APROVA Instrução Normativa CGGDIESP-7/PGDI referente ao Anexo II, 3 – Tabela de Providências Complementares e Responsáveis – Monitoramento, Revisão e Atualização: **Orientação Técnica - Programa de Revisão e Atualização de Políticas, Normas, Processos e Procedimentos**, da Deliberação Normativa CGGDIESP-1, de 30/12/2021.

ORIENTAÇÃO TÉCNICA

Programa de Revisão e Atualização de Políticas, Normas, Processos e Procedimentos

1. Objetivos

Esta orientação técnica tem os seguintes objetivos:

- Recomendar procedimentos e práticas para implantação do Programa de Revisão e Atualização de Políticas, Normas, Processos e Procedimentos, providência requerida pela Política de Governança de Dados e Informações (PGDI), no âmbito da Administração Pública estadual, instituída pela Deliberação Normativa CGGDIESP-1, de 30 de dezembro de 2021.
- Disseminar a importância da gestão do ciclo de vida de políticas, normas, processos e procedimentos, considerando as variáveis de controle das mudanças necessárias, de forma a manter a padronização, a estabilidade e a previsibilidade na execução das regras e das atividades operacionais envolvidas.
- Instruir sobre o monitoramento e o acompanhamento das medidas de controle instituídas.

2. Sumário

3. Abrangência

Órgãos e entidades da Administração Pública estadual.

4. Principais documentos relacionados e referenciais bibliográficos

- Política de Governança de Dados e Informações (PGDI), considerando, em seu Anexo II, a providência para a elaboração de orientação técnica para implantação de Programa de Revisão e Atualização de Políticas, Normas, Processos e Procedimentos.
- Procedimento Operacional Padrão (POP) da SSCTI referente ao macroprocesso Planejamento e Gestão da LGPD, com formulação de políticas e diretrizes, e ao subprocesso SP 01 – Formulação de Políticas e Diretrizes.
- Norma Técnica ABNT NBR ISO 9001:2015 – Sistemas de Gestão da Qualidade – Requisitos.
- Norma Técnica ABNT NBR ISO 10013:2021 – Sistemas de Gestão da Qualidade – Orientação para Documentação Orientada.
- ABPMP BRASIL. Guia para o gerenciamento de processos de negócio – Corpo comum de conhecimento – ABPMP BPM CBOK V3.0. 3. ed. [s.l.]: ABPMP, 2013.
- SECCHI, Leonardo. *Políticas públicas*: conceitos, esquemas de análise, casos práticos. São Paulo: Cengage Learning, 2012.
- OLIVEIRA, Vanessa. As fases do processo de políticas públicas. In: MARCHETTI, Vitor (org.). *Políticas públicas em debate*. São Bernardo do Campo: MP Editora, 2013.

5. Glossário

Termos e siglas	Definição
ABNT	Associação Brasileira de Normas Técnicas.
ABPMP	*Association of Business Process Management Professionals International* (Associação Internacional de Profissionais de Gerenciamento de Processos de Negócios).
BPM	*Business Process Management* (Gerenciamento de Processos de Negócios).
BPM CBOK	*Guia para o gerenciamento de processos de negócio – Corpo comum de conhecimento* (publicação da ABPMP).
CGGDIESP	Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo. Órgão colegiado de caráter consultivo, normativo e deliberativo, responsável pela gestão da CDESP e por auxiliar o controlador no desempenho das atividades indicadas no artigo 3º do Decreto Estadual nº 65.347/2020.
ISO	*International Organization for Standardization* (Organização Internacional de Normalização).
LGPD	Lei Geral de Proteção de Dados – Lei nº 13.709/2018. Promulgada para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo, essa Lei rege o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado, englobando amplo conjunto de operações que podem ocorrer em meios manuais ou digitais.
Macroprocesso	Agrupamento de processos necessários para a produção de uma ação ou, ainda, conjunto de atividades pelo qual a organização cumpre suas demandas.

Termos e siglas	Definição
NBR	Norma Técnica.
Norma	Documento, estabelecido por autoridade reconhecida, que assegura as características desejáveis de produtos, serviços e comportamentos, visando a qualidade, segurança, confiabilidade e eficiência.
PDCA	Metodologia de ciclo de vida de processos, de Deming – *Plan*, *Do*, *Check*, *Act* (Planejar, Executar, Verificar, Ajustar).
PGDI	Política de Governança de Dados e Informações. Instituída pela Deliberação Normativa CGGDIESP-1, de 30 de dezembro de 2021, publicada no DOE de 31 de dezembro de 2021, que estabelece parâmetros para as boas práticas em segurança da informação, para a privacidade e proteção de dados pessoais e para a gestão de dados e informações, de observância obrigatória pelos Órgãos e Entidades da Administração Pública estadual.
Política	Documento que estabelece as diretrizes a serem aplicadas em uma organização tendo em vista os objetivos definidos para ela.
POP	Procedimento Operacional Padrão.
PPDP	Política de Proteção de Dados Pessoais. Instituída pela Deliberação Normativa CGGDIESP-2, de 30 de dezembro de 2021, publicada no DOE de 31 de dezembro de 2021, e corresponde à compilação de normas e regras de boas práticas de governança e proteção para tratamento de Dados Pessoais, de observância obrigatória pelos Órgãos e Entidades da Administração Pública estadual.
Procedimento ou Procedimento operacional	Descrição detalhada de todas as operações necessárias para a realização de um processo ou de uma tarefa, ou seja, roteiro padronizado para realizar uma atividade.
Processo	Deve ser entendido como a especificação processual, os insumos, o fluxo de trabalho, as atividades de tratamento e os produtos resultantes esperados de um serviço finalístico (processos de negócios) prestado ao cidadão pela Administração Pública do estado.
SSCTI	Subsecretaria de Serviços ao Cidadão, Tecnologia e Inovação da Secretaria de Governo do Estado de São Paulo.
Subprocesso	Conjunto de atividades dentro de um macroprocesso ou processo, que tem entrada, processamento e saída próprios.
TIC	Tecnologia da Informação e Comunicação.

6. Contexto

As ações para adequação à LGPD dispostas na PGDI e na PPDP e em seus respectivos Anexos II e III implicam a implementação, de forma ampla e transversal, de políticas, diretrizes, normas, metodologias, processos, procedimentos e tecnologias de TIC direcionadas à governança e à proteção das informações e dos dados pessoais, resultando em ações inter-relacionadas e indissociáveis.

Também é parte essencial desse objetivo a promoção de uma mudança cultural dos gestores e colaboradores de todos os níveis da Administração Pública estadual na execução dos serviços públicos, com foco em garantir proteção, eficácia e segurança no tratamento dos dados e das informações pelo Estado, para o que é fundamental a adoção das boas práticas recomendadas pelo CGGDIESP.

A mudança cultural requer a disseminação do conhecimento aliada ao aumento da responsabilidade dos órgãos e das entidades para a estruturação de ações de proteção às informações de maneira geral e aos dados pessoais e dados pessoais sensíveis dos cidadãos em especial, exigindo que os servidores públicos adquiram novas habilidades e adotem novas estratégias e, consequentemente,

maior rigidez no controle, no monitoramento, na manutenção e na atualização das documentações relacionadas às normas e aos processos.

Para lograr êxito em tais objetivos, o Programa de Revisão e Atualização de Políticas, Normas, Processos e Procedimentos é um processo permanente e sistemático, a ser estabelecido, gerenciado e monitorado pela alta administração dos órgãos e entidades, contemplando atividades para identificar, avaliar, monitorar e gerenciar suas políticas, normas, processos e sistemas de forma a mantê-los revisados e atualizados.

Esse processo de revisão sistemática é um elemento importante para a boa governança de dados e da informação e auxilia o gestor a antecipar, identificar e lidar com situações de mudanças, bem como a se preparar para manter níveis adequados de proteção e segurança às informações e ao tratamento de dados.

7. Relação de temas abordados

- Abordagem metodológica.
- Escopo.
- Comprometimento das lideranças.
- Ciclo de vida das políticas e normas e dos processos e procedimentos.
- Revisão sistemática de políticas e normas.
- Revisão sistemática de processos e procedimentos.

8. Descrição das orientações técnicas (diretrizes, regras e/ou procedimentos)

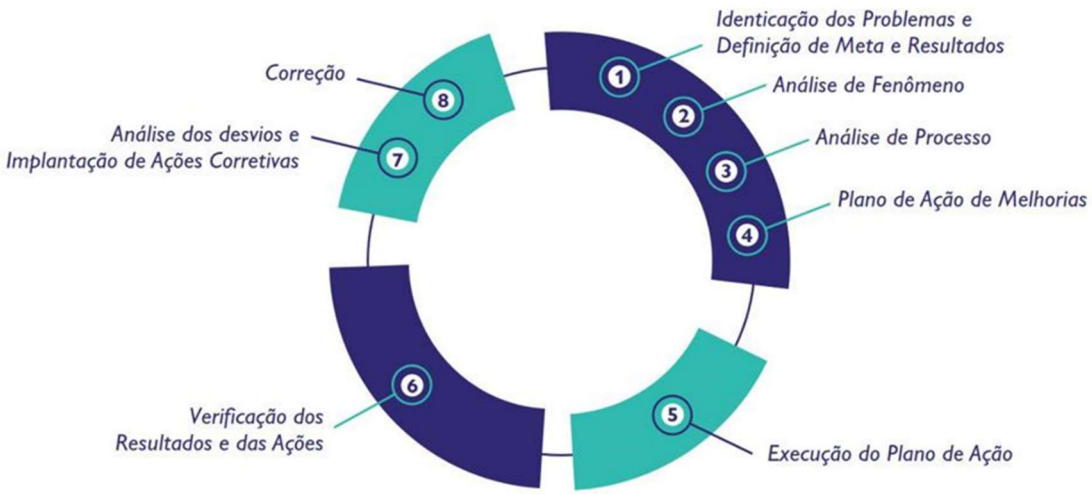
8.1. Abordagem metodológica

A orientação para a aplicação de uma abordagem metodológica na gestão do processo de revisão de políticas, normas, processos e procedimentos proporcionará:

- entendimento e consistência no atendimento aos requisitos e diretrizes da PGDI;
- implementação de valor agregado aos processos e procedimentos, considerando as questões de segurança da informação e da proteção das informações e dos dados;
- atingimento da efetividade (eficiência + eficácia) no desempenho dos processos;
- melhoria de processos baseada na avaliação sistemática de dados e informação.

Os pontos de monitoramento e medição necessários para controle e revisão podem ser específicos para políticas e normas e para processos e procedimentos.

Orienta-se a aplicação dos conceitos da metodologia PDCA (ou Ciclo PDCA, como também é conhecida), que podem ser adotados para todos os processos, em especial para o programa de revisão objeto desta orientação técnica. A seguir, é apresentado o diagrama dessa metodologia.



Metodologia PDCA (Planejar, Executar, Verificar, Ajustar)

O termo PDCA (Planejar, Executar, Verificar, Ajustar – do inglês *Plan*, *Do*, *Check*, *Act*) designa um método interativo de gestão constituído de quatro passos e utilizado para controle, revisão e melhoria contínua de processos e produtos. É também conhecido como "ciclo de controle".

8.2. Escopo

Esta orientação recomenda questões técnicas para a implantação de Programa de Revisão e Atualização de Políticas, Normas, Processos e Procedimentos.

Todos os requisitos desta orientação técnica são genéricos e aplicáveis a todos os órgãos e entidades da Administração Pública estadual, independentemente de seu tipo, de seu tamanho e dos serviços públicos que executem.

O escopo deste documento compreende a:

- revisão e atualização sistemática e periódica de políticas e normas, em especial as relacionadas com as ações de segurança da informação e de proteção de dados pessoais e de dados pessoais sensíveis;
- revisão e atualização sistemática e periódica de processos e procedimentos, de forma a garantir permanente segurança da informação e proteção aos dados pessoais e aos dados pessoais sensíveis.

8.3. Comprometimento das lideranças

A alta direção dos órgãos e entidades deve demonstrar liderança e comprometimento com relação à implantação e à manutenção do Programa de Revisão e Atualização de Políticas, Normas, Processos e Procedimentos:

- responsabilizando-se por designar e alocar equipes de controle e monitoramento para assegurar a execução e a eficácia do programa;

- assegurando que o programa e os seus objetivos sejam alcançados e que sejam compatíveis com o contexto e a estratégia de adequação à LGPD;
- assegurando a integração das políticas, das normas, dos processos e dos procedimentos de gestão e operação, inclusive com os diversos sistemas automatizados de gestão utilizados pelos órgãos e entidades;
- promovendo o uso da metodologia PDCA, o entendimento do conceito de ciclo de vida de políticas, normas, processos e procedimentos, bem como da mentalidade de revisão sistemática;
- assegurando que os recursos necessários para a execução plena do programa estejam disponíveis;
- comunicando a importância do programa e de sua conformidade com a PGDI;
- assegurando o engajamento dos servidores envolvidos, de forma a contribuir para a efetividade do programa;
- promovendo o conceito da melhoria contínua;
- demonstrando liderança e comprometimento com relação ao foco na segurança da informação e na proteção dos dados pessoais e dos dados pessoais sensíveis dos cidadãos.

8.4. Ciclo de vida das políticas e normas e dos processos e procedimentos

Para a adequada implantação e execução do Programa de Revisão e Atualização de Políticas, Normas, Processos e Procedimentos é importante conhecer e difundir os conceitos de ciclo de vida. Ciclo de vida pode ser considerado, conceitualmente, como o conjunto de transformações pelas quais podem passar indivíduos, instituições, serviços, produtos, programas, políticas, normas ou processos, de forma a assegurar a sua continuidade.

8.4.1. Ciclo de vida das políticas e normas

Conforme Leonardo Secchi (2012), o que define se uma política é pública, ou não, é a sua intenção em responder a um problema público. Segundo Secchi, políticas governamentais são aquelas elaboradas e estabelecidas por atores governamentais e são o subgrupo mais importante das políticas públicas.

Conforme Vanessa Oliveira (2013) o termo "política pública" não abarca uma única dimensão da política, mas sim um conjunto de processos que podem ser desagregados em etapas que, no todo, são denominados por "ciclo de política pública". Considerando a literatura sobre o assunto, pode-se depreender que o ciclo das políticas públicas compreende as seguintes etapas: 1) definição ou diretriz do Estado indicando a necessidade da política ou norma; 2) formulação da política ou norma; 3) processo decisório; 4) publicação; 5) implementação; 6) avaliação; e 7) revisão. Essas etapas podem ser consideradas para as políticas e normas específicas e de responsabilidade dos órgãos e entidades.

Para as políticas e normas de responsabilidade do CGGDIESP, as etapas a serem consideradas constam no macroprocesso **Planejamento e Gestão da LGPD, com formulação de políticas e diretrizes**, e no subprocesso **SP 01 – Formulação de Políticas e Diretrizes**, a saber: 1) definição e planejamento da política ou norma; 2) alocação de especialistas de conteúdo; 3) estruturação da política ou norma; 4) aprovação interna; 5) tramitação da política ou norma e validação; 6) apreciação de outros agentes; 7) validação do CGGDIESP; 8) assinatura e publicação; e 9) desdobramento da política ou norma em providências técnicas operacionais.

Para efeitos desta orientação técnica, além das etapas previstas no subprocesso SP 01 – Formulação de Políticas e Diretrizes, deve-se considerar também a etapa de revisão, objeto deste documento.

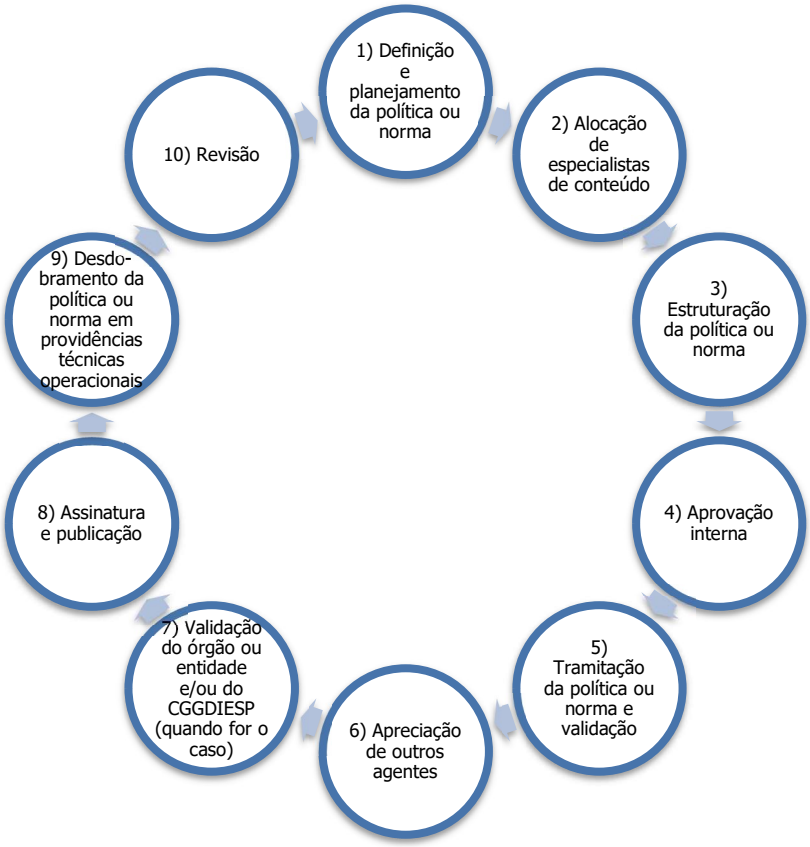


Diagrama do ciclo de vida de políticas e normas

8.4.2. Ciclo de vida dos processos e procedimentos

Conforme o BPM CBOK V3.0, processos e procedimentos devem ser gerenciados em um ciclo contínuo para manter sua integridade e permitir a transformação, o que implica o comprometimento permanente e sistemático dos órgãos e entidades para o gerenciamento de seus processos. O ciclo de vida de processos e procedimentos compreende o planejamento, a análise, o desenho, a implementação, o monitoramento e controle e o refinamento ou revisão. Os processos e procedimentos devem estar alinhados com a estratégia institucional dos órgãos e entidades, com a PGDI e, quando for o caso, com a estratégia de implementação das adequações à LGPD definida pelo CGGDIESP.

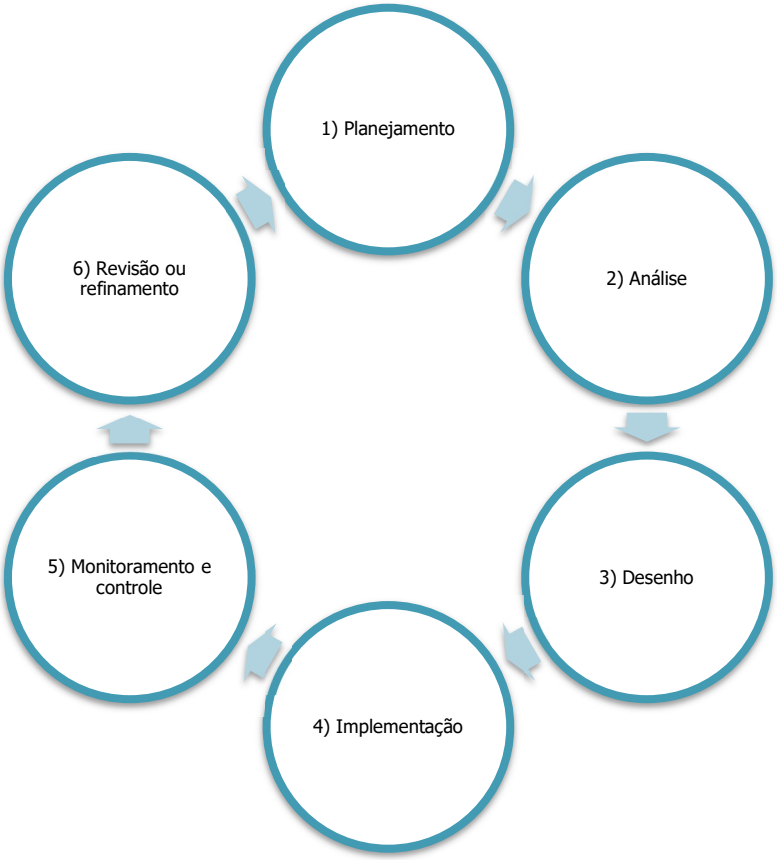


Diagrama do ciclo de vida de processos e procedimentos

8.5. Revisão sistemática das políticas e normas

Vários fatores, considerados gatilhos, podem indicar a necessidade da revisão de políticas e normas, por exemplo, data predefinida para revisão prestes a vencer, requisitos legais, decisão da alta administração, indicadores de resultado da aplicação (identificados na etapa de validação das políticas e das normas), implantação ou atualização de sistemas automatizados e edição de nova regulamentação superveniente. Os órgãos e entidades devem estabelecer um prazo adequado de antecedência da data de validade ou de revisão, para iniciar as ações de revisão.

Uma das etapas consideradas críticas de uma política ou norma é a avaliação. Com este propósito, os responsáveis pela execução da política regulamentada devem estabelecer indicadores para a medição de seus resultados e impactos (estratégicos e operacionais ou sociais) e para a apuração da capacidade de atender aos seus objetivos e garantir serviços públicos adequados aos cidadãos.

Os parâmetros e indicadores podem ser baseados em questões técnicas, bem como na avaliação dos recursos econômicos, de infraestrutura, tecnológicos, humanos, materiais e de atendimento aos cidadãos e instituições, além da análise de conformidade com os preceitos legais do tema em questão. Os parâmetros e indicadores também devem medir os resultados alcançados, isto é, as realizações e/ou os impactos decorrentes da execução das políticas e normas.

Portanto, a etapa de avaliação das políticas e normas é um indicador para o exame de sua real efetividade e para a aferição da necessidade de continuação, reestruturação ou mesmo da extinção da política ou norma em questão.

Da mesma forma que a documentação de processos e procedimentos deve ser gerenciada e controlada, as políticas e normas também devem ser documentadas e controladas.

Ao criar ou atualizar uma documentação de política ou norma, os órgãos e entidades devem assegurar sua identificação e sua descrição, como, título, número de referência, responsável pela autoria e/ou aprovação, data de publicação ou vigência, versionamento e data de validade ou data de revisão.

Os órgãos e entidades devem assegurar que as documentações da política ou norma:

- estejam disponíveis e adequadas para uso, onde e quando elas forem necessárias;
- estejam protegidas suficientemente contra perda de confidencialidade, uso impróprio, indisponibilidade ou perda de integridade, incluindo o armazenamento, a preservação e a legibilidade;
- tenham controle de alterações e de versionamento;
- sejam mantidas em guarda controlada, com possibilidade de distribuição, acesso, recuperação e uso.

8.6. Revisão sistemática dos processos e procedimentos

Conforme o BPM CBOK V3.0, o gerenciamento de mudança e/ou de revisão é um processo iterativo que utiliza um conjunto de técnicas para auxiliar uma organização e seus colaboradores na transição do estado atual de processos e procedimentos para um estado futuro sustentável.

Um Programa de Revisão e Atualização de Políticas, Normas, Processos e Procedimentos requer que as documentações sejam controladas. Para tanto, durante as fases de desenho e implementação, é vital que os processos e procedimentos sejam documentados.

Ao criar ou atualizar uma documentação de processo ou procedimento, os órgãos e entidades devem assegurar sua identificação e sua descrição, como, título, número de referência, responsável pela autoria e/ou aprovação, data de publicação ou vigência, versionamento e data de validade ou data de revisão.

Os órgãos e entidades devem assegurar que as documentações do processo ou procedimento:

- estejam disponíveis e adequadas para uso, onde e quando elas forem necessárias;
- estejam protegidas suficientemente contra perda de confidencialidade, uso impróprio, indisponibilidade ou perda de integridade, incluindo o armazenamento, a preservação e a legibilidade;
- tenham controle de alterações e de versionamento;
- sejam mantidas em guarda controlada, com possibilidade de distribuição, acesso, recuperação e uso.

Os órgãos e entidades devem manter uma estrutura ou arquitetura de processos que contenha um repositório das documentações dos processos institucionais (políticas ou normas de processos;

regras; fluxogramas; POP; matriz de atribuições e responsabilidades; mapa de indicadores; modelos de controles utilizados; lista mestra dos serviços, macroprocessos e subprocessos organizados em visão integrada; base de conhecimento de lições aprendidas, entre outros).

Depois de implantado o processo ou procedimento, seguem-se dois momentos: um tempo para a estabilização da operação e outro correspondente ao processo ou procedimento controlado. Nesses períodos deve-se avaliar os indicadores de processo e de resultados, se as metas estabelecidas estão sendo alcançadas e se há indicação de inconformidades entre a prática e a documentação institucional do processo ou procedimento (essas inconformidades podem ser identificadas por auditorias internas ou externas ou por ação de mapeamento e de revisão dos processos).

É recomendável que os órgãos e entidades estabeleçam uma equipe multidisciplinar para avaliação e aprovação das solicitações de mudanças nos processos e nos procedimentos.

Data de revisão prestes a vencer, requisitos legais, decisão da alta administração, solicitações de mudança (aprovadas pela equipe multidisciplinar) e implantação ou atualização de sistemas automatizados podem ser considerados gatilhos para a implementação da revisão e de possíveis mudanças nos processos e procedimentos. Deve-se estabelecer um prazo adequado de antecedência da data de validade ou de revisão da documentação do processo ou procedimento, para iniciar as ações de revisão. A periodicidade da revisão (vigência) da documentação do processo ou procedimento (redesenho do processo ou procedimento) não deve exceder 24 meses.

A partir de um dos gatilhos de mudança ou de revisão acionados, os órgãos e entidades devem aplicar os conceitos de melhoria contínua (ciclo PDCA) e/ou estabelecer ações ou projetos de revisão, alocando equipes de especialistas para apoio técnico e envolvendo e engajando as equipes gerenciais e operacionais na execução do programa de revisão.

A revisão e as mudanças propostas devem ser aprovadas por equipe multidisciplinar, que deve avaliar todos os impactos que a mudança poderá gerar, considerando questões institucionais, estratégicas, táticas e operacionais. Caso a implementação de mudança tenha impacto nas políticas e normas publicadas pelo CGGDIESP, é necessário o encaminhamento para análise e deliberação desse Comitê.