábrica	Controlado
N	Estratégia ou plano de testes	Controlado
O	Caso e roteiro de teste	Controlado
P	Relatório de execução de testes	Controlado
Q	Roteiro de homologação	Controlado
R	Termo de homologação funcional	Controlado
S	Parecer de validação técnica	Controlado
T	Checklist da Definition of Done	Controlado
U	Termo de aceite funcional	Controlado
V	Termo de recebimento provisório	Controlado
W	Termo de recebimento definitivo	Controlado
X	Checklist para medição ou faturamento	Controlado
Y	Plano de implantação	Controlado

Código	Instrumento	Categoria
Z	Plano de rollback	Controlado
AA	Checklist de prontidão para produção	Controlado
AB	Registro de incidente	Controlado
AC	Relatório de problema e causa raiz	Controlado
AD	Registro de mudança e hotfix	Controlado
AE	Plano de sustentação	Controlado
AF	Checklist de segurança e privacidade	Controlado
AG	Registro de vulnerabilidade	Controlado
AH	Registro de risco	Controlado
AI	Solicitação e aprovação de exceção	Controlado
AJ	Triagem de proteção de dados e RIPD	Controlado
AK	Registro interno de incidente com dados pessoais	Controlado
AL	Referência para comunicação à ANPD	Dinâmico
AM	Solicitação de direitos do titular	Controlado
AN	Termo de consentimento, quando aplicável	Controlado
AO	Ficha de indicador	Controlado
AP	Plano de capacitação	Controlado
AQ	Registro de transferência de conhecimento	Controlado
AR	Registro de lições aprendidas	Controlado
AS	Checklist de encerramento	Controlado
AT	Matriz RACI de referência	Normativo

15.4.1 Quadro-resumo de artefatos, responsáveis e fontes oficiais

O quadro-resumo organiza, por etapa, os principais artefatos, o responsável principal, os participantes de apoio, a fonte oficial, o gate relacionado e a entrega esperada. Sua finalidade é orientar a consulta rápida e reduzir dúvidas sobre onde registrar e quem deve produzir, validar ou acompanhar cada informação.

Uso do quadro: a figura não substitui os modelos dos Anexos A a AT nem os instrumentos administrativos e contratuais. Havendo divergência, prevalecem o capítulo correspondente, o modelo vigente e o sistema oficial competente.

SEMA SECRETARIA DE ESTADO DE MEIO AMBIENTE — GOVERNO DE MATO GROSSO

QUADRO-RESUMO DE ARTEFATOS, RESPONSÁVEIS E FONTES OFICIAIS

Visão consolidada dos artefatos produzidos em cada etapa, responsáveis principais, participantes de apoio e fontes oficiais

PDS v2.0

ETAPA DO PROCESSO	DESCRIÇÃO DA ETAPA	ARTEFATOS PRINCIPAIS	RESPONSÁVEL PRINCIPAL	PARTICIPANTES DE APOIO	FONTE / FERRAMENTA OFICIAL	GATE RELACIONADO	ENTREGA PRINCIPAL DA ETAPA
1 DEMANDA E TRIAGEM	Registro da demanda e triagem inicial para classificação e enquadramento.	• Formulário de Demanda • Análise Preliminar • Classificação da Demanda	Área Demandante	CSTI, Gestor de Negócio (PO), CQPSI	Redmine	G1 Demanda Registrada	Demanda registrada e classificada no Redmine.
2 ANÁLISE E PLANEJAMENTO	Análise preliminar, priorização e definição do plano de execução.	• Documento de Visão / Backlog • Priorização (MoSCoW/WSJF) • Plano de Trabalho / Sprint	CSTI	Área Demandante, PO, CQPSI, CTII	Redmine	G3 Viabilidade Aprovada	Plano de execução aprovado e backlog priorizado.
3 EXECUÇÃO	Desenvolvimento, interação contínua e geração de entregas incrementais.	• Código Fonte • Merge Request • Builds e Artefatos • Relatórios de Execução	Fábrica de Software / TI	CTII, QA, Segurança da Informação	GitLab	G5 Code Review Aprovado	Funcionalidades desenvolvidas e disponíveis em ambiente de testes.
4 TESTES E VALIDAÇÕES	Testes automatizados, funcionais e não funcionais, e validações técnicas.	• Plano de Testes • Casos de Teste • Relatórios de Testes • Evidências de Teste	QA / Fábrica de Software	Área Demandante, CTII, CQPSI, Segurança	GitLab (ou Redmine EA)	G7 Testes Aprovados	Solução validada tecnicamente e pronta para homologação.
5 HOMOLOGAÇÃO E ACEITE	Homologação funcional pela área demandante e aceite formal da solução.	• Termo de Homologação • Termo de Aceite	Área Demandante	CSTI, Fábrica, Fiscalização do Contrato	Redmine	G10 Aceite Formalizado	Solução homologada e aceita formalmente.
6 RECEBIMENTO E IMPLANTAÇÃO	Recebimento provisório e definitivo e implantação em produção.	• Termo de Recebimento Provisório • Termo de Recebimento Definitivo • Plano de Implantação • Release Notes	Fiscalização do Contrato	Fábrica de Software, TI / DevOps, Área Demandante	OpenShift (ambiente oficial)	G13 Recebimento Definitivo	Solução implantada em produção e recebida definitivamente.
7 SUSTENTAÇÃO E MELHORIA	Operação, suporte, monitoramento e gestão de melhorias contínuas.	• Plano de Sustentação • Registros de Incidentes e Problemas • Solicitações/Backlog de Melhoria • Relatórios de Service Desk	TI / Fábrica	Área Demandante, CSTI, Fiscalização, CQPSI	Observabilidade (Zabbix/Prometheus ou equivalente)	G18 Sustentação Estabilizada	Solução operando, monitorada e em evolução contínua.

LEGENDA DE ÍCONES E CORES

- 1 Demanda e Análise
- 2 Execução e Desenvolvimento
- 4 Testes e Validações
- 5 Homologação e Aceite
- 5 Implantação e Recebimento
- 6 Sustentação e Melhoria

GATES (PONTOS DE CONTROLE)

G1, G3, G5, G7, G10, G13 e G15 representam os momentos formais de aprovação e controle de qualidade ao longo do ciclo de vida.

PRINCIPAIS FERRAMENTAS

- **Redmine:** gestão de demandas, backlog, artefatos e workflow.
- **GitLab:** versionamento, CI/CD, code review e rastreabilidade.
- **OpenShift:** ambientes de execução, implantação e orquestração.
- **Observabilidade:** monitoramento, métricas e análise de desempenho.

OBSERVAÇÕES IMPORTANTES

- Todos os artefatos devem estar vinculados à demanda no Redmine.
- A rastreabilidade entre requisitos, código, testes e deploy é obrigatória.
- Os artefatos devem seguir os modelos oficiais do PDS.
- A fiscalização valida artefatos e aprova cada gate.
- Qualquer exceção deve ser registrada e justificada.

BENEFÍCIOS DO CONTROLE DE ARTEFATOS

- Transparência e rastreabilidade ponta a ponta
- Qualidade e conformidade desde o início
- Agilidade com governança e controle
- Redução de riscos e retrabalhos
- Geração de valor público e continuidade da solução

DOCUMENTO OFICIAL
PDS - Plano de Desenvolvimento de Sistemas SEMAD/MT - v2.0

REFERÊNCIA NORMATIVA
Capítulos 1 a 15 do PDS e Anexos A a T

PÚBLICO-ALVO
Todas as áreas da SEMA/MT, STI, Comissão, Fábrica de Software e Fiscalização do Contrato

OBJETIVO
Padronizar artefatos, responsabilidades e fontes para garantir qualidade e valor público.

DATA
Maio/2025

15.5 Diagramas e representações do processo

Os fluxos oficiais devem utilizar notação compreensível e independente de produto. BPMN poderá ser modelado no Enterprise Architect ou em solução institucional homologada. O GovFlow poderá automatizar verificações e transições, sem substituir as autoridades definidas no PDS. Diagramas exportados devem manter vínculo com o arquivo-fonte versionado.

15.6 Referências, vínculos e armazenamento oficial

Os instrumentos preenchidos deverão ser vinculados à demanda, produto, projeto, versão, Ordem de Serviço, processo administrativo ou contrato correspondente. O Redmine deverá armazenar o registro operacional e os links; documentos administrativos permanecem no sistema oficial competente; código e documentação versionável permanecem no Git/GitLab; modelos e arquitetura permanecem no Enterprise Architect quando aplicável.

15.7 Lista dos anexos integrantes

Os anexos A a AT apresentados a seguir constituem referência institucional. A versão editável e vigente de cada modelo deverá ser disponibilizada em repositório oficial controlado.

ANEXO A - Glossário do PDS

> ***NOTA DE APLICAÇÃO:*** *Termos usados no processo, organizados alfabeticamente. A definição contextual prevalece sobre usos informais.*

A.1 Glossário resumido para não técnicos

Antes do glossário técnico completo, a Figura abaixo apresenta os termos mais recorrentes em linguagem acessível. Ela foi concebida para apoiar áreas demandantes, gestores, homologadores, fiscais e demais participantes que não atuam diretamente em desenvolvimento de software.

Complementaridade: o glossário visual facilita a compreensão inicial. Para definições formais, siglas, termos técnicos e interpretações específicas, deve ser consultada a tabela completa deste Anexo A.

SEMA Secretaria de Estado de Meio Ambiente — Governo de Mato Grosso

SEMA SECRETARIA DE ESTADO DE MEIO AMBIENTE — GOVERNO DE MATO GROSSO

GLOSSÁRIO RESUMIDO DO PDS – PARA NÃO TÉCNICOS

PDS v2.0

Principais termos do Processo de Desenvolvimento de Software explicados de forma simples, objetiva e contextualizada

TERMO	O QUE SIGNIFICA	PARA QUE SERVE	EXEMPLO PRÁTICO
Demanda	Solicitação de uma necessidade ou problema a ser resolvido por meio de TI.	Inicia oficialmente o pedido de solução.	Uma secretaria solicita um sistema para controle de licenças ambientais.
Triagem	Análise inicial para entender, categorizar e direcionar a demanda para o caminho correto.	Garantir que cada demanda seja tratada da forma adequada desde o início.	A equipe verifica se a solicitação é de um novo sistema ou melhoria em um sistema existente.
Área Demandante	Setor ou pessoa que identifica a necessidade e solicita a solução.	Representa quem será beneficiado pela solução.	A Coordenação de Fiscalização é quem pede o sistema.
Backlog	Lista organizada de todas as demandas que aguardam atendimento.	Permite priorizar e planejar o que será feito.	As demandas aprovadas ficam no backlog e aguardando desenvolvimento.
História de Usuário	Descrição simples da necessidade do usuário e do valor esperado.	Ajuda a equipe a entender o que deve ser entregue.	"Como fiscal, quero registrar uma multa para acompanhar os processos."
Critério de Aceite	Condições que devem ser atendidas para considerar que a solução está pronta.	Garantir que todos entendam o que é "feito" e "aprovado".	"O sistema deve gerar relatório em PDF com filtros por data."
Homologação	Validação da solução pela área demandante em ambiente de testes.	Confirma se a solução atende às necessidades reais.	A área testará o sistema e dará seu OK para ir para a a produção.
Aceite	Confirmação formal de que a solução atende às necessidades e pode ser usada.	Autoriza o escalonamento e implantação.	A área assina o termo de aceite autorizando a implantação.
Recebimento Provisório	Entrega inicial da solução para teste, com acompanhamento por um período.	Permite verificar se tudo está funcionando como esperado na prática.	O sistema entra em produção e será acompanhado por 30 dias.

TERMO	O QUE SIGNIFICA	PARA QUE SERVE	EXEMPLO PRÁTICO
Recebimento Definitivo	Confirmação final de que a solução está estável e atende totalmente ao esperado.	Encerrar a entrega e formalizar a conclusão do contrato.	Após o período de acompanhamento, a solução é aprovada definitivamente.
Implantação	Disponibilização da solução em ambiente de produção para os usuários.	Tornar o sistema disponível para uso real.	O sistema é publicado para todos os fiscais utilizarem.
Incidente	Qualquer falha ou problema que interrompa ou prejudique o uso do sistema.	Restaurar o funcionamento o mais rápido possível.	O sistema apresenta erro e o usuário abre um chamado.
Problema	Causa raiz de um ou mais incidentes.	Eliminar a causa para evitar novas falhas.	A equipe descobre que o erro ocorre por uma configuração incorreta do servidor.
Risco	Evento que pode acontecer e gerar impacto negativo no projeto ou na solução.	Antecipar e reduzir impactos negativos.	Risco de atraso no entrega por falta de recursos.
Risco Residual	Risco que permanece mesmo após as ações de mitigação.	Manter sob controle e monitoramento contínuo.	Mesmo com ações, ainda pode haver pequeno risco de falha.
Pipeline (CI/CD)	Automação que compila, testa e entrega o código de forma automatizada.	Agiliza entregas e reduz erros humanos.	Toda vez que o código é alterado, os testes rodam automaticamente.
Teste Automatizado	Testes executados por ferramentas para verificar se o sistema funciona corretamente.	Garante mais qualidade e rapidez nas validações.	Testes que validam se a função cadastrou ou calculou certo, funcionando.
Indicadores	Métricas usadas para acompanhar desempenho, qualidade e resultados.	Permitem avaliar se os objetivos estão sendo alcançados.	Ex.: prazo médio de entrega, % de testes aprovados, número de incidentes.

POR QUE ESSES TERMOS IMPORTAM?

Eles ajudam todos os times a falarem a mesma língua, tomarem decisões melhores e garantirem que a solução entregue gere valor público de forma transparente, segura e com qualidade.

LEGENDA DE ÍCONES

- Início e Planejamento
- Execução e Desenvolvimento
- Validação e Aceite
- Implantação e Operação
- Controle e Melhoria

DICA RÁPIDA

Em caso de dúvida, consulte o PDS completo ou fale com a Coordenação de Sistemas e Tecnologia da Informação (CSTI).

Controle do instrumento	Preenchimento
Código e versão	PDS-A | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Termo	Definição
Aceite funcional	Manifestação da área competente de que a entrega atende aos critérios funcionais aplicáveis.
ADR	Registro de decisão arquitetural, contexto, alternativas, decisão e consequências.
Backlog	Lista priorizada e continuamente refinada de demandas, capacidades, requisitos, histórias, defeitos ou melhorias.
CI/CD	Práticas e automações de integração, teste, empacotamento e entrega ou implantação contínua.
Critério de aceite	**Condição objetiva e verificável para validar o comportamento ou resultado esperado.**
Cycle time	Tempo entre o início efetivo do trabalho e sua conclusão no fluxo definido.
DAST	Teste dinâmico de segurança realizado sobre aplicação em execução.
Defeito	Não conformidade em artefato ou software que pode causar falha.
Definition of Done	Conjunto mínimo de condições para considerar um item concluído.
Definition of Ready	Conjunto mínimo de condições para considerar um item apto à execução.
DevSecOps	Integração de desenvolvimento, segurança e operação ao longo do ciclo de vida.
EA	Enterprise Architect, repositório de modelagem, arquitetura, processos e rastreabilidade técnica.
Evidência	Registro verificável que demonstra execução, decisão, resultado ou conformidade.
Falha	Manifestação observável de comportamento incorreto durante a execução.
Gate	Ponto de verificação que condiciona a continuidade do fluxo ao atendimento de critérios.

Termo	Definição
GovFlow	Camada de orquestração, automação, integração e validação das regras do PDS.
História de usuário	**Descrição de necessidade sob a perspectiva de um perfil, benefício e critérios de aceite.**
Homologação	Validação funcional realizada por representante competente do negócio em ambiente apropriado.
Hotfix	Mudança emergencial e controlada para restaurar ou proteger serviço crítico.
IaC	Infraestrutura como código, com configuração versionada e automatizável.
Incidente	Evento que interrompe ou degrada serviço ou ameaça sua disponibilidade, integridade ou confidencialidade.
Lead time	Tempo total entre a entrada da demanda no fluxo e a entrega do resultado.
Merge request	Proposta controlada de integração de alterações ao repositório.
MTTR	Tempo médio de restauração ou recuperação, conforme definição do indicador.
Observabilidade	Capacidade de compreender o estado interno do sistema por logs, métricas, traces e eventos.
Ordem de Serviço	**Instrumento que autoriza e delimita execução contratada, produtos, prazos e critérios.**
Pipeline	Sequência automatizada de build, testes, análises, empacotamento e implantação.
Problema	Causa ou condição subjacente relacionada a um ou mais incidentes.
Rastreabilidade	Capacidade de relacionar demanda, requisito, código, teste, versão, evidência, aceite e decisão.
Recebimento definitivo	Ato contratual posterior às verificações e ao cumprimento das condições aplicáveis.
Recebimento provisório	Ato inicial de recebimento contratual para verificação posterior.
Redmine	Plataforma operacional e fonte oficial dos registros do fluxo do PDS.
Release	**Versão preparada e autorizada para disponibilização em ambiente definido.**
RIPD	Relatório de Impacto à Proteção de Dados Pessoais, elaborado quando aplicável conforme risco e orientação competente.

Termo	Definição
Risco inerente	Nível de risco antes da aplicação dos controles.
Risco residual	Nível de risco remanescente após controles e respostas.
Rollback	Retorno controlado a estado estável anterior após falha ou decisão de reversão.
SAST	Análise estática de segurança sobre código ou artefato sem execução da aplicação.
SBOM	Inventário dos componentes de software presentes em um produto ou artefato.
SCA	Análise de componentes, dependências, vulnerabilidades conhecidas e licenças.
SLA	Acordo ou nível de serviço com metas e critérios definidos em instrumento aplicável.
Sprint	Ciclo time-boxed usado em abordagens Scrum; não é obrigatório para todas as iniciativas.
Stakeholder	Pessoa, grupo ou unidade afetada, interessada ou com influência sobre a iniciativa.
Teste de regressão	Verificação de que alterações não comprometeram comportamentos já validados.
Teste unitário	Teste automatizado de pequena unidade de código, preferencialmente isolada.
Vulnerabilidade	Fraqueza que pode ser explorada e produzir impacto adverso.
WSJF	Método de priorização que relaciona custo do atraso e tamanho do trabalho.

ANEXO B - Visão consolidada do ciclo do PDS

> ***NOTA DE APLICAÇÃO:*** *Macrofluxo institucional para comunicação, treinamento e rastreabilidade. A representação gráfica completa está na Figura 2, Seção 3.1.1.*

Controle do instrumento	Preenchimento
Código e versão	PDS-B | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Etapa	Resultado principal	Gate ou decisão
1. Registro	**Demanda formal, responsável e resultado esperado.**	**Admissibilidade e completude.**
2. Triagem	Classificação, criticidade e encaminhamento.	Aceitar, complementar, rejeitar ou redirecionar.
3. Análise	Viabilidade, escopo, riscos, dados e arquitetura.	Recomendação técnica e de negócio.
4. Priorização	Posição no portfólio e capacidade alocada.	Autoridade competente.
5. Planejamento	Backlog, OS, estimativas e critérios.	Definition of Ready.
6. Execução	Código, configuração, documentação e evidências.	Revisões e controles técnicos.
7. Testes	**Resultados funcionais e não funcionais.**	**Critérios de saída.**
8. Validação técnica	Parecer sobre qualidade, segurança e prontidão.	Apto, condicionado ou não apto.
9. Homologação	Validação do negócio.	Aprovação, ressalva ou reprovação.
10. Aceite e recebimento	Atos funcionais e contratuais distintos.	Autoridades competentes.
11. Implantação	Release em produção com monitoramento e rollback.	Go/no-go.
12. Operação	Serviço monitorado e sustentado.	SLA, incidentes e mudanças.
13. Encerramento	Conhecimento, pendências e lições preservados.	Checklist de encerramento.

> ***NOTA DE APLICAÇÃO:*** *Representação textual: Demanda → Triagem → Análise → Priorização → Planejamento → Execução → Testes → Validação técnica → Homologação → Aceite → Recebimento → Implantação → Operação e sustentação → Encerramento.*

ANEXO C - Matriz das fontes oficiais

Controle do instrumento	Preenchimento
Código e versão	PDS-C | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Objeto de informação	Fonte oficial primária	Referência complementar
Demanda, backlog, workflow e decisões operacionais	Redmine	GovFlow e documentos vinculados
Arquitetura, BPMN, UML, dados e baselines	Enterprise Architect	Redmine e Git/GitLab
Código, IaC, documentação versionável e pipeline	Git/GitLab	Redmine
Regras de automação e validação	GovFlow	Repositório versionado e Redmine
Builds, testes, scans e artefatos	Pipeline CI/CD e repositório de artefatos	Git/GitLab e Redmine
Processo administrativo e contrato	Sistema administrativo oficial	Redmine como referência operacional
Homologação, aceite e pareceres	Redmine e documento oficial aplicável	Evidências anexas
Implantação e observabilidade	Plataforma operacional	Redmine, pipeline e dashboards

ANEXO D - Formulário de abertura de demanda

Controle do instrumento	Preenchimento
Código e versão	PDS-D | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Identificação

Campo	Preenchimento / evidência
ID da demanda	
Unidade demandante	
Solicitante e contato	
Gestor do Negócio	
Patrocinador, quando aplicável	
Data da solicitação	

Necessidade

Campo	Preenchimento / evidência
Problema ou oportunidade	
Resultado esperado	
Usuários e públicos afetados	
Processo de negócio relacionado	
Prazo motivador e justificativa	
Obrigação legal ou compromisso	

Campo	Preenchimento / evidência
Sistemas e integrações relacionadas	
Dados pessoais ou sensíveis envolvidos	
Benefícios esperados e indicadores	

Validação da área demandante

Item de verificação	Sim	Não	N/A	Evidência / observação
A necessidade foi validada pela chefia ou autoridade competente.	☐	☐	☐	
O Gestor do Negócio foi indicado e conhece suas responsabilidades.	☐	☐	☐	
Foram anexadas evidências, normas, fluxos ou documentos relevantes.	☐	☐	☐	
O resultado esperado está descrito sem antecipar indevidamente a solução.	☐	☐	☐	

ANEXO E - Análise preliminar da demanda

Controle do instrumento	Preenchimento
Código e versão	PDS-E | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Síntese

Campo	Preenchimento / evidência
ID da demanda	
Analista responsável	
Entendimento do problema	
Escopo inicial	
Itens fora do escopo	
Alternativas consideradas	

Avaliação

Campo	Preenchimento / evidência
Viabilidade técnica	
Viabilidade operacional	
Impacto arquitetural	
Dados e privacidade	
Segurança	
Dependências	
Riscos iniciais	
Estimativa preliminar	

Campo	Preenchimento / evidência
Modalidade de execução	
Disponibilidade contratual ou capacidade interna	

Recomendação

Campo	Preenchimento / evidência
Recomendação final	
Condições para prosseguir	
Autoridade ou instância decisória	
Data e responsáveis	

ANEXO F - Documento de visão do produto

Controle do instrumento	Preenchimento
Código e versão	PDS-F | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Visão

Campo	Preenchimento / evidência
Nome do produto	
Propósito	
Problema central	
Públicos e personas	
Proposta de valor público	
Resultados mensuráveis	

Escopo

Campo	Preenchimento / evidência
Capacidades principais	
Escopo inicial	
Fora do escopo	
Premissas	
Restrições	
Dependências	
Roadmap inicial	

Governança

Campo	Preenchimento / evidência
Gestor do Negócio	
Responsável pelo backlog	
Responsável técnico	
Unidades participantes	
Indicadores de sucesso	
Riscos estratégicos	

ANEXO G - Registro de priorização

Controle do instrumento	Preenchimento
Código e versão	PDS-G | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Item

Campo	Preenchimento / evidência
ID	
Descrição resumida	
Tipo	
Área	
Criticidade	
Esforço ou tamanho	
Dependências	

Critério	Avaliação	Justificativa
Obrigação legal		
Impacto ambiental		
Impacto no cidadão		
Valor público		
Urgência		
Risco		
Redução de dívida técnica		
Custo do atraso		
Capacidade disponível		

Critério	Avaliação	Justificativa
Disponibilidade contratual		

Decisão

Campo	Preenchimento / evidência
Método utilizado: MoSCoW / WSJF / outro	
Posição ou classe de prioridade	
Autoridade responsável	
Data	
Condições e observações	

ANEXO H - História de usuário e critérios de aceite

Controle do instrumento	Preenchimento
Código e versão	PDS-H | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Identificação

Campo	Preenchimento / evidência
ID da história	
Épico ou capacidade	
Prioridade	
Gestor do Negócio	
Responsável pelo refinamento	

Como [perfil], quero [capacidade], para [benefício].

Detalhamento

Campo	Preenchimento / evidência
Contexto	
Regras de negócio	
Dados envolvidos	
Requisitos não funcionais	
Dependências	
Riscos	
Protótipo ou modelo relacionado	

Cenário	Dado que (Given)	Quando (When)	Então (Then)
1			
2			
3			

Definition of Ready

Item de verificação	Sim	Não	N/A	Evidência / observação
Valor e perfil estão claros.	☐	☐	☐	
Critérios de aceite são verificáveis.	☐	☐	☐	
Dependências relevantes foram tratadas.	☐	☐	☐	
Dados e regras de negócio estão definidos.	☐	☐	☐	
Requisitos de segurança e privacidade foram avaliados.	☐	☐	☐	
O item pode ser estimado e testado.	☐	☐	☐	

ANEXO I - Especificação de requisito

Controle do instrumento	Preenchimento
Código e versão	PDS-I | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Identificação

Campo	Preenchimento / evidência
ID	
Tipo: funcional / não funcional / regra / integração / dados	
Origem	
Prioridade	
Responsável	

Especificação

Campo	Preenchimento / evidência
Descrição	
Justificativa	
Pré-condições	
Entradas	
Processamento ou regra	
Saídas	
Exceções	
Critérios de verificação	

Campo	Preenchimento / evidência
Rastreabilidade	
Restrições	

ANEXO J - Checklist da Definition of Ready

Controle do instrumento	Preenchimento
Código e versão	PDS-J | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Prontidão do item

Item de verificação	Sim	Não	N/A	Evidência / observação
Problema, usuário e benefício estão claros.	☐	☐	☐	
Escopo e limites estão compreendidos.	☐	☐	☐	
Critérios de aceite estão objetivos e testáveis.	☐	☐	☐	
Regras de negócio foram validadas.	☐	☐	☐	
Dependências foram identificadas.	☐	☐	☐	
Dados e integrações foram avaliados.	☐	☐	☐	
Arquitetura e requisitos não funcionais foram tratados quando aplicável.	☐	☐	☐	
Segurança, privacidade e acessibilidade foram consideradas.	☐	☐	☐	
Riscos relevantes estão registrados.	☐	☐	☐	
O item foi estimado ou possui informação suficiente para planejamento.	☐	☐	☐	
Responsáveis e homologadores foram definidos.	☐	☐	☐	
Não há impedimento conhecido que inviabilize o início.	☐	☐	☐	

ANEXO K - Plano de ciclo de execução

Controle do instrumento	Preenchimento
Código e versão	PDS-K | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Ciclo

Campo	Preenchimento / evidência
Projeto ou produto	
Período	
Objetivo do ciclo	
Método de trabalho	
Capacidade planejada	
Equipe e participantes	

Item	Objet.	Resp.	Estim.	Depend.	Critério final

Controle

Campo	Preenchimento / evidência
Riscos e impedimentos	
Marcos	

Campo	Preenchimento / evidência
Reuniões e cadência	
Critérios de encerramento	
Observações	

ANEXO L - Ordem de Serviço e plano de execução

> ***NOTA DE APLICAÇÃO:*** *Checklist operacional complementar ao instrumento contratual oficial.*

Controle do instrumento	Preenchimento
Código e versão	PDS-L | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Referências

Campo	Preenchimento / evidência
Contrato	
Processo administrativo	
Número da OS	
Demanda ou projeto	
Fornecedor	
Preposto	
Fiscais e gestor do contrato	

Objeto e produtos

Campo	Preenchimento / evidência
Objeto	
Produtos ou resultados	
Escopo	
Fora do escopo	
Prazo	

Campo	Preenchimento / evidência
Estimativa e unidade contratual	
Critérios de aceite	
SLA aplicáveis	
Documentação e evidências	
Segurança e proteção de dados	
Transferência de conhecimento	

Autorizações

Campo	Preenchimento / evidência
Responsável pela elaboração	
Fiscal técnico	
Fiscal requisitante	
Gestor do contrato	
Data de autorização	

ANEXO M - Relatório de acompanhamento da fábrica

Controle do instrumento	Preenchimento
Código e versão	PDS-M | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Período

Campo	Preenchimento / evidência
Contrato e OS	
Período de referência	
Preposto	
Fiscal técnico	
Gestor do produto	

Dimensão	Planejado	Realizado	Desvio	Ação
Entregas				
Prazo				
Consumo				
Qualidade				
Testes				
Documentação				
Segurança				
Transferência de conhecimento				

Síntese

Campo	Preenchimento / evidência
Riscos	

Campo	Preenchimento / evidência
Impedimentos	
Defeitos e retrabalho	
Pendências	
Decisões	
Recomendação	

ANEXO N - Estratégia ou plano de testes

Controle do instrumento	Preenchimento
Código e versão	PDS-N | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Planejamento

Campo	Preenchimento / evidência
Produto e versão	
Responsável	
Escopo de teste	
Fora do escopo	
Ambientes	
Dados de teste	
Ferramentas	
Cronograma	

Nível ou tipo	Aplic.	Resp.	Autom.	Critério de saída
Unitário	☐			
Componente	☐			
Integração	☐			
Contrato/API	☐			
Sistema/funcional	☐			
Aceitação/homologação	☐			
Regressão	☐			
Smoke	☐			
Exploratório	☐			

Nível ou tipo	Aplic.	Resp.	Autom.	Critério de saída
Usabilidade	☐			
Acessibilidade	☐			
Desempenho	☐			
Segurança	☐			
Compatibilidade	☐			
Migração	☐			
Resiliência e recuperação	☐			

Controle

Campo	Preenchimento / evidência
Critérios de entrada	
Critérios de saída	
Riscos de teste	
Cobertura esperada	
Tratamento de defeitos	
Evidências	
Risco residual	

ANEXO O - Caso e roteiro de teste

Controle do instrumento	Preenchimento
Código e versão	PDS-O | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Identificação

Campo	Preenchimento / evidência
ID do teste	
Requisito ou história	
Objetivo	
Tipo	
Prioridade	
Responsável	

Preparação

Campo	Preenchimento / evidência
Pré-condições	
Dados	
Ambiente	
Dependências	

Passo	Ação	Resultado esperado	Resultado obtido	Evidência
1				
2				
3				

Passo	Ação	Resultado esperado	Resultado obtido	Evidência
4				
5				
6				
7				

Resultado

Campo	Preenchimento / evidência
Status: aprovado / reprovado / bloqueado	
Defeito associado	
Data	
Observações	

ANEXO P - Relatório de execução de testes

Controle do instrumento	Preenchimento
Código e versão	PDS-P | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Identificação

Campo	Preenchimento / evidência
Produto e versão	
Período	
Ambiente	
Responsável	
Plano de testes	

Indicador	Resultado	Observação
Casos previstos		
Executados		
Aprovados		
Reprovados		
Bloqueados		
Cobertura de requisitos		
Cobertura unitária, quando aplicável		
Defeitos críticos/altos		
Defeitos abertos		
Testes instáveis		

Conclusão

Campo	Preenchimento / evidência
Riscos e limitações	
Pendências	
Risco residual	
Recomendação: apto / condicionado / não apto	
Responsável e data	

ANEXO Q - Roteiro de homologação

Controle do instrumento	Preenchimento
Código e versão	PDS-Q | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Planejamento

Campo	Preenchimento / evidência
Produto e versão	
Área homologadora	
Responsável pela homologação	
Ambiente	
Período	
Dados de homologação	

Cenário	Critério de aceite	Resultado	Evidência	Pend.

Encerramento

Campo	Preenchimento / evidência
Conclusão	
Itens não homologados	
Ressalvas	
Prazo para correção	
Responsável	

ANEXO R - Termo de homologação funcional

Controle do instrumento	Preenchimento
Código e versão	PDS-R | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Identificação

Campo	Preenchimento / evidência
Demanda ou projeto	
Produto	
Versão	
Área demandante	
Gestor do Negócio	
Período de homologação	

Resultado

Item de verificação	Sim	Não	N/A	Evidência / observação
Aprovação integral.	☐	☐	☐	
Aprovação parcial.	☐	☐	☐	
Aprovação com ressalvas.	☐	☐	☐	
Reprovação.	☐	☐	☐	

Manifestação

Campo	Preenchimento / evidência
Escopo homologado	

Campo	Preenchimento / evidência
Cenários executados	
Pendências e ressalvas	
Impacto das pendências	
Prazo acordado	
Evidências	
Responsável e data	

> ***NOTA DE APLICAÇÃO***
> *A homologação funcional não substitui validação técnica, aceite de risco, recebimento contratual ou autorização de implantação.*

ANEXO S - Parecer de validação técnica

Controle do instrumento	Preenchimento
Código e versão	PDS-S | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Identificação

Campo	Preenchimento / evidência
Produto e versão	
Responsável técnico	
Demanda ou OS	
Data	

Verificações

Item de verificação	Sim	Não	N/A	Evidência / observação
Arquitetura e padrões atendidos.	☐	☐	☐	
Revisão de código concluída.	☐	☐	☐	
Testes unitários e de integração executados.	☐	☐	☐	
Testes funcionais e regressão concluídos.	☐	☐	☐	
Controles de segurança executados.	☐	☐	☐	
Vulnerabilidades tratadas ou formalmente aceitas.	☐	☐	☐	
Documentação atualizada.	☐	☐	☐	
Rastreabilidade completa.	☐	☐	☐	
Plano de implantação e rollback disponíveis.	☐	☐	☐	
Observabilidade e suporte preparados.	☐	☐	☐	

Parecer

Campo	Preenchimento / evidência
Riscos e exceções	
Pendências	
Risco residual	
Conclusão: apto / condicionado / não apto	
Responsável e aprovação	

ANEXO T - Checklist da Definition of Done

Controle do instrumento	Preenchimento
Código e versão	PDS-T | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Condições de conclusão

Item de verificação	Sim	Não	N/A	Evidência / observação
Código implementado e versionado.	☐	☐	☐	
Merge request revisada e aprovada.	☐	☐	☐	
Testes unitários criados e executados.	☐	☐	☐	
Testes de integração e funcionais concluídos.	☐	☐	☐	
Critérios de aceite atendidos.	☐	☐	☐	
Regressão executada conforme risco.	☐	☐	☐	
SAST, SCA, secrets e demais verificações aplicáveis concluídas.	☐	☐	☐	
Documentação técnica e funcional atualizada.	☐	☐	☐	
Evidências anexadas.	☐	☐	☐	
Rastreabilidade demanda-requisito-código-teste-versão mantida.	☐	☐	☐	
Débitos técnicos e limitações registrados.	☐	☐	☐	
Homologação realizada quando aplicável.	☐	☐	☐	
Pacote e versão identificados.	☐	☐	☐	
Prontidão operacional confirmada.	☐	☐	☐	

ANEXO U - Termo de aceite funcional

Controle do instrumento	Preenchimento
Código e versão	PDS-U | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Identificação

Campo	Preenchimento / evidência
Demanda	
Produto e versão	
Área responsável	
Gestor do Negócio	
Critérios de aceite de referência	

Manifestação

Campo	Preenchimento / evidência
Escopo aceito	
Evidências	
Ressalvas	
Pendências não impeditivas	
Conclusão	
Responsável e data	

> ***NOTA DE APLICAÇÃO***
> *O aceite funcional não autoriza, por si só, pagamento ou recebimento contratual definitivo.*

ANEXO V - Termo de recebimento provisório

Controle do instrumento	Preenchimento
Código e versão	PDS-V | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Referências

Campo	Preenchimento / evidência
Contrato	
OS	
Processo administrativo	
Fornecedor	
Produto	
Fiscal responsável	

Verificações iniciais

Item de verificação	Sim	Não	N/A	Evidência / observação
Produto foi entregue no prazo ou desvio foi registrado.	☐	☐	☐	
Evidências mínimas foram apresentadas.	☐	☐	☐	
Documentação foi recebida.	☐	☐	☐	
Versão e artefatos estão identificados.	☐	☐	☐	
Pendências para verificação definitiva foram registradas.	☐	☐	☐	

Manifestação

Campo	Preenchimento / evidência
Data do recebimento provisório	
Pendências	
Prazo para verificação/correção	
Responsável	
Assinaturas ou aceite eletrônico	

ANEXO W - Termo de recebimento definitivo

Controle do instrumento	Preenchimento
Código e versão	PDS-W | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Referências

Campo	Preenchimento / evidência
Contrato	
OS	
Recebimento provisório	
Produto e versão	
Fornecedor	

Condições

Item de verificação	Sim	Não	N/A	Evidência / observação
Correções e pendências foram tratadas.	☐	☐	☐	
Homologação e aceite aplicáveis foram concluídos.	☐	☐	☐	
Validação técnica foi concluída.	☐	☐	☐	
Documentação e transferência de conhecimento foram entregues.	☐	☐	☐	
Obrigações de segurança e proteção de dados foram verificadas.	☐	☐	☐	
Critérios contratuais foram atendidos.	☐	☐	☐	
Glosas e não conformidades foram registradas.	☐	☐	☐	

Manifestação

Campo	Preenchimento / evidência
Resultado	
Ressalvas	
Valor ou medição relacionada	
Responsáveis e data	

ANEXO X - Checklist para autorização de medição ou faturamento

Controle do instrumento	Preenchimento
Código e versão	PDS-X | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Conferência

Item de verificação	Sim	Não	N/A	Evidência / observação
OS válida e autorizada.	☐	☐	☐	
Produto previsto foi entregue.	☐	☐	☐	
Evidências são suficientes e rastreáveis.	☐	☐	☐	
Homologação e aceite aplicáveis estão registrados.	☐	☐	☐	
Recebimento provisório/definitivo está compatível com o contrato.	☐	☐	☐	
SLA e prazos foram verificados.	☐	☐	☐	
Defeitos, retrabalho e não conformidades foram considerados.	☐	☐	☐	
Glosas foram calculadas e justificadas.	☐	☐	☐	
Documentação foi entregue.	☐	☐	☐	
Saldo contratual e valores foram conferidos.	☐	☐	☐	
Autoridades competentes manifestaram-se.	☐	☐	☐	

Decisão

Campo	Preenchimento / evidência
Medição autorizada	

Campo	Preenchimento / evidência
Valor bruto	
Glosas	
Valor líquido	
Justificativa	
Responsáveis e data	

ANEXO Y - Plano de implantação

Controle do instrumento	Preenchimento
Código e versão	PDS-Y | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Identificação

Campo	Preenchimento / evidência
Produto e versão	
Ambiente	
Janela	
Responsável pela implantação	
Responsável pelo negócio	
Mudança relacionada	

Preparação

Campo	Preenchimento / evidência
Escopo	
Dependências	
Backup	
Migração	
Configurações	
Comunicação	
Validação pós-implantação	
Monitoramento reforçado	

Etapa	Resp.	Início	Fim	Evidência

Decisão

Campo	Preenchimento / evidência
Critérios go/no-go	
Riscos	
Plano de rollback	
Aprovações	

ANEXO Z - Plano de rollback

Controle do instrumento	Preenchimento
Código e versão	PDS-Z | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Identificação

Campo	Preenchimento / evidência
Implantação relacionada	
Produto e versão	
Estado anterior	
Responsável	

Acionamento

Campo	Preenchimento / evidência
Gatilhos	
Autoridade para decidir	
Prazo máximo	
Impacto esperado	

Passo	Ação	Responsável	Validação
1			
2			
3			
4			

Passo	Ação	Responsável	Validação
5			
6			
7			

Recuperação

Campo	Preenchimento / evidência
Dados e restauração	
Comunicação	
Validação funcional	
Validação técnica	
Encerramento	

ANEXO AA - Checklist de prontidão para produção

Controle do instrumento	Preenchimento
Código e versão	PDS-AA | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Prontidão

Item de verificação	Sim	Não	N/A	Evidência / observação
Homologação funcional concluída.	☐	☐	☐	
Validação técnica concluída.	☐	☐	☐	
Testes e regressão atendem aos critérios de saída.	☐	☐	☐	
Vulnerabilidades impeditivas foram tratadas.	☐	☐	☐	
Risco residual foi avaliado e aceito quando necessário.	☐	☐	☐	
Plano de implantação e rollback estão aprovados.	☐	☐	☐	
Backup e restauração foram considerados.	☐	☐	☐	
Configuração e segredos estão corretos.	☐	☐	☐	
Monitoramento, logs e alertas estão disponíveis.	☐	☐	☐	
Capacidade e desempenho foram avaliados.	☐	☐	☐	
Suporte e responsáveis estão informados.	☐	☐	☐	
Documentação e base de conhecimento foram atualizadas.	☐	☐	☐	
Comunicação aos usuários foi preparada.	☐	☐	☐	

ANEXO AB - Registro de incidente

Controle do instrumento	Preenchimento
Código e versão	PDS-AB | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Identificação

Campo	Preenchimento / evidência
ID	
Serviço ou sistema	
Data e hora	
Detectado por	
Canal	
Severidade	

Descrição

Campo	Preenchimento / evidência
Sintomas	
Impacto	
Usuários afetados	
Escopo	
Linha do tempo	
Ações de contenção	
Serviço restaurado em	
Evidências	

Encaminhamento

Campo	Preenchimento / evidência
Responsável	
Escalonamento	
Problema relacionado	
Mudança relacionada	
Comunicação	
Situação final	

ANEXO AC - Relatório de problema e causa raiz

Controle do instrumento	Preenchimento
Código e versão	PDS-AC | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Identificação

Campo	Preenchimento / evidência
Problema	
Incidentes relacionados	
Responsável	
Data	

Análise

Campo	Preenchimento / evidência
Descrição	
Linha do tempo	
Causa imediata	
Causa raiz	
Fatores contribuintes	
Método: 5 porquês / Ishikawa / outro	
Impacto	

Ação	Tipo: corretiva/preventiva	Responsável	Prazo	Evidência

Ação	Tipo: corretiva/preventiva	Responsável	Prazo	Evidência

Conclusão

Campo	Preenchimento / evidência
Risco residual	
Lição aprendida	
Critério de encerramento	
Aprovação	

ANEXO AD - Registro de mudança e hotfix

Controle do instrumento	Preenchimento
Código e versão	PDS-AD | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Identificação

Campo	Preenchimento / evidência
ID	
Tipo: padrão / normal / emergencial	
Sistema	
Versão	
Solicitante	
Responsável	

Avaliação

Campo	Preenchimento / evidência
Descrição	
Justificativa	
Impacto	
Risco	
Dependências	
Janela	
Teste	
Backup	

Campo	Preenchimento / evidência
Rollback	
Comunicação	

Decisão e execução

Campo	Preenchimento / evidência
Aprovadores	
Resultado	
Incidentes relacionados	
Regularização pós-hotfix	
Evidências	
Encerramento	

ANEXO AE - Plano de sustentação

Controle do instrumento	Preenchimento
Código e versão	PDS-AE | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Escopo

Campo	Preenchimento / evidência
Produto	
Versão	
Serviços abrangidos	
Horário de suporte	
Usuários	
Criticidade	

Operação

Campo	Preenchimento / evidência
Níveis N1/N2/N3/N4	
Canais	
SLA	
Escalonamento	
Monitoramento	
Alertas	
Backup e recuperação	
Manutenção preventiva	

Campo	Preenchimento / evidência
Gestão de acessos	
Base de conhecimento	

Governança

Campo	Preenchimento / evidência
Responsáveis	
Fábrica ou fornecedor	
Riscos	
Indicadores	
Revisões	
Plano de continuidade	

ANEXO AF - Checklist de segurança e privacidade

Controle do instrumento	Preenchimento
Código e versão	PDS-AF | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Controles

Item de verificação	Sim	Não	N/A	Evidência / observação
Classificação de criticidade realizada.	☐	☐	☐	
Requisitos de segurança e privacidade definidos.	☐	☐	☐	
Modelagem de ameaças realizada quando aplicável.	☐	☐	☐	
Autenticação, autorização e menor privilégio verificados.	☐	☐	☐	
Criptografia e gestão de segredos tratadas.	☐	☐	☐	
Logs não expõem dados ou credenciais indevidos.	☐	☐	☐	
SAST, SCA, DAST e scans aplicáveis executados.	☐	☐	☐	
Dependências e imagens avaliadas.	☐	☐	☐	
Dados pessoais, finalidade e base legal identificados.	☐	☐	☐	
Retenção e descarte definidos.	☐	☐	☐	
Direitos dos titulares considerados.	☐	☐	☐	
RIPD avaliado conforme risco.	☐	☐	☐	
Incidentes e contatos definidos.	☐	☐	☐	
Exceções e riscos residuais formalizados.	☐	☐	☐	

Manifestações

Campo	Preenchimento / evidência
Responsável técnico	
Responsável pelo negócio	
Segurança/privacidade, quando aplicável	
Pendências	
Risco residual	
Conclusão	

ANEXO AG - Registro de vulnerabilidade

Controle do instrumento	Preenchimento
Código e versão	PDS-AG | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Identificação

Campo	Preenchimento / evidência
ID	
Ativo	
Origem	
Data	
CVE/CWE, quando aplicável	
Descrição	

Classificação

Campo	Preenchimento / evidência
Severidade técnica	
Exposição	
Exploração ativa	
Impacto	
Criticidade do ativo	
Prioridade	

Tratamento

Campo	Preenchimento / evidência
Responsável	
Correção ou mitigação	
Prazo	
Controle compensatório	
Reteste	
Exceção	
Risco residual	
Encerramento	

ANEXO AH - Registro de risco

Controle do instrumento	Preenchimento
Código e versão	PDS-AH | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Identificação

Campo	Preenchimento / evidência
ID	
Iniciativa ou produto	
Categoria	
Proprietário do risco	
Responsável pela ação	

Descrição

Campo	Preenchimento / evidência
Causa	
Evento incerto	
Consequência	
Probabilidade	
Impacto	
Urgência/proximidade	
Risco inerente	

Resposta

Campo	Preenchimento / evidência
Estratégia	
Ações preventivas	
Gatilho	
Contingência	
Prazo	
Risco residual	
Autoridade de aceite	
Data de revisão	

ANEXO AI - Solicitação e aprovação de exceção

Controle do instrumento	Preenchimento
Código e versão	PDS-AI | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Solicitação

Campo	Preenchimento / evidência
Objeto da exceção	
Regra ou controle afetado	
Escopo	
Justificativa	
Prazo solicitado	
Responsável	

Avaliação

Campo	Preenchimento / evidência
Risco	
Impacto	
Alternativas	
Controle compensatório	
Plano de regularização	
Risco residual	

Decisão

Campo	Preenchimento / evidência
Autoridade competente	
Resultado	
Condições	
Data de expiração	
Data de revisão	
Evidências	

ANEXO AJ - Triagem de proteção de dados e necessidade de RIPD

Controle do instrumento	Preenchimento
Código e versão	PDS-AJ | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Triagem

Item de verificação	Sim	Não	N/A	Evidência / observação
A solução trata dados pessoais.	☐	☐	☐	
Trata dados pessoais sensíveis.	☐	☐	☐	
Abrange crianças, adolescentes ou grupos vulneráveis.	☐	☐	☐	
Opera em larga escala.	☐	☐	☐	
Realiza monitoramento sistemático.	☐	☐	☐	
Cruza bases ou enriquece perfis.	☐	☐	☐	
Utiliza tecnologia emergente ou inovadora.	☐	☐	☐	
Produz decisão automatizada com impacto relevante.	☐	☐	☐	
Compartilha dados com terceiros ou outros órgãos.	☐	☐	☐	
Realiza transferência internacional.	☐	☐	☐	
Pode produzir alto risco aos direitos e liberdades.	☐	☐	☐	
Há solicitação da autoridade ou orientação institucional para RIPD.	☐	☐	☐	

Conclusão

Campo	Preenchimento / evidência
Finalidades	
Categorias de dados e titulares	
Base legal preliminar	
Controlador e operadores	
Medidas existentes	
Riscos identificados	
RIPD: necessário / não necessário / reavaliar	
Justificativa	
Consulta ao encarregado e áreas competentes	

ANEXO AK - Registro interno de incidente com dados pessoais

Controle do instrumento	Preenchimento
Código e versão	PDS-AK | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Identificação

Campo	Preenchimento / evidência
ID	
Data e hora	
Sistema	
Unidade	
Responsável pelo registro	

Incidente

Campo	Preenchimento / evidência
Descrição	
Categorias de dados	
Titulares afetados	
Quantidade estimada	
Confidencialidade/integridade/disponibilidade	
Causa conhecida	
Medidas de contenção	
Evidências preservadas	

Avaliação

Campo	Preenchimento / evidência
Probabilidade de risco ou dano relevante	
Natureza e gravidade	
Possíveis consequências	
Medidas de mitigação	
Recomendação de comunicação	
Decisão do controlador	
Comunicação aos titulares	
Comunicação à ANPD	
Atualizações e encerramento	

> ***NOTA DE APLICAÇÃO:*** *A avaliação e a comunicação devem observar a LGPD, a Resolução CD/ANPD nº 15/2024 e os canais oficiais vigentes.*

ANEXO AL - Referência para comunicação à ANPD

> ***NOTA DE APLICAÇÃO:*** *Instrumento dinâmico. Utilizar o formulário e o canal oficial vigentes da ANPD, evitando cópias desatualizadas.*

Controle do instrumento	Preenchimento
Código e versão	PDS-AL | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Verificação	Registro
Critérios de comunicação avaliados	
Decisão do controlador	
Data de ciência do incidente	
Data da comunicação	
Protocolo oficial	
Comunicação preliminar ou completa	
Informações complementares pendentes	
Comunicação aos titulares	
Responsável pelo acompanhamento	

> ***NOTA DE APLICAÇÃO:*** *Referência normativa: Lei nº 13.709/2018 e Resolução CD/ANPD nº 15/2024, além de orientações oficiais posteriores vigentes.*

ANEXO AM - Solicitação de exercício de direitos do titular

Controle do instrumento	Preenchimento
Código e versão	PDS-AM | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Identificação segura

Campo	Preenchimento / evidência
Nome do titular ou representante	
Canal de contato	
Relação com a SEMA/MT	
Representação ou procuração, quando aplicável	
Forma proporcional de confirmação de identidade	

Direito solicitado

Item de verificação	Sim	Não	N/A	Evidência / observação
Confirmação da existência de tratamento.	☐	☐	☐	
Acesso aos dados.	☐	☐	☐	
Correção de dados incompletos, inexatos ou desatualizados.	☐	☐	☐	
Informações sobre compartilhamento.	☐	☐	☐	
Anonimização, bloqueio ou eliminação, quando juridicamente cabível.	☐	☐	☐	
Portabilidade, quando regulamentada e aplicável.	☐	☐	☐	

Item de verificação	Sim	Não	N/A	Evidência / observação
Revogação de consentimento, quando esta for a base legal.	☐	☐	☐	
Oposição ao tratamento, nas hipóteses legais.	☐	☐	☐	
Revisão ou informações sobre decisão automatizada, quando aplicável.	☐	☐	☐	
Outro direito previsto em lei.	☐	☐	☐	

Descrição e tramitação

Campo	Preenchimento / evidência
Descrição da solicitação	
Sistemas ou serviços relacionados	
Documentos estritamente necessários	
Data do recebimento	
Unidade responsável	
Resposta simplificada imediata ou declaração completa, quando aplicável	
Fundamentação para eventual limitação	
Data e canal da resposta	

> ***NOTA DE APLICAÇÃO:*** *A coleta de documentos deve ser proporcional e segura. A eliminação ou entrega de dados pode ser limitada por obrigação legal, interesse público, segurança, direitos de terceiros ou outras hipóteses legais.*

ANEXO AN - Termo de consentimento, quando aplicável

> ***NOTA DE APLICAÇÃO:*** *Usar somente após confirmação de que o consentimento é a base legal adequada, livre e revogável para a finalidade específica.*

Controle do instrumento	Preenchimento
Código e versão	PDS-AN | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Controlador e titular

Campo	Preenchimento / evidência
Controlador	
Canal do encarregado	
Titular	
Representante, quando aplicável	

Tratamento

Campo	Preenchimento / evidência
Finalidade específica	
Dados abrangidos	
Operações	
Compartilhamentos	
Prazo ou critério de retenção	
Consequências reais da recusa	
Forma de revogação	

Manifestação

Item de verificação	Sim	Não	N/A	Evidência / observação
Autorizo a finalidade 1: _____.	☐	☐	☐	
Autorizo a finalidade 2: _____.	☐	☐	☐	
Não autorizo finalidades opcionais não essenciais.	☐	☐	☐	

Registro

Campo	Preenchimento / evidência
Linguagem e versão apresentadas	
Data e hora	
Canal	
Manifestação inequívoca	
Responsável pelo registro	

> ***NOTA DE APLICAÇÃO:*** *O consentimento não deve ser utilizado para substituir base legal mais adequada nem condicionar indevidamente serviço público obrigatório.*

ANEXO AO - Ficha de indicador

Controle do instrumento	Preenchimento
Código e versão	PDS-AO | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Identificação

Campo	Preenchimento / evidência
Código	
Nome	
Objetivo	
Pergunta de gestão	
Dimensão	
Responsável	

Especificação

Campo	Preenchimento / evidência
Definição	_____
Fórmula	_____
Unidade	_____
Fonte	_____
Filtros e segmentações	_____
Periodicidade	_____
Linha de base	_____
Meta ou faixa	_____

Campo	Preenchimento / evidência
Interpretação	_____
Limitações	_____
Ação esperada	_____
Qualidade do dado	_____
Data de revisão	_____

ANEXO AP - Plano de capacitação

Controle do instrumento	Preenchimento
Código e versão	PDS-AP | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Planejamento

Campo	Preenchimento / evidência
Período	
Responsável	
Objetivos	
Públicos	
Lacunas priorizadas	
Recursos	

Trilha/ação	Público	Conteúdo	Modalidade	Resp.	Data	Avaliação

Avaliação

Campo	Preenchimento / evidência
Indicadores	
Aplicação prática esperada	
Materiais a atualizar	
Ações extraordinárias	

ANEXO AQ - Registro de transferência de conhecimento

Controle do instrumento	Preenchimento
Código e versão	PDS-AQ | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Identificação

Campo	Preenchimento / evidência
Origem do conhecimento	
Destinatários	
Produto ou tecnologia	
Período	
Responsável	

Tema	Atividade	Evidência	Participantes	Pendência

Conclusão

Campo	Preenchimento / evidência
Competências transferidas	

Campo	Preenchimento / evidência
Materiais entregues	
Acesso e repositório	
Riscos de dependência remanescentes	
Aceite	

ANEXO AR - Registro de lições aprendidas

Controle do instrumento	Preenchimento
Código e versão	PDS-AR | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Contexto

Campo	Preenchimento / evidência
Iniciativa	
Fase	
Evento	
Participantes	
Data	

O que ocorreu	Causa ou contexto	Impacto	Recomendação	Destino da ação

Incorporação

Campo	Preenchimento / evidência
Ação no backlog	
Atualização de processo	

Campo	Preenchimento / evidência
Atualização de material	
Responsável	
Prazo	

ANEXO AS - Checklist de encerramento

Controle do instrumento	Preenchimento
Código e versão	PDS-AS | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Encerramento

Item de verificação	Sim	Não	N/A	Evidência / observação
Produtos e versões estão identificados.	☐	☐	☐	
Homologação, aceite e recebimentos foram concluídos ou pendências formalizadas.	☐	☐	☐	
Documentação foi atualizada e armazenada.	☐	☐	☐	
Riscos foram encerrados, transferidos ou aceitos.	☐	☐	☐	
Débitos técnicos e backlog residual foram registrados.	☐	☐	☐	
Acessos temporários foram revogados.	☐	☐	☐	
Ativos, licenças e credenciais foram tratados.	☐	☐	☐	
Transferência de conhecimento foi concluída.	☐	☐	☐	
Plano de sustentação está ativo.	☐	☐	☐	
Contratos e OS foram encerrados conforme regras aplicáveis.	☐	☐	☐	
Indicadores e benefícios foram avaliados.	☐	☐	☐	
Lições aprendidas foram registradas.	☐	☐	☐	
Registros e evidências foram arquivados.	☐	☐	☐	

Manifestação

Campo	Preenchimento / evidência
Pendências	
Responsáveis	
Prazo	
Conclusão	
Aprovação	

ANEXO AT - Matriz RACI de referência

> ***NOTA DE APLICAÇÃO:*** *A matriz deve ser adaptada à iniciativa e não substitui competências legais, regimentais ou contratuais.*

Controle do instrumento	Preenchimento
Código e versão	PDS-AT | Versão: ____
Responsável pelo modelo	_____
Data de atualização	____/____/_____
Repositório oficial	_____

Atividade	Área demandante / Gestor do Negócio	CSTI	CPQSI	CITI	Fábrica	Fiscalização / Gestão contratual	Instância decisória
Registrar e justificar demanda	R	C	I	I	I	I	A
Qualificar e analisar demanda	C	R	C	C	I	I	A
Definir e validar requisitos	A/R	R	C	C	C	I	I
Priorizar portfólio	C	C	C	I	I	I	A/R
Definir arquitetura	C	A/R	C	C	C	I	I
Desenvolver e testar	C	A	C	C	R	I	I
Validar tecnicamente	C	A/R	C	C	C	I	I
Homologar funcionalmente	A/R	C	I	I	C	I	I
Aceitar risco institucional	C	C	C	C	I	I	A/R
Autorizar implantação	C	R	C	R	C	I	A
Receber entrega contratual	C	C	I	I	I	A/R	I

Atividade	Área demandante / Gestor do Negócio	CSTI	CPQSI	CITI	Fábrica	Fiscalização / Gestão contratual	Instância decisória
Sustentar e operar	C	R	C	R	C	I	I

> ***NOTA DE APLICAÇÃO:*** *Legenda: R = Responsável pela execução; A = Autoridade final; C = Consultado; I = Informado. A combinação A/R é admitida quando a mesma unidade possui competência e executa a atividade.*

Modelos externos e instrumentos complementares

> ***NOTA DE APLICAÇÃO:*** *Cartilha Operacional do PDS: instrumento digital, responsivo e interativo destinado à consulta rápida, treinamento e apoio à execução. A cartilha complementa este documento e não o substitui; em caso de divergência, prevalecem o PDS, os normativos, os instrumentos contratuais e os registros oficiais.*

Quando houver modelo oficial mais específico, este deverá ser utilizado. Os anexos do PDS poderão ser convertidos em formulários eletrônicos, templates do Redmine, conteúdo controlado no GovFlow, documentos editáveis ou registros em sistemas administrativos, preservando os campos mínimos, a rastreabilidade e as autoridades definidas.

Referências de proteção de dados utilizadas na revisão dos anexos: Lei nº 13.709/2018; Resolução CD/ANPD nº 15/2024; regulamentação vigente sobre a atuação do encarregado; orientações oficiais da ANPD sobre direitos dos titulares, incidentes e RIPD.

_____	_____	_____
ASSINATURA	ASSINATURA	ASSINATURA
DATA: 02 de ago. de 2026	DATA: 02 de ago. de 2026	DATA: 02 de ago. de 2026
Nome: Carlos Gracioli Neto	Nome: Dirlene Ramalho da Silva	Nome: Rafael Bezerra Scarselli
Telefone: 66 99925-0185	Telefone: 65 9622-8543	Telefone: 65 9607-7042