

APROVA Instrução Normativa CGGDIESP-2/PGDI referente ao Anexo II, 3 – Tabela de Providências Complementares e Responsáveis – Análise dos processos e Ativos de Dados e Informação: **Orientação Técnica - Procedimento de Análise Periódica dos Processos e Ativos de Dados e Informações**, da Deliberação Normativa CGGDIESP-1, de 30/12/2021.

ORIENTAÇÃO TÉCNICA

Orientação Técnica - Procedimento de Análise Periódica dos Processos e Ativos de Dados e Informações

1. Objetivos

Esta orientação técnica tem os seguintes objetivos:

- Recomendar procedimentos e práticas à implementação do processo Análise Periódica dos Processos e Ativos de Dados e Informações; Controle do Inventário dos Processos e Ativos de Dados e Informações; e Identificação dos Gestores dos Processos e Ativos de Dados e Informações, 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 revisão, da atualização e da classificação periódicas dos inventários de processos e ativos de dados e informações, dada a natureza dinâmica da prestação de serviços, das mudanças normativas, da evolução tecnológica e das mudanças em ambientes produtivos, visando garantir disponibilidade e conformidade com a operação e manter a padronização, a estabilidade e a previsibilidade na execução das regras e atividades operacionais envolvidas.
- Instruir sobre o monitoramento e o acompanhamento das medidas de controle instituídas.

2. Sumário

1. Objetivos

2. Sumário

3. Abrangência

4. Principais documentos relacionados e referenciais bibliográficos

5. Glossário

6. Contexto

7. Relação de temas abordados

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

8.1. Abordagem metodológica

8.1.1. Metodologia ITIL®

8.1.2. Metodologia Controles CIS®

8.2. Escopo

8.3. Comprometimento das lideranças

8.4. Ciclo de vida de processos de inventário

8.4.1. Estrutura básica para o ciclo de vida dos inventários

8.5. Análise periódica dos processos e ativos de dados e informações

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 décima providência, voltada à análise periódica dos processos e ativos de dados e informações, tendo como base o artigo 16 da PGDI – “Os órgãos e entidades, em intervalos regulares, devem analisar os respectivos processos e ativos de informação, visando assegurar que estejam devidamente inventariados e classificados, com identificação e ciência dos respectivos gestores, controladores e operadores [...]”.
- Política de Proteção de Dados Pessoais (PPDP), em especial seu Anexo III.
- Orientação Técnica do CGGDIESP que define modelo padrão e instrui sobre “Preenchimento do documento com a relação dos serviços finalísticos prestados ao cidadão, contendo informações sobre as respectivas finalidades, atribuição das bases legais e quais dados pessoais são tratados”, conforme primeira providência requerida pela PPDP, em seu Anexo III.
- Orientação Técnica do CGGDIESP que instrui sobre como fazer o “inventário de dados objeto de tratamento nos serviços prestados ao cidadão ou serviços finalísticos”, conforme quarta providência requerida pela PGDI, em seu Anexo II.
- 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.
- Norma Técnica ABNT-NBR ISO/IEC 27001:2022 –Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos.
- Norma Técnica ABNT-NBR ISO/IEC 27002:2022 – Segurança da Informação, Segurança Cibernética e Proteção à Privacidade — Controles de Segurança da Informação.
- MARQUES, Pedro. Guia completo para ITIL® 4. Desenho de Serviços, [s.d]. Disponível em <https://desenhodeservicos.com.br/guia-completo-para-til4/>. Acesso em: 29 jun. 2022.
- CENTER FOR INTERNET SECURITY (CIS). Controles CIS – Versão 8. [s.l.]: CIS, 2021. Disponível em: <https://learn.cisecurity.org/cis-controls-download>. Acesso em: 28 jun. 2022.

5. Glossário

Termos e siglas	Definição
ABNT	Associação Brasileira de Normas Técnicas.
Ativos de Tecnologia da Informação	Quaisquer meios de armazenamento, transmissão e tratamento das informações, como softwares, hardwares e ambientes físicos.
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.
Checklist	Lista de verificação.
CIS	<i>Center for Internet Security</i> , organização sem fins lucrativos com a missão de tornar o mundo tecnológico mais seguro nas questões cibernéticas.
CIS Controls® ou Controles CIS®	Conjunto de melhores práticas, atualmente na versão 8, composto por 18 controles, conhecidos também como salvaguardas, com objetivo de mitigar os ataques cibernéticos mais prevalentes contra sistemas e redes de tecnologia atuais.
Framework	Estrutura composta por um conjunto de códigos genéricos que permite o desenvolvimento de sistemas e aplicações. Funciona como <i>template</i> ou modelo que, quando utilizado, oferece elementos estruturais básicos para a criação de uma aplicação ou software, bem como para a aplicação de métodos e controles.
IG	<i>Implementation Group</i> (Grupo de Implementação dos Controles CIS®).
Internet das Coisas (IoT)	Sistema interrelacionado de dispositivos computacionais, equipamentos digitais e mecânicos, e objetos aos quais são vinculados UIDs e que possuem a habilidade de transferir dados pela rede sem a necessidade de interação do tipo pessoa-pessoa ou pessoa-computador.
ISO	<i>International Organization for Standardization</i> (Organização Internacional de Normalização).
ITIL®	<i>Information Technology Infrastructure Library</i> (Biblioteca de Tecnologia da Informação e Infraestrutura).
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.
Lista mestra	Documento do tipo catálogo com lista atualizada de todos os documentos que os órgãos e as entidades utilizam internamente, contendo, no mínimo, o código, a descrição e as datas de revisão desses documentos.
Log ou Log de dados	Expressão utilizada para descrever o processo de registro de eventos relevantes em um sistema computacional.
MER	Modelo Entidade e Relacionamento. Representa um banco de dados.
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.
OGC	<i>Office of Government Commerce</i> (Escritório de Comércio do Governo do Reino Unido).
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.
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

Termos e siglas	Definição
	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.
RoPA	<i>Record of Processing Activities</i> (Registro das Atividades de Tratamento de Dados Pessoais).
SGBD	Sistema Gerenciador de Banco de Dados.
SSCTI	Subsecretaria de Serviços ao Cidadão, Tecnologia e Inovação da Secretaria de Governo do Estado de São Paulo.
SVS	Sistema de Valor de Serviço.
TI	Tecnologia da Informação.
TIC	Tecnologia da Informação e Comunicação.

6. Contexto

As ações para adequação aos preceitos da LGPD e às boas práticas de governança de dados e informações 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, inclusive dos dados pessoais e dos dados pessoais sensíveis, resultando em ações inter-relacionadas e indissociáveis.

Também é parte essencial desse objetivo a promoção de uma mudança cultural dos gestores e colaboradores em 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 sensíveis dos cidadãos em especial, exigindo que os servidores públicos adquiram novas habilidades e adotem novas estratégias e, conseqüentemente, maior rigidez no controle, no monitoramento, na manutenção e na atualização das documentações relacionadas às normas e aos processos, bem como no controle e na atualização dos diversos inventários de dados e informações.

Para lograr êxito em tais objetivos, a análise periódica dos processos e ativos de dados e informações 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 os inventários de dados e de informações de forma a mantê-los revisados e atualizados.

A análise periódica ou revisão sistemática dos processos e ativos de dados e informações é, portanto, 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 de processos de inventário.
- Estrutura básica para o ciclo de vida dos inventários.
- Análise periódica dos processos e ativos de dados e informações.

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 análise periódica dos processos e ativos de dados e informações, controle do inventário dos processos e ativos de dados e informações proporcionará:

- entendimento e consistência no atendimento aos requisitos e diretrizes da PGDI;
- base de conhecimento dos diversos dispositivos que se conectam à rede de estrutura tecnológica dos órgãos e entidades, com conexão permanente ou não, e dos *softwares* utilizados por cada um dos ativos de TI;
- garantia de que os ativos de TI sob guarda dos órgãos e entidades sejam gerenciados, inventariados e atualizados de forma efetiva, com a finalidade de apoiar as demandas decorrentes da prestação dos serviços públicos ofertados;
- apoio aos órgãos e entidades na mitigação ou eliminação de possíveis vulnerabilidades de segurança em razão do uso de ativos não autorizados ou falta de parametrização dos mecanismos de proteção e controle;
- garantia de que os ativos de TI, constantes no catálogo ou na lista mestra de controle de inventários de ativos de TI dos órgãos e entidades, sejam devidamente identificados, classificados, organizados e atualizados, de modo a serem controlados, utilizados e monitorados, tendo em vista sua confiabilidade, disponibilidade e preservação;
- melhoria contínua de processos baseada na atualização sistemática dos inventários de ativos de TI.

Os pontos de monitoramento e medição necessários para controle e revisão podem ser específicos para os diferentes tipos de inventário.

As normas técnicas ABNT-NBR ISO/IEC 27001:2022 e ABNT-NBR ISO/IEC 27002:2022 oferecem orientações ou requisitos complementares sobre uma gama de controles para o processo global de segurança da informação, e a atenção a estas orientações e requisitos contribui para o adequado processo de análise periódica dos processos e ativos de dados e informações, controle do inventário dos processos e ativos de dados e informações. A norma técnica ABNT-NBR ISO/IEC 27002:2022 no capítulo 5.9, que trata do “Inventário de informações e outros ativos associados”, orienta que os inventários sejam desenvolvidos e mantidos, bem como orienta que os inventários devem ser precisos, atualizados, consistentes e alinhados com outros inventários considerando: a) análises críticas regulares das informações e dos ativos identificados; e b) impor automaticamente uma atualização dos inventários nos processos de instalação, alteração ou remoção de ativos.

Além das orientações e requisitos das normas técnicas ABNT-NBR ISO/IEC acima citadas, orienta-se a aplicação dos conceitos das metodologias ITIL® e Controles CIS®, apresentados a seguir.

8.1.1. Metodologia ITIL®

Trata-se de um conjunto de procedimentos e boas práticas de gerenciamento operacional padrão para permitir que a instituição gerencie uma operação de TI e a infraestrutura a ela associada. É uma biblioteca em constante evolução, atualmente na versão 4, publicada em 2019, considerada um *framework* para gerenciar serviços de TI.

ITIL® é marca registrada do OGC e os procedimentos e as práticas operacionais recomendadas por ele se aplicam a todos os aspectos da infraestrutura de TI. O ciclo de vida do ITIL considera o SVS, que pode ser visto como uma visão panorâmica do cenário de gerenciamento de serviços de TI dos órgãos e entidades, composta pelos seguintes elementos:

- princípios orientadores;
- governança;
- cadeia de valor de serviço;
- práticas;
- melhoria contínua.

No âmbito desta orientação técnica, o elemento “melhoria contínua” deve ser considerado para embasar a execução do processo Análise Periódica dos Processos e Ativos de Dados e Informações; Controle do Inventário dos Processos e Ativos de Dados e Informações; e Identificação dos Gestores dos Processos e Ativos de Dados e Informações, recomendado pelo ITIL® 4 como prática de gerenciamento geral. A seguir é apresentado o diagrama do ciclo de vida do SVS do ITIL®.



Diagrama do ciclo de vida do SVS do ITIL® 4

8.1.2. Metodologia Controles CIS®

Os Controles CIS® foram criados pelo CIS¹ e são agrupados em IGs. O CIS tem como missão tornar o mundo tecnológico mais seguro desenvolvendo, validando e promovendo soluções oportunas de melhores práticas que ajudam pessoas, empresas e governos a se protegerem contra ameaças cibernéticas generalizadas.

O Controle 01 – Inventário e Controle de Ativos Corporativos estabelece que o inventário e o controle de ativos de TI devem ter gestão ativa (inventariar, rastrear e corrigir) de todos os ativos corporativos (como dispositivos de usuário final, incluindo portáteis e móveis; dispositivos de rede; dispositivos não computacionais; IoT; servidores) conectados física, virtual ou remotamente à infraestrutura tecnológica, bem como daqueles hospedados em ambientes de nuvem, de forma a permitir conhecer com precisão a totalidade dos ativos que precisam ser monitorados e protegidos. De acordo com as definições desse controle, o inventário auxilia na identificação de ativos não autorizados e não gerenciados com vistas a removê-los ou remediá-los.

O Controle 02 – Inventário e Controle de Ativos de *Software* estabelece que o inventário e o controle de ativos de *software* devem ter gestão ativa (inventariar, rastrear e corrigir) de todos os *softwares* (sistemas operacionais e aplicações) existentes na infraestrutura tecnológica, de forma a garantir que apenas *softwares* autorizados sejam instalados e/ou executados e que *softwares* não autorizados e não gerenciados sejam localizados e impedidos de serem instalados e/ou executados.

A seguir é apresentado o diagrama da estrutura dos Controles CIS® versão 8.

¹ Fonte: Site do *Center for Internet Security (CIS)* em <http://www.cisecurity.org/controls/>



v8



Diagrama da estrutura dos Controles CIS® versão 8

8.2. Escopo

Esta orientação técnica recomenda abordagens técnicas para a implantação de procedimento de análise periódica dos processos e ativos de dados e informações, controle do inventário dos processos e ativos de dados e informações e identificação dos gestores dos processos e ativos de dados e informações. Os requisitos apresentados são gerais 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 análise periódica dos processos e ativos de dados e informações, o controle do inventário dos processos e ativos de dados e informações e a identificação dos gestores dos processos e ativos de dados e informações. Para isso, compreende a análise e a atualização sistemática dos seguintes inventários:

- **Inventário de processos**, considerando a) a identificação do processo (incluindo seu nome, sua finalidade, sua base normativa e o responsável por ele); b) os dados tratados pelo processo; c) como é executado o tratamento (com indicação do fluxo do processo, das relações e das interdependências com outros processos); e d) a classificação do processo. O resultado deve ser registrado no documento do inventário dos serviços finalísticos e dos processos a eles relacionados, com foco no tratamento de dados pessoais e dados pessoais sensíveis, conhecido como RoPA, conforme primeira providência requerida pela PPDP, em seu Anexo III.
- **Inventário de dados**, considerando a) a identificação do dado/campo; b) o nome do banco de dados; c) o local onde o banco de dados está hospedado (endereço do servidor); d) o nome do SGBD; e) a indicação das regras de validação ou fórmulas; f) a relação dos sistemas que utilizam o dado; g) o código de identificação do RoPA relacionado ao inventário de dados; h) o *link* para acesso ao diagrama de MER; i) o *link* para acesso aos *logs* que registram as transações e os tratamentos realizados com os dados; e j) a indicação dos nomes dos

processos que utilizam o banco de dados, conforme quarta providência requerida pela PGDI, em seu Anexo II.

- **Inventário de sistemas**, considerando a) a estratégia para o inventário; b) os critérios de classificação de *software* e *hardware*; c) o inventário de sistemas; d) o inventário de bases de dados; e) o inventário de *hardwares*; e f) o inventário de *softwares*, conforme décima terceira providência requerida pela PGDI. A norma técnica ABNT-NBR ISO/IEC 27002:2022 também orienta, no capítulo 5.12, que informações e ativos sejam classificados de acordo com a necessidade de segurança da informação, considerando a confidencialidade, a integridade, a disponibilidade, e os requisitos relevantes à proteção dos ativos. Conforme a norma a classificação dos ativos pode ser determinada pelo nível de impacto que seu comprometimento teria para os órgãos e entidades.

8.3. Comprometimento das lideranças

O comprometimento e a liderança da alta direção dos órgãos e entidades são fundamentais para o processo Análise Periódica dos Processos e Ativos de Dados e Informações; Controle do Inventário dos Processos e Ativos de Dados e Informações; e Identificação dos Gestores dos Processos e Ativos de Dados e Informações, na medida em que ela:

- responsabilize-se por designar e alocar equipe de controle e monitoramento para assegurar a execução e a eficácia do processo, conforme recomendação no item 8.5 desta orientação técnica;
- assegure que o processo e os seus objetivos sejam alcançados e que sejam compatíveis com o contexto e a estratégia de promoção da governança de dados e informações e de adequação à LGPD;
- assegure a integração com outras providências, declaradas na PGDI e na PPDP, correlacionadas com esta orientação técnica;
- promova o uso adequado das metodologias indicadas para controle e atualização dos inventários declarados no escopo desta orientação técnica, bem como a mentalidade de análise e atualização periódica dos inventários;
- assegure que os recursos necessários para a execução plena do processo estejam disponíveis;
- comunique a importância do processo e de sua conformidade com a PGDI;
- assegure o engajamento dos servidores envolvidos, de forma a contribuir para a efetividade do processo;
- promova o conceito de melhoria contínua;
- demonstre liderança e comprometimento com relação ao foco no controle e no monitoramento dos ativos de TI.

8.4. Ciclo de vida de processos de inventário

Para a adequada implantação e execução do processo Análise Periódica dos Processos e Ativos de Dados e Informações; Controle do Inventário dos Processos e Ativos de Dados e Informações; e Identificação dos Gestores dos Processos e Ativos de Dados e Informações 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.

Independentemente do tamanho do órgão ou entidade, do tipo de serviço público que oferta e da quantidade de ativos de TI que possui, a elaboração e a correta manutenção do inventário facilitam o gerenciamento da infraestrutura tecnológica. Para a renovação constante do ciclo de vida, deve-se manter o inventário sempre revisado e atualizado.

8.4.1. Estrutura básica para o ciclo de vida dos inventários

O ciclo de vida dos inventários de ativos de TI deve ser um processo formalizado e, se possível, suportado por *softwares* ou sistemas especializados em gestão de ativos. Existem vários *frameworks* ou versões para a gestão do ciclo de vida dos ativos de TI, e esta orientação técnica considera a estrutura básica que compreende as seguintes etapas: 1) concepção ou planejamento; 2) execução; 3) implantação; 4) monitoramento; 5) manutenção; e 6) descarte.



Diagrama da estrutura básica do ciclo de vida dos inventários de ativos de TI

As seguintes etapas são consideradas críticas à análise periódica dos processos e ativos de dados e informações:

- **Monitoramento:** consiste no acompanhamento sistemático do uso dos ativos inventariados, visando garantir o uso ideal e eficiente e identificar possíveis riscos à proteção

da informação, entre outros. Nessa etapa, os dados relevantes devem ser capturados e analisados, e os resultados devem ser registrados e disponibilizados à gestão do órgão ou entidade. A análise periódica deve ser considerada parte integrante do monitoramento.

- **Manutenção:** os ativos de TI devem permanecer operacionais e disponíveis, e isso requer manutenção contínua, atualizações programadas ou mesmo ações de emergência. A análise periódica é uma das formas de garantir que essa etapa seja executada para cada ativo do órgão ou entidade.
- **Descarte:** a análise periódica deve identificar quando um ativo atinge o final de seu ciclo de vida, e o órgão ou entidade deve decidir sobre sua substituição ou descarte, mantendo sob controle a segurança das informações.

A análise periódica dos processos e ativos de dados e informações deve estar alinhada 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.

8.5. Análise periódica dos processos e ativos de dados e informações

Vários fatores, considerados gatilhos, podem indicar a necessidade de execução do processo de análise periódica, por exemplo, data predefinida para análise periódica, requisitos legais, decisão da alta administração, alteração no serviço público finalístico ofertado pelo órgão ou entidade, implantação ou atualização de sistemas automatizados, suspeita de perda de ativo(s), solicitação de inventário feita por órgão regulador ou competente 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 análise periódica. A periodicidade da análise periódica (vigência) não deve exceder 24 meses.

A documentação do processo de inventário e de análise periódica dos processos e ativos de dados e informações deve ser gerenciada e controlada. Ao criar ou atualizar tal documentação, os órgãos e entidades devem assegurar que ela:

- esteja disponível e adequada para uso, onde e quando for necessária;
- tenha identificação, por exemplo, título, número de referência, responsável pela autoria e/ou aprovação, data de publicação ou vigência e data de validade;
- esteja protegida suficientemente contra perda de confidencialidade, uso impróprio, indisponibilidade ou perda de integridade, incluindo o armazenamento, a preservação e a legibilidade;
- tenha controle de alterações e de versionamento;
- seja mantida em guarda controlada, com possibilidade de distribuição, acesso, recuperação e uso.

É recomendável que os órgãos e entidades designem uma equipe multidisciplinar como responsável por executar a análise periódica dos ativos de dados e informações e por garantir que nenhum detalhe seja desconsiderado e que todo o processo seja documentado.

A partir de um dos gatilhos de mudança ou de revisão acionados, os órgãos e entidades devem aplicar os conceitos das abordagens metodológicas presentes nesta orientação técnica e/ou estabelecer ações ou projetos de revisão, alocando especialistas de TI para apoio técnico e envolvendo e engajando as equipes gerenciais e operacionais na execução dessa ação.

A documentação do processo e do resultado da análise periódica dos processos e ativos de dados e informações deve ser salva em um repositório seguro, protegido e com acesso controlado, de forma a garantir que ela não seja alterada indevidamente nem perdida.

Na execução da análise, revisão ou atualização dos inventários de processos e ativos de dados e informações, é importante seguir um procedimento preestabelecido. Nesse sentido, o órgão ou entidade deve elaborar e seguir um *checklist*, com vistas a garantir que nenhum dado relevante seja esquecido. Uma boa prática é o agendamento de manutenções preventivas dos ativos de TI, cujos resultados devem ser considerados na etapa de monitoramento e no processo de análise periódica.

O processo de análise periódica dos processos e ativos de dados e informações deve considerar também:

- nos **inventários de processos**, a finalidade, o tratamento e os demais componentes relacionados com os dados tratados;
- nos **inventários de dados**, entre outras questões, a possibilidade de eliminação de dados não mais necessários em razão tanto da expiração do prazo de retenção estabelecido para tal quanto de mudança na relação da coleta mínima de dados exigidos à execução do processo ao qual pertencem;
- nos **inventários de *hardwares e softwares***, as implementações de novos dispositivos (equipamentos, ferramentas ou sistemas automatizados), bem como a atualização daqueles já existentes, incluindo a relação de novos módulos ou funcionalidades implantadas.

Os resultados da análise periódica dos inventários devem ser consolidados com o inventário de período anterior, e suas divergências devem ser encaminhadas às áreas competentes para avaliação e correção.

Conforme a décima providência prevista na PGDI, os órgãos e entidades devem elaborar Manual Técnico Procedimental considerando esta orientação técnica, agregando diretrizes, regras locais e procedimentos (passo a passo) para a revisão e a atualização periódica dos inventários de processos, dados e sistemas.