Diário Oficial do Estado de Rondônia nº 72
Disponibilização: 15/04/2026
Publicação: 15/04/2026

RONDÔNIA
Governo do Estado

GOVERNO DO ESTADO DE RONDÔNIA

Superintendência Estadual de Tecnologia da Informação e Comunicação - SETIC

Instrução Normativa nº 5/2026/SETIC-ASGAB

Dispõe sobre a institucionalização da abordagem orientada por dados (data-driven) no âmbito da Superintendência Estadual de Tecnologia da Informação e Comunicação – SETIC, estabelecendo diretrizes para o desenvolvimento de soluções inteligentes, a governança de dados e a promoção da gestão estratégica baseada em evidências.

O SUPERINTENDENTE ESTADUAL DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – SETIC, no uso das atribuições que lhe são conferidas pelo art. 114-A, inciso II, da Lei Complementar Estadual nº 965, de 20 de dezembro de 2017, e considerando:

I – a necessidade de aprimorar os processos decisórios por meio do uso sistemático e qualificado de dados e informações;

II – a importância de estabelecer padrões institucionais para a gestão, governança e utilização de dados;

III – a relevância da transformação digital no âmbito da Administração Pública, com foco em eficiência, transparência e inovação;

IV – a necessidade de assegurar conformidade com normas de proteção de dados e segurança da informação;

V – a aprovação na reunião extraordinária do CGGE, realizada em 10 de abril de 2026.

RESOLVE:

Art. 1° Ficam instituídas as diretrizes para a adoção da abordagem orientada por dados (data-driven) no desenvolvimento, manutenção e evolução de soluções tecnológicas no âmbito da SETIC.

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Art. 2º Para os fins desta Instrução Normativa, considera-se:

I – Dado: representação elementar de fatos, observações ou registros, em formato bruto ou processado, passível de armazenamento, tratamento e análise;

II – Ciclo de Vida do Dado: conjunto de fases pelas quais os dados transitam, compreendendo sua criação, coleta, processamento, armazenamento, uso, compartilhamento, arquivamento e descarte;

III – Gestão Orientada por Dados (GDD): modelo de gestão baseado na coleta, análise e utilização estratégica de dados para subsidiar a tomada de decisão;

IV – Metadados: dados estruturados que descrevem características, contexto, conteúdo e estrutura de outros dados;

V – Integridade dos Dados: garantia de exatidão, consistência e confiabilidade dos dados ao longo de seu ciclo de vida;

VI – Interoperabilidade: capacidade de sistemas e organizações de compartilhar e utilizar dados de forma integrada, segura e padronizada;

VII – Soluções Inteligentes: sistemas, aplicações ou ferramentas que utilizam dados, algoritmos e técnicas analíticas para apoiar ou automatizar processos decisórios;

VIII – Administrador do Dado (*Data Steward*): agente responsável pela gestão operacional, qualidade e padronização dos dados;

IX – Dono do Dado (Data Owner): agente responsável pela governança, definição de regras e uso estratégico dos dados;

X – Dono do Produto (*Product Owner*): responsável pela definição, priorização e validação dos requisitos do produto;

XI – Segurança dos Dados (*Data Security*): conjunto de práticas e responsabilidades voltadas à proteção, confidencialidade, integridade e disponibilidade dos dados.

Art. 3º Esta Instrução Normativa estabelece diretrizes para a gestão de dados ao longo de todo o ciclo de vida das soluções tecnológicas, desde sua concepção até sua descontinuação.

Art. 4º A abordagem data-driven constitui princípio estruturante da atuação da SETIC, devendo orientar decisões com base em evidências analíticas, com vistas à mitigação de subjetividades e à ampliação da eficiência

institucional.

CAPÍTULO II

DO ESCOPO DE ATUAÇÃO

Art. 5º A SETIC organiza sua atuação por meio das seguintes unidades:

I – COGE: responsável pela articulação estratégica, definição de diretrizes e alinhamento das iniciativas de dados aos objetivos institucionais;

II – CODE: responsável pelo desenvolvimento, manutenção e evolução de sistemas e soluções tecnológicas;

III – CAGD: responsável pela governança, qualidade, segurança e análise estratégica dos dados institucionais.

Art. 6º As unidades atuarão de forma integrada, assegurando alinhamento entre tecnologia, governança e estratégia institucional.

Parágrafo único. Os gestores de projetos e *Product Owners* atuarão como elo entre as áreas técnicas e os demandantes, assegurando a aderência dos ativos de dados às necessidades institucionais e à governança estabelecida.

CAPÍTULO III

DO CICLO DE VIDA DOS PROJETOS

Art. 7º Os projetos observarão, no mínimo, as seguintes fases:

I - Concepção e idealização: Identificação do problema ou oportunidade, definição dos

dados necessários e validação inicial com stakeholders.

II - Governança e conformidade: Garantia do tratamento dos dados conforme normas e regulamentos.

III - Desenvolvimento do projeto: Construção da solução de forma incremental, podendo incluir, conforme a maturidade e os objetivos do projeto, processos de ETL (extração, transformação e carga), dashboards e modelos analíticos.

IV - Implantação: Disponibilização da solução, ou de suas funcionalidades, para uso operacional, permitindo implantação parcial ou evolutiva, com monitoramento contínuo para ajustes, melhorias e expansão das capacidades analíticas.

V - Geração de insights e tomada de decisão: Transformação dos dados analisados em informações estratégicas para embasar decisões e otimizar processos.

CAPÍTULO IV

DAS DIRETRIZES PARA SOLUÇÕES DATA-DRIVEN

Art. 8º O desenvolvimento de soluções inteligentes orientadas a dados deverá observar as seguintes diretrizes:

I - Planejamento:

a) Levantar de forma inicial e progressiva as necessidades de dados, conforme o ciclo de desenvolvimento de soluções tecnológicas, garantindo que o sistema atenda às demandas estratégicas, permitindo ajustes e evoluções conforme os objetivos e funcionalidades forem implementados; e

b) Estabelecer objetivos específicos para o uso de dados, alinhando-os aos resultados esperados do sistema.

II - Integração:

a) Garantir que o sistema seja integrado de forma eficiente a fontes externas e internas de dados, promovendo a centralização e acessibilidade das informações; e

b) Utilizar tecnologias como APIs e outras ferramentas para facilitar a interoperabilidade entre sistemas, assegurando a troca de dados de maneira fluida e segura, adotando padrões técnicos como APIs abertas e o protocolo RESTful.

III - Avaliação:

a) Acompanhar o desempenho do sistema de forma contínua, com foco na capacidade de gerar insights acionáveis a partir dos dados coletados; e

b) Realizar avaliações periódicas, identificando áreas de melhoria e ajustando o sistema conforme as necessidades do negócio.

IV - Coleta e Armazenamento de Dados:

a) Coletar dados estruturados de maneira segura, acessível e organizada, facilitando sua análise e o processo de tomada de decisões. Adicionalmente, considerar a utilização de Inteligência Artificial (IA) na coleta de dados para análise preditiva, permitindo a identificação de padrões e tendências futuras, contribuindo para decisões mais eficazes e ágeis; e

b) Assegurar a integração com bases de dados já existentes, evitando redundâncias e garantindo a consistência das informações, permitindo uma análise mais eficiente e a correlação entre diferentes fontes de dados.

V - Mensuração e Visibilidade:

a) Buscar assegurar que as funcionalidades e os processos possam ser acompanhados por meio de indicadores de desempenho, métricas e painéis de monitoramento, a serem definidos e utilizados conforme alinhamento e concordância do cliente, de modo a apoiar o acompanhamento de resultados, a avaliação da eficiência, a identificação de desvios e a tomada de decisão; e

b) Prever e prover relatórios, considerando a relevância dos dados desde a concepção até a implementação, em atuação conjunta entre a CAGD, a CODE e o Dono do Dado, cabendo à CAGD a consolidação, análise e governança das informações, especialmente nos relatórios que não envolvam regras de negócio, mediante avaliação e alinhamento prévios; e

c) Evitar a adoção de soluções que não proporcionem visibilidade ou rastreabilidade dos dados, como o armazenamento isolado de documentos sem indicadores, histórico de alterações ou mecanismos de controle, devendo tais soluções, quando inevitáveis, ser avaliadas e autorizadas pelas instâncias de governança e pela alta gestão.

CAPÍTULO V

DAS BOAS PRÁTICAS NO CICLO DE VIDA DOS DADOS

Art. 9º O ciclo de vida dos dados deve ser gerido de acordo com as seguintes fases:

I - Coleta:

a) Definir claramente quais dados serão coletados, assegurando sua relevância e necessidade para os objetivos propostos, por meio da documentação das funcionalidades e requisitos do sistema, tais como Histórias de Usuários, requisitos funcionais e regras de negócio;

b) Assegurar que a coleta de dados respeite as normas de privacidade e proteção de dados pessoais; e

c) Definir os métodos e ferramentas para coleta de dados, considerando a periodicidade (tempo real ou periódica) e os mecanismos de captura, como sistemas transacionais (operações CRUD), integrações via APIs, cargas automatizadas e outros meios adequados.

II - Processamento:

a) Definir como e onde os dados serão processados e armazenados, identificando se são dados estruturados (como bancos de dados e planilhas) ou não estruturados (como documentos, PDFs, imagens, áudios, entre outros). Deverão ser registrados os metadados técnicos, como estrutura, formato, tamanho e restrições, bem como os metadados de negócio, que descrevem o significado, as definições, os conceitos e as regras de negócio associadas aos dados. Para dados não estruturados, devem ser identificadas informações como origem do arquivo, tipo de mídia, autor, tamanho e data de criação. Esse processo deverá ser realizado de forma conjunta entre as áreas técnicas e de negócio, visando à adoção de uma nomenclatura padronizada, clara e compreensível no banco de dados, garantindo melhor entendimento, rastreabilidade e uso adequado das informações; e

b) Implementar as transformações necessárias, executar processos de ETL (Extração, Transformação e Carga) e aplicar ferramentas de NLP (*Natural Language Processing*) para extrair informações de textos e áudios, converter formatos e organizar dados.

III - Armazenamento:

a) Utilizar soluções de armazenamento que garantam a segurança e integridade dos dados; e

b) Manter um inventário atualizado dos dados armazenados, facilitando o acesso e a gestão.

IV - Desativação:

a) Definir critérios claros para a desativação, retenção e exclusão de dados desnecessários ou inativos, observando as regras próprias de cada sistema e as obrigações legais aplicáveis;

b) Garantir que a exclusão ou o tratamento dos dados pessoais e sensíveis esteja em conformidade com a LGPD, respeitando os prazos legais de retenção e adotando métodos seguros, como anonimização, descarte adequado de mídias físicas ou exclusão definitiva de registros digitais, quando permitido; e

c) Implementar auditoria de logs para monitorar acessos e exclusões, registrando quem realizou a ação, quando e por que, garantindo integridade e conformidade com a política de retenção.

CAPÍTULO VI

DAS RESPONSABILIDADES

Art. 10. Compete à Coordenadoria de Análise e Gestão de Dados:

I - Estimular a aplicação dos princípios data-driven no desenvolvimento de soluções inteligentes;

II - Orientar equipes técnicas quanto às boas práticas de coleta, análise e utilização de dados;

III - Acompanhar a aderência dos sistemas às diretrizes estabelecidas neste ato normativo e recomendar ajustes quando necessário;

IV - Promover apoio aos gestores para utilização eficiente dos dados extraídos dos sistemas;

V - Analisar e estruturar os dados de forma alinhada às necessidades identificadas na etapa de tomada de decisão, garantindo que a análise resultante forneça informações relevantes para os objetivos estratégicos do governo;

VI - Na qualidade de Administrador do Dado (*Data Steward*), compete à CAGD:

a) Garantir a qualidade, consistência e confiabilidade dos dados, assegurando conformidade com padrões internos e regulamentares;

b) Definir parâmetros e regras de qualidade e autorizar o acesso às informações sob seu domínio;

c) Implementar e monitorar processos para a padronização, limpeza e validação dos dados;

d) Atuar em parceria com o Dono do Dado (*Data Owner*) para garantir a correta gestão e governança dos dados;

e) Monitorar e relatar inconsistências ou problemas de qualidade nos dados, propondo soluções adequadas;

f) Apoiar na definição e aplicação de políticas de governança de dados, garantindo a integridade e segurança das informações;

g) Responsabilizar-se pelo armazenamento dos dados e pela gestão das bases de dados institucionais, assegurando sua organização, disponibilidade e controle de acesso.

Art. 11. Compete ao Comitê de Gestão de dados e Sistemas de Informações (CGDS):

I - Acompanhar a implementação das diretrizes de governança de dados e realizar ajustes estratégicos conforme necessário;

II - Avaliar e aprovar as mudanças estruturais nos processos de dados, assegurando alinhamento com os objetivos e as prioridades institucionais; e

III - Garantir a adequação às regulamentações e à legislação vigente sobre privacidade e proteção de dados.

Art. 12. Compete ao Dono do Dado (*Data Owner*):

I - Garantir a qualidade e a integridade dos dados sob sua responsabilidade, assegurando que estejam adequadamente coletados, armazenados e utilizados;

II - Definir prioridades e tomar decisões sobre os dados sob sua responsabilidade, além de atuar em conjunto com o Administrador do Dado (*Data Steward*) na definição de diretrizes específicas;

III - Definir as regras de acesso, segurança e compartilhamento dos dados dentro da organização, observando as políticas institucionais, a legislação vigente e as regras próprias de cada sistema, que deverão implementar tais diretrizes por meio de perfis, permissões e controles de acesso;

IV - Promover a educação e a conscientização sobre o uso adequado dos dados entre as equipes envolvidas;

V - Monitorar a utilização dos dados, assegurando que atendam às necessidades de

negócios e às diretrizes estabelecidas; e

VI - Assegurar o controle e a proteção dos dados, garantindo conformidade com normas internas e regulamentações aplicáveis.

Parágrafo único. O papel de Dono do Dado é exercido pelo gestor da área responsável pelo processo de negócio ao qual o dado está vinculado, caracterizado como o cliente demandante do dado ou da informação.

Art. 13. Compete ao responsável pela Segurança de Dados (*Data Security)*:

I - Garantir a proteção e segurança dos dados sensíveis e pessoais tratados pela organização;

II - Conscientizar os colaboradores sobre as melhores práticas de segurança da informação e proteção de dados; e

III - Assegurar a conformidade com a LGPD (Lei Geral de Proteção de Dados Pessoais) e demais normas correlatas.

CAPÍTULO VII

DA PROMOÇÃO DA CULTURA DATA-DRIVEN

Art. 14. Para incentivar a cultura data-driven, serão promovidas ações como:

I - Promover uma cultura de questionamento, estimulando os gestores a refletirem sobre seus processos, formularem as perguntas certas e avaliarem com precisão a eficácia das ações realizadas;

II - Estabelecer parcerias com entidades estudantis para fomentar pesquisas e inovação na gestão de dados; e

III - Realizar *hackathons* e desafios para estimular soluções inovadoras baseadas em dados.

CAPÍTULO VIII

DOS INDICADORES DE DESEMPENHO

Art. 15. A efetividade da implementação da abordagem *data-driven* será mensurada por meio de indicadores como, entre outros:

I - Taxa de aderência das soluções inteligentes ao modelo *data-driven;*

II - Grau de utilização de dados nos processos decisórios;

III - Nível de qualidade, atualidade e integridade dos dados utilizados;

IV - Taxa de reutilização de dados em diferentes projetos ou áreas.

CAPÍTULO IX

DA AUDITORIA E COMPLIANCE

Art. 16. Para garantir a conformidade com esta Instrução Normativa, serão implementadas as seguintes medidas:

I - Emitir relatórios periódicos de conformidade, avaliando a aderência do órgão às diretrizes; e

II - Aplicar sanções administrativas ao descumprimento das diretrizes estabelecidas.

CAPÍTULO X

DAS DISPOSIÇÕES FINAIS

Art. 17. Compete aos gestores e responsáveis pelas áreas envolvidas assegurar o cumprimento das diretrizes estabelecidas, promovendo a cultura de gestão *data-driven* na instituição.

Art. 18. Esta Instrução Normativa entra em vigor na data de sua publicação.

DELNER FREIRE

Superintendente Estadual de Tecnologia da Informação e Comunicação - SETIC

Documento assinado eletronicamente por **DELNER FREIRE**, **Superintendente**, em 15/04/2026, às 11:08, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

A autenticidade deste documento pode ser conferida no site portal do SEI, informando o código verificador **71156654** e o código CRC **1F07A2B6**.

Referência: Caso responda esta Instrução Normativa, indicar expressamente o Processo nº 0070.000843/2025-49 SEI nº 71156654