Termos e siglas	Definição
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	*Record of Processing Activities* (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.

14. 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, consequentemente, 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.

15. 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.

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

16.1. 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.

16.1.1. 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®.

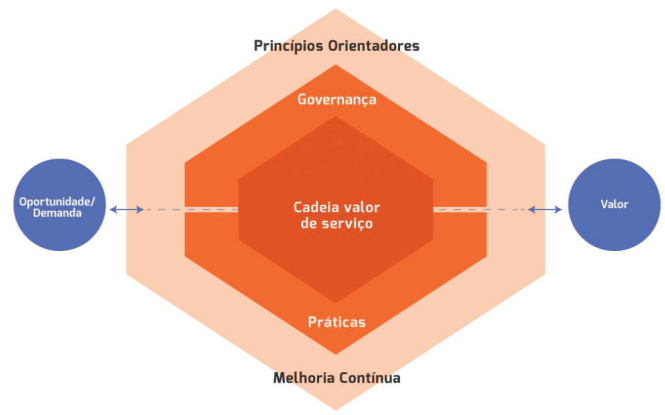

Diagrama do ciclo de vida do SVS do ITIL® 4

16.1.2. Metodologia Controles CIS®

Os Controles CIS® foram criados pelo CIS[1] 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/