**APROVA** Instrução Normativa CGGDIESP-3/PGDI referente ao Anexo II, 3 – Tabela de Providências Complementares e Responsáveis – Uso dos Ativos de Informação: **Orientação Técnica – Inventário de Hardware e Software**, da Deliberação Normativa CGGDIESP-1, de 30/12/2021.

# ORIENTAÇÃO TÉCNICA
## Inventário de Hardware e Software

## 1. Objetivos

Esta orientação técnica tem os seguintes objetivos:

- Recomendar procedimentos e práticas à implementação do processo de "Inventário de *hardware* e de *software*", décima terceira 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 de se realizar inventários de *hardware* e *software*, visando garantir que os ativos de informação sejam identificados adequadamente por meio de atividades de mapeamento, de monitoramento e controle dos ativos tecnológicos, subsidiando as atualizações, a implementação de controles de segurança e a gestão de risco dos órgãos e entidades.

## 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, no seu Anexo II, a décima terceira providência definida com base no Artigo 19 da PGDI, que normatiza que: "Os órgãos e entidades da Administração Pública estadual devem realizar e manter devidamente atualizado inventário de hardwares e softwares de sua propriedade".
- Guia Orientativo do CGGDIESP para "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.

- Norma Técnica ABNT NBR ISO/IEC 19770-1:2017 – Tecnologia da Informação — Gerenciamento de Ativos de TI — Parte 1: Sistemas de Gerenciamento de Ativos de TI — Requisitos. Descreve as práticas recomendadas para o gerenciamento de ativos de TI.
- Norma Técnica ABNT NBR ISO/IEC 19770-2:2015 – Tecnologia da Informação – Gerenciamento de Ativos de TI – Parte 2: Etiqueta de Identificação de software. Ajuda a identificar programas de software em determinado dispositivo.
- Norma Técnica ABNT NBR ISO/IEC 19770-4:2017 – Tecnologia da Informação — Gerenciamento de Ativos de TI — Parte 4: Medição de Utilização de Recursos. Permite a geração de relatórios padronizados sobre o uso de recursos, importante ao gerenciar licenças mais complexas e software e hardware baseados na nuvem.
- MARQUES, Pedro. Guia completo para ITIL® 4. Desenho de serviços, [s. d]. Disponível em: https://desenhodeservicos.com.br/guia-completo-para-itil4/. 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** | *Center for Internet Security*, 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 de 18 controles, conhecidos também como salvaguardas, com o objetivo de mitigar os ataques cibernéticos mais prevalentes contra sistemas e redes de tecnologia atuais. |
| **COETIC** | Conselho Estadual de Tecnologia da Informação e Comunicação. Órgão colegiado de caráter consultivo, normativo e deliberativo, regido pelos Decretos nº 64.601/2019 e nº 64.731/2020, responsável, entre outros, por analisar e aprovar políticas públicas referentes à Tecnologia, Informação e Comunicação, no âmbito do Estado de São Paulo. |
| ***Framework*** | Estrutura composta por um conjunto de códigos genéricos que permite o desenvolvimento de sistemas e aplicações. Funciona como *template* 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** | *Implementation Group* (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** | *International Organization for Standardization* (Organização Internacional de Normalização). |
| **ITIL®** | *Information Technology Infrastructure Library* (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 |

| Termos e siglas | Definição |
|---|---|
| | 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. |
| **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** | *Office of Government Commerce* (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 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. |
| **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 e pelo COETIC.

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 exigindo também, 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, o inventário de *hardware* e de *software* 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 todos os *hardwares* e *softwares* sob sua responsabilidade.

O inventário de *hardware* e de *software* é de extrema importância para a segurança da informação, e para o controle dos ativos de TI. É um procedimento que tem a finalidade de prover o conhecimento de todos os dispositivos que se conectam à rede de infraestrutura tecnológica dos órgãos e entidades, e os respectivos *softwares*, sistemas, ferramentas e aplicativos, físicos ou virtualizados, correspondentes, bem como tem a finalidade de indicar aos responsáveis quais ações são necessárias para a mitigação de possíveis vulnerabilidades de segurança, e para identificar ativos não autorizados.

Os inventários também têm por objetivo conciliar a contagem apurada de dispositivos existentes com as quantidades registradas nos sistemas de controle de ativos e com os registros patrimoniais e contábeis.

O inventário de *hardware* e de *software* 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.
- Inventário de *hardware* e de *software*.

## 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 inventário de *hardware* e de *software* proporcionará:

- entendimento e consistência no atendimento aos requisitos e diretrizes da PGDI;
- base de conhecimento dos diversos dispositivos, em especial *hardwares* e *softwares*, 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; e
- 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.

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. Por esta norma os inventários devem ser realizados e mantidos por sua função relevante à segurança da informação, por isso orienta que a localização dos ativos seja incluída como informação importante e de forma apropriada, indicando que a granularidade das informações dos inventários esteja em nível adequado a gestão dos ativos e para as necessidades dos órgãos e entidades. Também orienta que os órgãos e entidades identifiquem e documentos os ativos (*hardwares* e *softwares*) que estejam em posse de pessoal ou instituições contratadas, com o propósito de proteger e controlar as respectivas devoluções dos ativos, quando do encerramento dos contratos.

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 por ele recomendadas 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:

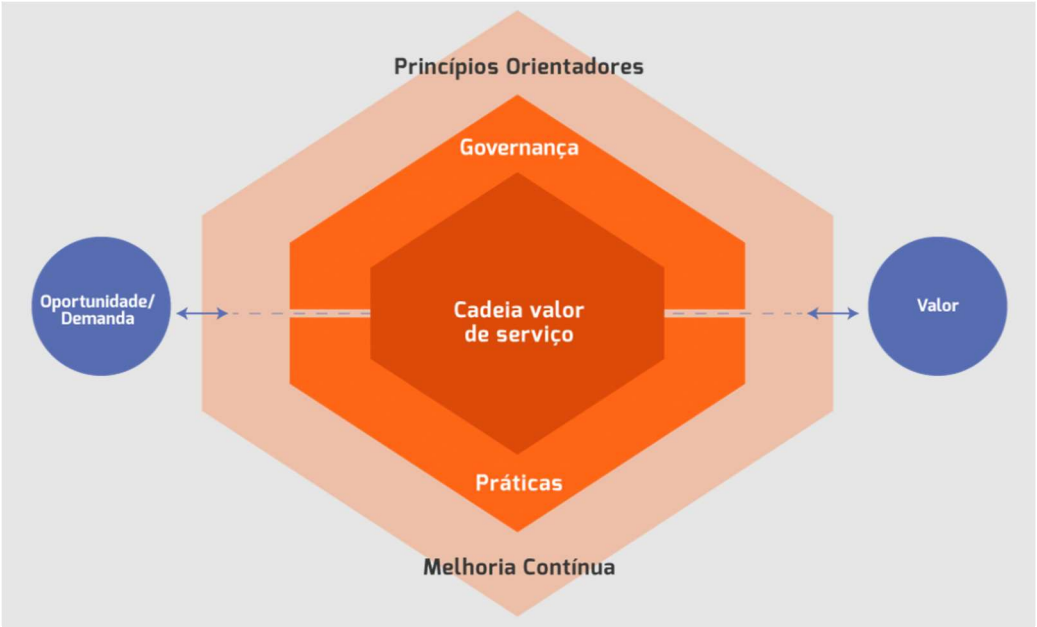
- princípios orientadores;
- governança;
- cadeia de valor de serviço;
- práticas; e
- melhoria contínua.

No âmbito desta orientação técnica, consideramos dois principais elementos:

1. o elemento "governança", que conforme o ITIL® 4 envolve ações de avaliação, de direção e de monitoramento de atividades cujo objetivo final é garantir que a cadeia de valor do serviço e as práticas da instituição funcionem bem e em linha com os objetivos dos serviços finalísticos de cada órgão ou entidade.

2. o elemento "práticas" que deve ser considerado para embasar a execução do processo Inventário de *hardware* e de *software*, recomendado pelo ITIL® 4 em práticas de gerenciamento de serviços, que inclui o gerenciamento de ativos de TI, bem como em práticas de gerenciamento técnico, que inclui: o gerenciamento de infraestrutura e plataforma; e o desenvolvimento e o gerenciamento de *softwares*.

A seguir é apresentado o diagrama do ciclo de vida do SVS do ITIL®.



### 8.1.2. 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 proteger 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 devem 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 executados, e que *softwares* não autorizados e não gerenciados sejam localizados e impedidos de serem instalados e executados.

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


**Diagrama da estrutura dos Controles CIS® versão 8**

[1] Fonte: *Site* do *Center for Internet Security* (CIS): http://www.cisecurity.org/controls/ (acesso em: 12 ago. 2022).

## 8.2. Escopo

Esta orientação técnica recomenda abordagens técnicas para a implantação de procedimento de inventário de *hardware* e de *software*. 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 as orientações técnicas necessárias para o inventário de *hardware* e de *software*, que deverá contemplar os seguintes itens:

- **Sistema de Negócios (que implementa o processo ou serviço finalístico)**, incluindo o nome do sistema, quem é o responsável ou proprietário do sistema (*system owner*), se foi desenvolvido internamente ou se é comercial, qual é a versão atual, quais são as configurações técnicas e de controle, se o sistema possui política de *backup* estabelecida e quais são as relações e interdependências com outros sistemas.
- **Sistema de Gerenciamento de Base de Dados**, incluindo o nome da base de dados, quem é o responsável ou proprietário da base de dados (*data base owner*), se foi desenvolvida internamente ou se é comercial, qual é a versão atual, quais são os dados que compõem essa base de dados, a quais sistemas ela atende, qual é a arquitetura e quais são as configurações técnicas e de controle, se a base de dados possui política de *backup* estabelecida etc.
- ***Hardware***, elencando quantos e quais são os ativos de TI existentes na área ou que rodam ou armazenam os sistemas existentes e detalhando a categoria de cada *hardware*, fabricante, localização, quem é o responsável ou proprietário, quais são as configurações técnicas e de controle de cada *hardware* etc.
- ***Software***, elencando quantos e quais são os *softwares* utilizados e detalhando a categoria de cada *software*, o fabricante, a versão e atualização, quem é o responsável ou proprietário, a quantidade em uso e a forma de licenciamento, quais são as configurações técnicas e de controle de cada *software* etc.

## 8.3. Comprometimento das lideranças

O comprometimento e a liderança da alta direção dos órgãos e entidades são fundamentais para o processo de Inventário de *hardware* e de *software*, na medida em que esta:

- designe e aloque equipe para assegurar a execução e a eficácia do processo, conforme recomendação no item 8.5.1.1. desta orientação técnica;
- assegure que o processo e os seus objetivos sejam alcançados e 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 os recursos necessários para a execução do processo, dentre os recursos 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, em especial quanto ao processo de inventário de *hardware* e de *software*.

## 8.4. Ciclo de vida de processos de inventário

Para a adequada implantação e execução do processo de inventário de *hardware* e de *software*, é importante conhecer e difundir os conceitos abrangidos pelo ciclo de vida. Ciclo de vida pode ser considerado, conceitualmente, como o conjunto de transformações pelas quais passam 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 permitem e 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.

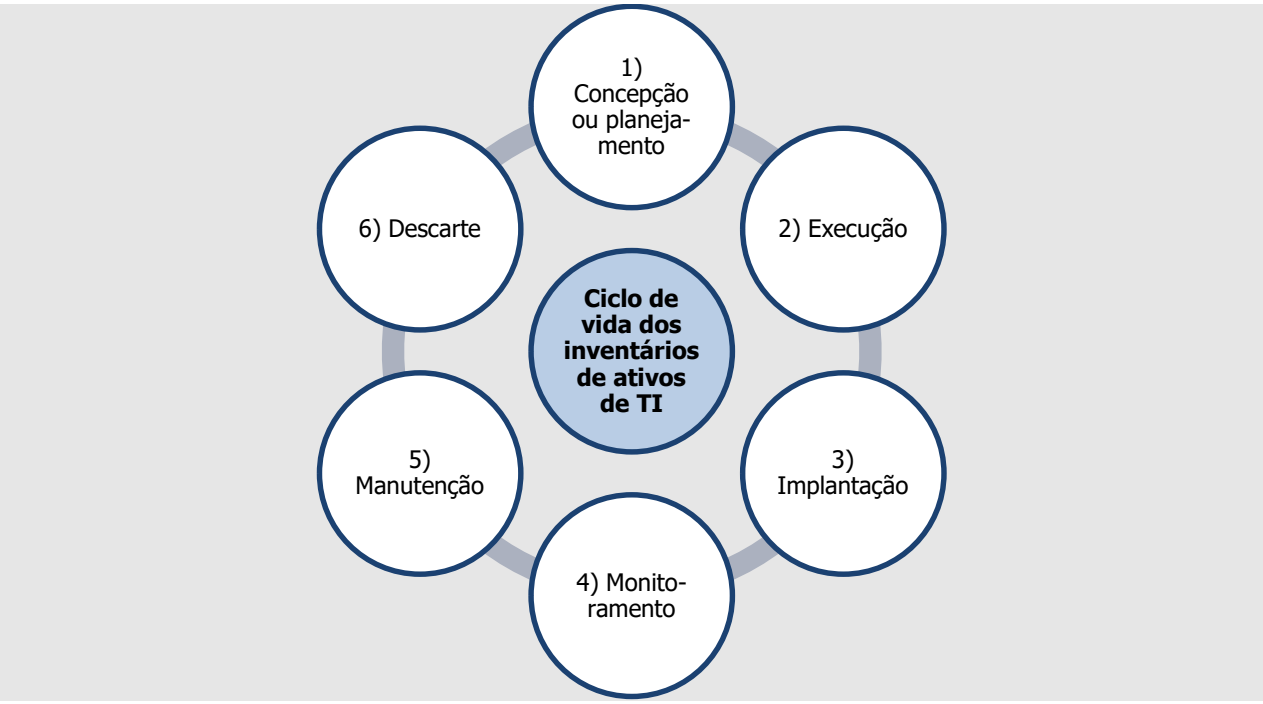



**Diagrama da estrutura básica do ciclo de vida dos inventários de ativos de TI**

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. O inventário sistemático de *hardware* e de *software* é uma das formas de garantir que essa etapa seja executada para cada ativo do órgão ou entidade.
- **Descarte**: o inventário de *hardware* e de *software* 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.

Os inventários de *hardware* e de *software* devem ser alinhados com a estratégia institucional dos órgãos e entidades, com as diretrizes do COETIC, sempre que houver, com a PGDI e, quando for o caso, com a estratégia de implementação das adequações à LGPD definida pelo CGGDIESP.

## 8.5. Inventário de *hardware* e de *software*

Vários fatores, considerados gatilhos, podem indicar a necessidade de execução do processo de inventário de *hardware* e de *software*, 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.

Recomenda-se realizar inventários considerando periodicidade predefinida e os seguintes tipos:

- anual: deve ser realizado até a terceira semana de janeiro do ano subsequente;
- inicial: deve ser realizado em caso de ser estabelecida uma nova área, departamento, pasta, órgão ou entidade, assim ficará registrada a lista inicial de ativos de TI;
- cíclico ou rotativo: consiste na realização de inventários periódicos em vez de fazer um único inventário anual. Este processo está previsto na Orientação Técnica do CGGDIESP que atende à décima providência prevista na PGDI, "Procedimento de análise periódica dos processos e ativos de dados e informações";
- por transferência de responsabilidade: nos casos em que um novo gestor assuma a responsabilidade de uma área, formalizando, assim, os ativos que ficarão sob sua responsabilidade;
- por descarte ou movimentação entre áreas: quando houver necessidade de baixa do ativo ou se ele for movimentado (transferido) para outra área;
- eventual: deve ser realizado sob demanda do gestor responsável pelo ativo de TI, como forma de manutenção da gestão e do controle, visando antecipar a resolução de possíveis inconsistências.

Para melhor compreensão, este capítulo será subdividido em três tópicos, sendo: a) Gerenciamento dos ativos de tecnologia da informação; b) Inventário de *hardware*; e c) Inventário de *software*.

### 8.5.1. Gerenciamento dos ativos de tecnologia da informação

Um ativo de tecnologia da informação pode ser definido como quaisquer meios, equipamentos e sistemas necessários para armazenamento, transmissão, processamento e tratamento das informações, como *softwares*, *hardwares* e ambientes físicos ou virtuais (os locais onde se encontram esses meios).

Faça o gerenciamento dos ativos de TI ao longo de seu ciclo de vida para garantir que o uso de cada ativo seja efetivo, que permaneçam operacionais, sejam contabilizados adequadamente, e que sejam fisicamente protegidos. Garanta que os ativos de TI que são críticos para suportar os serviços finalísticos de órgãos e entidades sejam confiáveis e disponíveis. Para um melhor entendimento da gestão de ativos de TI, recomendamos analisar e verificar a viabilidade da aplicação dos conceitos e dos requisitos constantes na família das normas ISO/IEC 19770, em especial as partes 1, 2 e 4.

É importante gerenciar também as licenças de *software* para garantir que seu uso e a quantidade requerida pelos processos estejam compatíveis com os sistemas instalados e considerem a possibilidade de escalabilidade do serviço prestado, bem como estejam em conformidade com os devidos contratos de licenças. O gerenciamento das licenças deve ser feito também para os *softwares* utilizados em equipamentos virtualizados (por computação em nuvem).

Um conceito importante para o gerenciamento dos ativos de TI é a depreciação, que pode ser entendida como a perda do valor financeiro do ativo ao longo do seu ciclo de vida. A partir desse entendimento, é possível inferir que quando a depreciação se completa, o ativo perdeu seu valor financeiro, e pode ter se desgastado ou se tornado obsoleto. Os gestores dos órgãos e entidades devem considerar a depreciação como uma referência para o tempo de vida útil de cada ativo. Comumente, a área contábil tem as informações sobre a depreciação.

#### 8.5.1.1. Estratégia para o inventário

O aspecto mais importante do gerenciamento de ativos de TI é estabelecer uma estratégia para a execução dos inventários.

A primeira ação estratégica que deve ser adotada pelos órgãos e entidades é a designação de uma equipe multidisciplinar, responsável por executar os inventários de *hardware* e de *software* e por garantir que nenhum detalhe seja desconsiderado.

A estratégia deve ser fundamentada nos objetivos que se deseja atingir, e recomendamos organizá-la considerando a seguinte estrutura de temas:

- objetivo do inventário;
- metodologia a ser adotada (vide a seguir);
- abrangência e escopo;
- localidades;
- tipo de equipamentos (categorias);
- data de início;
- data estimada para a conclusão;
- identificação visual de contabilização do equipamento (etiqueta) – para inventários físicos (realizados em campo);
- tipo de inventário: físico x automatizado x misto;
- periodicidade entre inventários;
- manutenção do inventário;
- critério de aceitação para encerramento do inventário;
- percentual de equipamentos localizados (total e/ou por departamento);
- percentual do valor base (inicial/compra) de equipamentos localizados (total e/ou por departamento);
- percentual do valor residual (saldo da depreciação) de equipamentos localizados (total e/ou por departamento);
- número máximo de verificações no mesmo local;
- número mínimo de pessoas diferentes que devem fazer a verificação em campo;
- ações previstas (aceitáveis) para tratamento das exceções;
- nome dos membros da equipe de execução do inventário;
- aprovador do inventário.

### 8.5.1.2. Abordagens para a execução dos inventários

Considerando as diversas metodologias aplicáveis à execução dos inventários, orientamos algumas abordagens técnicas que ajudarão na obtenção dos resultados esperados.

- **Levantamento em campo *versus* o livro de controle (*floor-to-book*):**
    - De forma "livre", ou seja, sem se utilizar de nenhuma lista de equipamentos prévia, a equipe de inventário deve ir a campo e listar todos os equipamentos que encontrar em uma determinada localidade.
    - Depois, de posse dessa lista recém-criada, a equipe de inventário deve comparar o levantamento feito em campo com um inventário (vigente) que foi coletado e validado em período anterior.
    - As possíveis divergências, identificadas entre o que foi encontrado *versus* o que deveria ter sido encontrado, devem ser analisadas, considerando que as justificativas devem ser documentadas, os controles do inventário atualizados, e requerida a aprovação da atualização do inventário.

Essa abordagem é mais utilizada quando se quer conferir/atualizar a qualidade do último inventário realizado (vigente).

- **Inventário de livro de controle *versus* o levantamento em campo (*book-to-floor*):**
    - De forma "amarrada", ou seja, de posse de uma lista de equipamentos obtida no inventário vigente, a equipe de inventário deve ir a campo e apontar a existência de todos os equipamentos da lista em uma determinada localidade.
    - Depois, de posse desses apontamentos aferidos em campo, a equipe de inventário deve analisar as divergências entre o que foi encontrado *versus* o que deveria ter sido encontrado, documentar suas razões, atualizar os controles do inventário, e solicitar aprovação de um novo inventário, que passa a ser o inventário vigente.

Essa abordagem é mais utilizada quando se quer dar celeridade ao processo de inventário de uma localidade (sem a preocupação de se inventariar 100% da localidade) e/ou confirmar a localização de um determinado equipamento em uma localidade.

- **Verificação de livro de controle *versus* documentos de entrada e saída (*book-to-book*):**
    - De posse de duas listas de equipamentos para uma localidade, uma obtida no inventário vigente e a outra do inventário do período imediatamente anterior a este, a equipe de inventário deve identificar as diferenças entre as listas, apontando os equipamentos da lista vigente que não estavam na lista anterior e os equipamentos que estavam na lista anterior, mas que não figuram mais na lista do inventário vigente.

- Depois, as inconsistências devem ser confrontadas com os documentos dos processos de tramitação de equipamentos (entradas e saídas), considerando as evidências correspondentes.
- As divergências que ainda persistirem dos equipamentos que não possuem a documentação de processo de tramitação correspondente e que justifique sua condição (presente ou ausente) devem ser analisadas, considerando documentar as devidas justificativas, bem como atualizar os controles do inventário, e requerer a aprovação do novo inventário.
- No caso de identificar falhas no processo de tramitação de equipamentos que mereçam atenção ou correções, estas deverão ser apontadas e encaminhadas para o gestor responsável para a tomada das providências necessárias.
- Se as falhas identificadas no processo de tramitação de equipamentos forem pontuais e/ou erro de entendimento da equipe de inventário, deve-se avaliar a necessidade de reforçar a capacitação da equipe.

Essa abordagem é mais utilizada quando se quer conferir a qualidade da execução dos processos de tramitação de equipamentos.

Independentemente das abordagens utilizadas, é recomendável que as equipes de inventário procedam com pelo menos duas contagens, e, no caso de divergência entre as duas, executar uma terceira. Outra recomendação é que as ações de inventário sejam acompanhadas por equipes de controle interno ou de auditoria interna, com autonomia e isenção para análise crítica dos procedimentos. É prerrogativa do gestor definir a necessidade do acompanhamento de uma auditoria externa.

#### 8.5.1.3. Controle da documentação do processo de inventário

A documentação do processo de inventário 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, como 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.

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, alocando especialistas de TI para apoio técnico e envolvendo e engajando as equipes gerenciais e operacionais na execução dos inventários.

A documentação do processo e do resultado dos inventários de *hardware* e de *software* deve ser salva em um repositório seguro, protegido e com acesso controlado, de forma a garantir que ela não seja alterada indevidamente nem perdida.

Os resultados 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 terceira 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 execução adequada dos inventários de *hardware* e de *software*.

### 8.5.2. Inventário de *hardware*

O conhecimento fornecido pelo inventário permite, aos órgãos e entidades, um planejamento mais efetivo, com a implementação de ações estratégicas preditivas.

Dentre os resultados obtidos com o inventário, podemos citar:

- visão da situação de cada *hardware;*
- *hardwares* não localizados, com recomendação para que o responsável tome as providências necessárias;
- *hardwares* subutilizados, com recomendação para realocação ou melhor aproveitamento do uso;
- *hardwares* inservíveis;
- *hardwares* sem identificação patrimonial, permitindo sua regularização;
- a qualidade dos *hardwares*, verificando o tempo de uso e de vida útil;
- possíveis equipamentos, de particulares ou de terceiros, e que estejam em uso pelos órgãos e entidades, para avaliar a forma de adequação e de normatização;
- se há transferência ou movimentação de *hardware* entre áreas ou órgãos/entidades, seja por empréstimo, seja por doação permanente.

#### 8.5.2.1. Orientações para procedimentos relacionados à infraestrutura tecnológica

Nesta orientação técnica, destacamos os procedimentos e controles gerais necessários à identificação e preservação da infraestrutura de TI, considerando todos os equipamentos e dispositivos integrantes desta infraestrutura:

- **Localização e proteção de equipamentos**: empregar controles para viabilizar a identificação da localização dos equipamentos e a proteção de servidores, considerando os utilizados no *datacenter*, nas áreas de escritório, e os equipamentos de uso pessoal.
- **Controle de rede de telecomunicações e dados**: elaborar topologia de rede e realizar inventário dos componentes de rede, com indicação de seus proprietários e dos procedimentos adotados para a manutenção da rede.
- **Controle de recepção e descarte de equipamentos**: executar procedimentos de controle relacionados com a recepção, a classificação, a ativação e a destinação inicial dos equipamentos. Em relação à destinação final, considerar a possibilidade de reuso, venda ou quebra, como também garantir que informações residuais sejam deletadas.
- **Controle de mídias móveis**: executar procedimentos de controle do recebimento, de expedição, de proteção física, de guarda/custódia, de catalogação e de identificação (por meio de etiquetas). Realizar também o controle da quantidade de gravações já efetuadas na mídia (apenas para fitas e cartuchos magnéticos), e, quando necessário, efetuar o descarte seguro de mídias móveis de armazenamento (fitas, cartuchos, *pen-drives* e discos externos).
- **Controle de dispositivos pessoais**: executar procedimentos de cadastro, de controle de segurança e de controle de acesso aos dispositivos móveis (celulares, *tablets* e *notebooks*) de uso pessoal, mas que são autorizados a acessar a infraestrutura tecnológica do órgão ou entidade.

#### 8.5.2.2. Orientações para procedimentos relacionados a inventários manuais

Na impossibilidade de o órgão ou entidade dispor de um sistema de gestão de ativos ou de gestão de inventários, é possível realizar o procedimento de forma manual. A seguir há algumas orientações à equipe de inventário visando apoiar a execução nesse contexto.

- Garantir o recebimento de uma lista de equipamentos a serem inventariados pontualmente (servidores, *desktops*, *notebooks*, *tablets*, celulares ou equipamentos de rede).
- Solicitar, aos respectivos gestores responsáveis, acesso de leitura aos sistemas envolvidos, e acesso liberado às áreas onde, em tese, estão localizados os equipamentos.
- Identificar manualmente a localização do *hardware*, fazendo uso da lista de equipamentos preestabelecida.
- Verificar nos controles de inventário as possíveis inconsistências identificadas e relatá-las aos respectivos gestores para a tomada de providências cabíveis, que podem ser relacionadas com a desinstalação do *hardware* ou ativação do equipamento.
- Acompanhar a resolução das divergências, atualizar os controles do inventário de *hardware* e solicitar ao gestor a aprovação do novo inventário.

### 8.5.2.3. Orientações para procedimentos relacionados a inventários automatizados

Considerando que o órgão ou a entidade dispõe de um sistema de gestão de ativos ou de gestão de inventários, a seguir estão algumas orientações gerais à equipe de inventário, considerando apoiar a execução nesse contexto.

- Fazer uso da ferramenta de descoberta ativa e/ou passiva (sistema de gestão de ativos ou de inventário) para fazer o levantamento periódico dos equipamentos em rede. É pré-requisito que o sistema esteja instalado, configurado, disponível e operacional para possibilitar o acesso de leitura de toda área de controle dos equipamentos sob inventário.
- Identificar, automaticamente, todo o *hardware* conectado à infraestrutura tecnológica, fazendo uso da lista de equipamentos de *hardware* preestabelecida.
- Confrontar, automaticamente, a lista de divergências com os controles de inventário e informar, aos respectivos gestores, as possíveis inconsistências verificadas para a tomada de providências, que podem ser a desinstalação ou a ativação do *hardware* correspondente.
- Acompanhar a resolução das possíveis divergências, atualizar os controles do inventário de *hardware* e solicitar a aprovação do novo inventário.

O inventário automatizado possui diversos benefícios, como o de ser feito com maior agilidade e ter índice de acurácia superior (quando comparado ao inventário tomado de forma manual). Outro importante benefício é a possibilidade de executá-lo com mais frequência, minimizando a exposição de uso de equipamentos não autorizados.

### 8.5.2.4. Exemplos de classificação de *hardwares*

Os *hardwares* identificados devem ser classificados visando auxiliar no processo de gestão de ativos.

- Por tipo de *hardware:* servidor, *desktop*, *notebook*, disco interno, sistema de discos (bateria de discos), disco removível (gaveta), disco externo, fita, cartucho, *switch*, *router*, *modem*, *wi-fi access point*, *gateway*, *bridge*, *firewall appliance*, *load balancer*, *cache memory appliance*, *printer*, *scanner*, monitor, *mouse*, teclado, *webcam*, *headset*, microfone, processador, pente de memória, placas internas, *tablet*, celular, rádio comunicador, antena de transmissão, câmera de Circuito Fechado de TV (CFTV), sensor de presença, outros sensores, *no-break*, estabilizador etc.
- Por tipo de mídia móvel: fita carretel, cartucho magnético, HD externo, SSD HD, *removable disk drawer*, *pen-drive* ou *memory key*; cartão de memória etc.
- Por situação (estado ou *status*) – ativo: *hardware* em uso (ligado e em produção); Inativo: *hardware* desligado e sem uso etc.

A granularidade das categorias ou classificações dependerá do nível de controle que os órgãos e entidades pretendem obter como resultado do processo de inventário.

#### 8.5.2.5. *Checklist* para o inventário de *hardware*

Na execução do inventário de *hardware*, considerar a seguinte lista sugerida de verificação, para identificar nos equipamentos de TI existentes na área:

- a categoria;
- o nome do fabricante;
- o tipo e o modelo;
- o número de série;
- o MAC *address*;
- o código IMEI (*International Mobile Equipment Identity* – ou identidade internacional de equipamento móvel, em português) para equipamentos ou dispositivos móveis, como celular, *tablet* etc.
- a localização física (sala e *rack*);
- o número da etiqueta de ativo fixo;
- o órgão ou entidade a qual o equipamento pertence;
- a situação (*status*): ativo ou inativo;
- a configuração técnica;
- o(s) processador(es), considerando tipo e modelo;
- a *clock/perfomance* do(s) processador(es);
- a capacidade de armazenamento do(s) disco(s);
- o *firmware*;
- o endereço de IP (IP *address*);
- o identificador do DHCP (*Dynamic Host Configuration Protocol*);
- a arquitetura de *storage*;
- a topologia e arquitetura de redes, avaliando a necessidade de identificar várias redes relacionadas ao uso do *hardware*;
- o controle das configurações de *setup* de produção;
- a existência de contratos de manutenção e suporte;
- a existência de contratos de atualização tecnológica e extensão de garantias;
- outras informações, como: nome do proprietário/gestor/responsável, nome dos usuários designados/responsáveis, data de compra, data da ativação, valor contábil, período de depreciação etc.

**Nota:** o número de série, MAC Address, código IMEI, número de etiqueta do ativo fixo, endereço IP são únicos e não podem fazer referência a mais de um ativo. E, ainda, idealmente, as configurações técnicas e o nível de *firmware* devem ser inventariados para cada unidade de ativo.

### 8.5.3. Inventário de *software*

Um inventário de *software* atualizado proporciona aos gestores a identificação de todos os *softwares* instalados em seus equipamentos, e ajuda a identificar possíveis *softwares* maliciosos que possam ter sido instalados, evitando que comprometam a segurança de dados e informações.

O ideal é que o inventário de *software* seja realizado em conjunto com o inventário de *hardware*.

Tão importante quanto o inventário dos *softwares* instalados, é a informação sobre as licenças de cada *software*.

Todos os órgãos e entidades devem estabelecer o controle das licenças de *software*, de forma a exercerem uma gestão efetiva, visando o planejamento e a manutenção adequada das licenças. Essa ação está relacionada a licenças de *softwares* adquiridos comercialmente, com despesa sistemática para custeio das licenças. *Softwares* desenvolvidos internamente ou sob encomenda e que não possuam controle por licença devem ter classificação específica, com registro de que não há licença relacionada a eles.

O inventário de *software* deve ser capaz de identificar quais são os sistemas, aplicativos, portais e ferramentas que implementam os processos que suportam os serviços finalísticos ofertados pelos órgãos e entidades.

#### 8.5.3.1. Orientações para procedimentos relacionados a inventários manuais

Na impossibilidade de o órgão ou entidade dispor de um sistema de gestão de ativos ou de gestão de inventários, é possível realizar o procedimento de forma manual. A seguir, estão algumas orientações à equipe de inventário, visando apoiar a execução nesse contexto.

- Garantir o recebimento de uma lista prévia de sistemas a serem inventariados.
- Solicitar, aos respectivos gestores responsáveis, acesso de leitura aos sistemas envolvidos.
- Identificar manualmente a localização dos *softwares* instalados em cada equipamento, fazendo uso da lista preestabelecida.
- Levantar a situação das licenças de cada *software*, considerando identificar também os que não necessitam de licença de uso.
- Verificar nos controles de inventário as possíveis inconsistências identificadas e relatar aos respectivos gestores para a tomada de providências cabíveis, que podem ser relacionadas com a desinstalação do *software* ou adequação/contratação da licença requerida.
- Acompanhar a resolução das divergências, atualizar os controles do inventário de *software* e solicitar ao gestor a aprovação do novo inventário.

### 8.5.3.2. Orientações para procedimentos relacionados a inventários automatizados

Considerando que o órgão ou a entidade dispõe de um sistema de gestão de ativos ou de gestão de inventários, a seguir estão algumas orientações gerais à equipe de inventário, visando apoiar a execução nesse contexto.

- Fazer uso da ferramenta de descoberta ativa e/ou passiva (sistema de gestão de ativos ou de inventário) para fazer o levantamento periódico dos *softwares* instalados. É pré-requisito que o sistema esteja instalado, configurado, disponível e operacional para possibilitar o acesso de leitura.
- Validar a identificação automática de todos os *softwares* conectados à infraestrutura tecnológica, fazendo uso da lista de *softwares* preestabelecida.
- Confrontar, automaticamente, a lista de divergências com os controles de inventário e informar, aos respectivos gestores, as possíveis inconsistências verificadas para a tomada de providências, que podem ser a desinstalação do *software* ou a adequação/contratação da licença de uso.
- Acompanhar a resolução das possíveis divergências, atualizar os controles do inventário de *software* e solicitar a aprovação do novo inventário.

### 8.5.3.3. Exemplos de classificação de licenças de *software*

As classificações das licenças de *software*:

- Licença de uso (modelo *on premises*): tipo de licença em que o *software* e as suas atualizações são instalados em apenas um equipamento.
- Licença perpétua de aquisição: tipo de licença mais comumente utilizada. Ela é comercializada como uma espécie de ativo, em que uma vez adquirido, tem o direito de uso vitalício, porém sem direito às atualizações do *software*.
- Licença de suporte e manutenção: tipo de licenciamento que permite atualizações, correções de erros, manutenção e suporte ao *software*.
- Locação: tipo de licença em que o *software* fica hospedado externamente, em um equipamento ou em uma tecnologia de nuvem *(cloud)*. O aluguel pode ser anual ou mensal, conforme a necessidade.
- SaaS – *Software as a Service*: tipo de licença na qual o *software* não fica instalado na infraestrutura tecnológica dos órgãos e entidades, e as licenças são baseadas na quantidade de pessoas que acessam o serviço.
- *Software* gratuito (*freeware*): são *softwares* que podem ser utilizados sem contratação de licenças. Alguns fornecedores disponibilizam apenas algumas funcionalidades, outros, o *software* completo.
- Desenvolvimento interno ou autofinanciamento: *softwares* desenvolvidos pelos órgãos ou entidades ou em conjunto com algum parceiro.

- *Software* livre: tipo que permite o uso livre do código fonte do *software*, com autorização para atualizações ou customizações. Esse tipo difere do *software* gratuito porque há autorização expressa para a permissão de cópia por outros, mas há a exigência do reconhecimento do direito autoral do fornecedor em todas as versões, mesmo as atualizadas ou customizadas.
- *Software open source* (ou *software* de código aberto): tipo que não requer aquisição inicial de licença, porém pode ter que contratar licenças para as manutenções e atualizações do *software*. Esse tipo permite a customização do código fonte do *software*, porém o fornecedor pode determinar algumas restrições de uso.

#### 8.5.3.4. *Checklist* para o inventário de *software*

Na execução do inventário de *software*, considerar a seguinte lista sugerida de verificação:

- Para sistemas de gestão de negócios (que implementam os processos ou serviços finalísticos) identificar:
    - o nome do sistema;
    - se foi desenvolvido internamente ou se foi adquirido comercialmente;
    - no caso de ser comercial, indicar:
        - o nome do fabricante do sistema;
        - a forma de contratação do sistema.
    - se o órgão ou entidade tem acesso ao código fonte do sistema;
    - a propriedade intelectual do sistema;
    - as informações sobre licença ou sobre a não necessidade dela;
    - a quantidade de licenças contratadas e a forma de licenciamento, por exemplo, por ambientes, por usuários totais, ou por usuários ativos/concorrentes;
    - a quantidade "consumida" do licenciamento, considerando, como exemplo, um contrato que prevê 8 licenças de Oracle Database, mas apenas 6 estão efetivamente em produção ou sendo usadas nos ambientes de testes e homologação, deixando 2 licenças livres para uso futuro;
    - a quantidade disponível para uso do licenciamento (quantidade contratada menos quantidade consumida);
    - a versão do sistema e se é a mais atual e estável disponível;
    - a que órgão ou entidade pertence o *software*;
    - o nome do responsável pelo *software*;
    - se o sistema possui procedimentos de *backup* estabelecidos;
    - se o sistema possui controle das configurações de *setup*;
    - se o sistema exige autenticação de acesso por múltiplo fator;
    - a arquitetura do sistema;

- se há contratos de manutenção e suporte e de atualização tecnológica.

- Para sistemas de gerenciamento de base de dados (que armazenam os dados dos processos e dos serviços finalísticos) identificar:

  - o nome da base de dados usada pelos sistemas identificados;
  - se o SGBD foi desenvolvido internamente ou se foi adquirido comercialmente;
  - caso tenha sido adquirido comercialmente, identificar:

    - o nome do fabricante;
    - a forma de contratação.

  - as informações sobre licença ou sobre a não necessidade dela;
  - a quantidade de licenças contratadas e a forma de licenciamento, por exemplo, por ambientes, por usuários totais, ou por usuários ativos/concorrentes;
  - a quantidade "consumida" do licenciamento, considerando, como exemplo, um contrato que prevê 8 licenças de Oracle Database, mas apenas 6 estão efetivamente em produção ou sendo usadas nos ambientes de testes e homologação, deixando 2 licenças livres para uso futuro;
  - a quantidade disponível para uso do licenciamento (quantidade contratada menos quantidade consumida);
  - a versão do SGBD e se é a mais atual disponível;
  - o órgão ou entidade proprietário do sistema;
  - o nome do responsável pelo SGBD;
  - se o SGBD possui procedimentos de *backup* estabelecidos;
  - quais sistemas, portais, aplicativos e ferramentas a base atende, indicando código e nome;
  - se a base de dados possui controle das configurações de *setup*;
  - se o SGBD exige autenticação de acesso por múltiplo fator;
  - o diagrama da arquitetura da base de dados ou o modelo de entidade e relacionamento (MER).

- Para os demais *softwares* utilizados que apoiam os sistemas de gestão de negócios, identificar:

  - quantos e quais são os *softwares* existentes;
  - a categoria de tipo de *software*;
  - o nome do desenvolver/fornecedor;
  - o nome do *software*;
  - a versão vigente, considerando atualizações e modificações;
  - a data da última atualização técnica;
  - o contrato de licenciamento, identificando o número de licença, a data de contratação e a data de validade da licença;

- o nome do órgão ou entidade que adquiriu o *software*;
- o nome do responsável pelo controle da licença;
- se o *software* possui procedimentos de *backup* estabelecidos;
- a quantidade de licenças contratadas e a forma de licenciamento, por exemplo, por ambientes, por usuários totais, ou por usuários ativos/concorrentes;
- a quantidade "consumida" do licenciamento, considerando, como exemplo, um contrato que prevê 8 licenças de Oracle Database, mas apenas 6 estão efetivamente em produção ou sendo usadas nos ambientes de testes e homologação, deixando 2 licenças livres para uso futuro;
- a quantidade disponível para uso do licenciamento (quantidade contratada menos quantidade consumida);
- o arquivo com as configurações técnicas do *setup* de produção;
- se o *software* exige autenticação de acesso por múltiplo fator;
- na lista de permissões de *software* autorizado: o controle técnico com a lista de permissões de aplicações, para garantir que apenas o *software* autorizado possa ser executado ou acessado;
- na lista de permissões de bibliotecas autorizadas: o controle técnico para garantir que apenas as bibliotecas de *software* autorizadas, como arquivos .dll, .ocx, .so etc. específicos tenham permissão para ser carregados e impedir que bibliotecas não autorizadas sejam carregadas em um processo do sistema;
- na lista de permissões de *scripts* autorizados: o controle técnico com as assinaturas digitais e o controle de versão, para garantir que apenas *scripts* autorizados, como arquivos .ps1, .py etc. específicos tenham permissão para executar e bloquear a execução de *scripts* não autorizados;
- os contratos de manutenção e suporte e os contratos de atualização tecnológica e extensão de garantias;
- dados das licenças nas modalidades de contratação SaaS, como o *software* Microsoft 365;
- outras informações que a equipe de inventários achar pertinentes, por exemplo, se há usuários designados/responsáveis, procedimentos de *backup* formalizados, valor contábil, entre outras.