# Política de Gestão e Preservação de Documentos DIGITAIS




Arquivo Público DO ESTADO DE SÃO PAULO

SÃO PAULO GOVERNO DO ESTADO

2022

# Política de Gestão e Preservação de Documentos DIGITAIS

SÃO PAULO
GOVERNO DO ESTADO

## Expediente

**Governador do Estado de São Paulo**
Rodrigo Garcia

**Secretário de Estado de Orçamento e Gestão**
Nelson Luiz Baeta Neves Filho

**Coordenador do Arquivo Público do Estado de São Paulo**
Thiago Lima Nicodemo

**Diretora Técnica do Departamento de Gestão do Sistema de Arquivos do Estado de São Paulo – DGSAESP**
Ieda Pimenta Bernardes

**Diretora Técnica do Departamento de Preservação e Difusão do Acervo – DPDA**
Camila Brandi de Souza Bentes

# POLÍTICA DE GESTÃO E PRESERVAÇÃO DE DOCUMENTOS DIGITAIS

**ARQUIVO PÚBLICO DO ESTADO DE SÃO PAULO**

**SÃO PAULO**

**2022**

## Produção Editorial

**Equipe Editorial**
Flávio Ricci Arantes
Josiane Roza de Oliveira
Solange Aparecida Moraes

**Revisão de Texto**
Márcio Amêndola de Oliveira

**Direção de Arte**
Márcio Hirosse Silva Castro

**Projeto Gráfico**
Glaice Meire Machado
Márcio Hirosse Silva Castro

**Diagramação**
Glaice Meire Machado

P829 Política de gestão e preservação de documentos digitais. – São Paulo : Arquivo Público do Estado de São Paulo, 2022.
129 p.

Publicado em formato PDF.
Disponível no sítio www.arquivoestado.sp.gov.br
Inclui glossário.
ISBN 978-85-69353-12-6

1. Documento digital. 2. Patrimônio digital. 3. Gestão documental – São Paulo (Estado). 4. Preservação digital. I. Arquivo Público do Estado de São Paulo

CDD 025.84

Ficha catalográfica elaborada por
Rita de Cássia Higa do Nascimento – CRB 8/9231

Copyright (C) 2022 by Arquivo Público do Estado de São Paulo
Rua Voluntários da Pátria, 596, 02010-000 – São Paulo -SP
Tel.: 2868-4500
faleconosco@arquivoestado.sp.gov.br
www.arquivoestado.sp.gov.br

# Equipe técnica de elaboração da política

**Coordenação/APESP**
Bruno Favotto Canesin
Cintya Takahaschi
Clarissa Emi Hirao
Fernando Victor Aguiar Ribeiro
Leonardo Vaccaro
Murilo Souza dos Santos
Thiago Lima Nicodemo
Willian de Carvalho Silva

**Departamento de Gestão do Sistema de Arquivos do Estado de São Paulo-DGSAESP**
Alexandre Bianchi Oliveira
Aline Ribeiro de Farias
Benedito Vanelli do Carmo Neto
Camila Giovana Ribeiro
Carmem Lúcia Batista
Elisângela Mendes Queiroz
Ieda Pimenta Bernardes
Jorge Leite Bittencourt
Maria Elisa Pereira
Renato Soares Bastos
Uiara Maria Pereira de Araújo Oliveira

**Departamento de Preservação e Difusão do Acervo-DPDA**
Antônio Gouveia de Sousa
Camila Brandi de Souza Bentes
Carlos Henrique Metidieri Menegozzo
Fabiana Araújo Marcolino
Janaína Yamamoto Santos
Milton Ricardo Vedoato Filho
Noemi Andreza da Penha
Rodrigo Otávio Garcia
Sheila Aparecida Rodrigues Soares
Victor Souza Santos

**Membro Externo:**
Humberto Celeste Innarelli – UNICAMP - Centro de Pesquisa e Documentação Social - Arquivo Edgard Leuenroth

Camila Brandi de Souza Bentes
Camila Giovana Ribeiro
Carlos Henrique Metidieri Menegozzo
Ieda Pimenta Bernardes
Leonardo Vaccaro
Maria Elisa Pereira
Thiago Lima Nicodemo

| | |
|---|---|
| AEL/UNiCAMP | Arquivo Edgard Leuenroth da Universidade Estadual de Campinas |
| ANPD | Autoridade Nacional de Proteção de Dados |
| APESP | Arquivo Público do Estado de São Paulo |
| AtoM | *Access to Memory* (Acesso à Memória) |
| CADA | Comissão de Avaliação de Documentos e Acesso |
| CAIC | Centro de Acerco Iconográfico e Cartográfico |
| CAP | Centro de Acervo Permanente |
| CDESP | Central de Dados do Estado de São Paulo |
| CEP | Código de Endereçamento Postal |
| CGD | Centro de Gestão Documental |
| CGGDIESP | Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo |
| CGU | Controladoria-Geral da União |
| CIA | Conselho Internacional de Arquivos |
| CNPJ | Cadastro Nacional da Pessoa Jurídica |
| COETIC | Conselho Estadual de Tecnologia da Informação e Comunicação |
| CONARQ | Conselho Nacional de Arquivos |
| CP | Centro de Preservação |
| CPF | Cadastro de Pessoas Físicas |
| CPID | Centro de Processamento de Informações Digitais |
| CSBD | Catálogo de Sistemas e Bases de Dados da Administração Pública do Estado de São Paulo |
| DER | Diagramas Entidade-Relacionamento |
| DGSAESP | Departamento de Gestão do Sistema de Arquivos do Estado de São Paulo |
| DPA | *Digital Process Automation* (Automação Digital de Processos) |
| DPDA | Departamento de Preservação e Difusão do Acervo |
| e-ARQ Brasil | Modelo de requisitos para sistemas informatizados de gestão arquivística de documentos |
| FAPESP | Fundação de Amparo à Pesquisa do Estado de São Paulo |
| FCAV | Fundação Carlos Alberto Vanzolini |
| ICA | *International Council on Archives* (Conselho Internacional de Arquivos) |
| INDA | Infraestrutura Nacional de Dados Abertos |
| InterPARES | *International Research on Permanent Authentic Records in Electronic Systems Project* (Pesquisa internacional sobre documentos arquivísticos permanentes autênticos em sistemas eletrônicos) |
| ISAD | *International Standard Archival Description* (Norma Internacional de Descrição Arquivística) |
| LAI | Lei de Acesso à Informação |
| LGPD | Lei Geral de Proteção de Dados |
| LTO | *Linear Tape-Open* (Tecnologia de armazenamento de dados em fita magnética) |
| MDA | Massa Documental Acumulada |
| MDDA | Massa Documental Digital Acumulada |
| NARA | *National Archives and Records Administration* (Arquivos Nacionais e |
| NASA | Administração de Documentos - Agência norte-americana)<br>*National Aeronautics and Space Administration* (Administração Nacional do Espaço e da Aeronáutica: Agência norte-americana) |
| OAIS | *Open Archival Information System* (Sistema Aberto de Arquivamento de Informação - SAAI) |
| OCR | Reconhecimento Ótico de Caracteres |
| ONU | Organização das Nações Unidas (*United Nations* **-** *UN*) |

| | |
|---|---|
| PAI | Pacotes de Arquivamento de Informação |
| PDI | Pacotes de Disseminação de Informação |
| PEN | Processo Eletrônico Nacional |
| PGDI | Política de Governança de Dados e Informações |
| PPDP | Política de Proteção de Dados Pessoais |
| PSI | Pacotes de Submissão de Informação |
| PUA | Plataforma Única de Acesso |
| RDC | Repositório Digital Confiável |
| RDC-Arq | Repositório Arquivístico Digital Confiável |
| RG | Registro Geral (ou Carteira de Identidade) |
| SAAI | Sistema Aberto de Arquivamento de Informação (SAAI) ou *Open Archival Information System (OAIS)* |
| SAESP | Sistema de Arquivos do Estado de São Paulo |
| SEI | Sistema Eletrônico de Informações |
| SETIC | Sistema Estadual de Tecnologia da Informação e Comunicação |
| SGBD | Sistema de Gerenciamento de Banco de Dados |
| SIADS | Sistema Integrado de Administração de Serviços |
| SIAFI | Sistema Integrado de Administração Financeira |
| SIAPE | Sistema Integrado de Administração de Pessoal |
| SIASG | Sistema Integrado de Administração de Serviços Gerais |
| SIC | Serviço de Informação ao Cidadão |
| SICONV | Sistema de Gestão de Convênios e Contratos de Repasse |
| SIGAD | Sistema Informatizado de Gestão Arquivística de Documentos |
| SIGA-Doc | Sistema Integrado de Gestão Documental |
| SINAR | Sistema Nacional de Arquivos |
| SIRC | Sistema Nacional de Informações de Registro Civil |
| SISG | Sistema de Serviços Gerais |
| SP Sem Papel | Programa São Paulo Sem Papel |
| SPdoc | Sistema Informatizado Unificado de Gestão Arquivística de Documentos |
| TIC | Tecnologia da Informação e Comunicação |
| TRAC | Trustworthy Repositories Audit & Certification ou Auditoria e Certificação de Repositórios Confiáveis |
| TRF-2 | Tribunal Regional Federal da 2ª Região / RJ |
| TRF-4 | Tribunal Regional Federal da 4ª Região / RS |
| UAPESP | Unidade do Arquivo Público do Estado de São Paulo |
| UNESCO | Organização das Nações Unidas para a Educação, a Ciência e a Cultura, ou *United Nations Educational, Scientific and Cultural Organization* |
| UNICAMP | Universidade Estadual de Campinas |

**Apresentação** ..... **11**

**1. Introdução** ..... **15**

**2. Contexto** ..... **18**

**3. Compromisso institucional** ..... **22**

**4. Objetivo** ..... **24**

**5. Princípios** ..... **25**

**6. Política Estadual de Arquivos e Tecnologias da Informação e Comunicação (TIC)** ..... **26**

**7. Ambientes arquivísticos digitais confiáveis** ..... **30**

**8. Gestão de documentos digitais** ..... **32**

8.1. Produção de documentos digitais ..... **33**

8.2. Avaliação de documentos ..... **35**

8.3. Eliminação de documentos digitais ..... **38**

**9. Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD) e Sistemas de Negócio** ..... **41**

9.1. Programa São Paulo Sem Papel ..... **43**

**10. Governança e gestão de dados públicos** ..... **46**

10.1. Política de dados abertos ..... **49**

10.2. Proteção de dados pessoais ..... **52**

**11. Preservação de documentos digitais** ..... **54**

11.1. Repositório Arquivístico Digital Confiável (RDC-Arq) ..... **57**

11.2. Gestão do repositório arquivístico digital confiável e plano de preservação ..... **61**

11.3. Ingresso de documentos em Repositório Arquivístico Digital Confiável ..... **62**

11.4. Admissão ..... **65**

11.5. Arquivamento ..... **69**

11.6. Disseminação ..... **72**

11.7. Armazenamento, cópias de segurança e backup ..... **73**

11.8. Digitalização do acervo de guarda permanente ..... **77**

11.9. Automação digital ..... **79**

**12. Segurança da informação e gestão de riscos** ..... **85**

**13. Acesso à informação** ..... **90**

**14. Glossário** ..... **95**

**Referências** ..... **114**

# Apresentação

O Arquivo Público do Estado de São Paulo (APESP), órgão central do Sistema de Arquivos do Estado de São Paulo (SAESP), está comprometido em buscar soluções técnicas e sustentáveis que apoiem a transição para um governo digital. Este compromisso inclui a preservação do patrimônio arquivístico digital, considerando o risco iminente de desaparecimento e a falta de confiabilidade do legado digital produzido no país e, em particular, no Estado de São Paulo.[1] Inclui também um compromisso vigilante com a transparência e com a proteção e sigilo sistêmico de dados, documentos e informações. Na medida em que sociedade e Estado se digitalizam, cada vez mais impõe-se também a tarefa de criar condições para um uso responsável e inteligente dos dados de Estado para aprimoramento dos serviços e das próprias políticas públicas. Trata-se de consolidar uma concepção republicana e democrática em que as informações que o Estado produz e tramita sejam utilizadas em prol do interesse coletivo e da construção de uma sociedade melhor.

Tendo em vista esse grande objetivo, apresentamos a *Política de Gestão e Preservação de Documentos Digitais*. Este documento técnico é resultado de um longo trabalho encampado como prioridade de Estado desde o ano de 2021. Como parte do Plano de Metas do Governo do Estado de São Paulo, a instituição aprovou o Programa "ArquivoDigital.SP", por meio da Portaria UAPESP/SAESP nº 2/2021, que tem como objetivo planejar, desenvolver e implementar ações de gestão, preservação e acesso a documentos, dados e informações digitais no âmbito da Administração Pública Estadual. Desde então, e ao longo desses dois anos de trabalho, o corpo técnico da instituição, dezenas servidores e de suas equipes, vêm trabalhando de forma multidisciplinar e transversal na definição de políticas, requisitos e metadados para orientar a produção, digitalização, contratação de serviços de digitalização, construção de repositórios arquivísticos digitais confiáveis, e também de processos para a captura, gestão, preservação e acesso aos documentos digitais, dentre outros.

Parte dessas entregas foram apresentadas no dia 17 de novembro de 2022, por ocasião das comemorações dos 130 anos do Arquivo Público do Estado. A instituição inaugurou o projeto piloto de construção de um "Repositório Arquivístico Digital Confiável (RDC-Arq)", propondo uma solução tecnológica segura para a

1 A "Carta para a Preservação do Patrimônio Digital" da Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO), de 2003, manifesta a necessidade dos Estados-membros, entre os quais se insere o Brasil, estabelecerem políticas e ações para proteger o patrimônio digital. Em 2004, motivada pela iniciativa da UNESCO, a Câmara Técnica de Documentos Eletrônicos do CONARQ elaborou a "Carta Brasileira para a Preservação do Patrimônio Arquivístico Digital" (CONARQ, 2005).

preservação de documentos digitais permanentes, o que exige um compromisso de longo prazo para sua expansão e evolução. Além de um repositório que cumpra os requisitos necessários para a guarda dos documentos nato-digitais produzidos pela administração pública paulista e para armazenar os representantes digitais advindos do nosso acervo histórico, oferecemos também ao público uma plataforma de acesso unificado, operada pelo sistema AtoM.

Esse conjunto de esforços conflui naquilo que denominamos Arquivo Público Digital do Estado de São Paulo.[2] Não apenas uma porta de acesso única aos documentos digitalizados do nosso acervo, mas um vetor que complementa e expande a política estadual de arquivos no universo digital. Seja preservando o nosso acervo histórico digitalizado, seja extraindo e consolidando informações estratégicas de documentos digitalizados, de modo a produzir uma base de dados cada vez mais rica e interconectada, seja preservando digitalmente acervos físicos cuja custódia não é nossa, seja sistematizando e centralizando informações de acesso a outros acervos, complementares àqueles sob a nossa custódia.

A *Política de Gestão e Preservação de Documentos Digitais* foi construída por muitas mãos e em camadas que se acumulam no tempo. Suas bases deitam raízes não apenas na fundação do Arquivo Público do Estado de São Paulo, há 130 anos, em 1892, mas também na criação de um Sistema de Arquivos Estadual, em 1984, e na consolidação da gestão documental no Estado, que ocorreu progressivamente, especialmente a partir de 2004. Como veremos mais adiante a preocupação com o digital vem desde, pelo menos, 2009, com a importante Instrução Normativa APE/SAESP nº 1/2009, mas se adensou com a adoção de um sistema de Gestão de Documentos nato-digitais, o bem-sucedido São Paulo Sem Papel, em 2019, instituído pelo Decreto nº 64.355, que tem como objetivo assegurar a produção, gestão, tramitação, armazenamento, preservação, segurança e acesso aos documentos e informações arquivísticas em ambiente digital; bem como com um conjunto de normas complementares, tais como a da Portaria UAPESP/SAESP nº 5/2021, que trata da digitalização documental e a Portaria UAPESP/SAESP nº 10/2022, que regula a eliminação, transferência ou recolhimento de documentos digitais aos repositórios arquivísticos digitais confiáveis do APESP. Certamente, esse processo de produção de normas vai continuar nos próximos meses e anos, o que nos ajuda a imaginar o papel estratégico que os arquivos públicos podem e devem ter junto aos governos, municipais, estaduais e o federal.

Por isso, é necessário não apenas fomentar a produção acadêmica e científica da área e um diálogo profícuo com iniciativas similares de instituições arquivísticas e de pesquisa, mas também compartilhar conhecimentos e experiências acumulados pelo Arquivo Público do Estado ao longo dos últimos trinta e oito anos

2 O Arquivo Público Digital do Estado de São Paulo está disponível em: http://atom.arquivoestado.sp.gov.br. Acesso em: 12 dez. 2022.

na implementação do Sistema de Arquivos do Estado de São Paulo (SAESP). Também é possível imaginar que os Arquivos Públicos, em especial o do Estado de São Paulo, se coloquem como instituições educativas, polos de formação, inovação e, porque não, de pesquisa. Não se trata aqui de exercitar a imaginação, mas de reconhecer algo que já é nossa realidade, haja vista a quantidade e a qualidade dos cursos, eventos e textos que publicamos ao longo de todos esses anos.

Sendo assim, o texto aqui apresentado tenciona presente e futuro. Ao mesmo tempo que sistematiza as normas vigentes a respeito da gestão da informação em formato digital, nos direciona para onde ainda devemos nos aprimorar. Muitas camadas de normas e de estudos o precederam assim como muitas camadas de normas e de conhecimentos devem ser produzidas a partir dele. Trata-se então de um compromisso para com o futuro, de uma agenda propositiva do Arquivo Público para com o Estado e do Estado para com a sociedade. Devemos, portanto, zelar pela continuidade desse trabalho com ininterrupto investimento, não só em infraestrutura, mas sobretudo na capacitação técnica dos servidores. A transformação digital é um processo irreversível e devemos estar cada vez mais bem preparados para dar conta desse desafio.

O contexto de produção desse documento foi o de uma corrida global de arquivos e outras instituições para buscar soluções sustentáveis para a preservação do patrimônio digital, nato-digital e daquilo que é digitalizado. Muitos arquivos, museus e universidades pelo mundo decidiram investir o seu tempo e recursos na elaboração de documentos norteadores entendidos como “políticas de preservação”. Ao longo desse percurso nos beneficiamos da interlocução com muitas dessas instituições e seus atores, e aqui fica nosso agradecimento à Universidade Estadual de Campinas, da qual sou orgulhosamente docente, à Universidade de São Paulo e à Universidade Estadual Paulista, ao Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT), como também à Pinacoteca de São Paulo, ao SESC, à Fundação Oswaldo Cruz, ao Arquivo Nacional, ao Archivo Nacional de Chile e ao Instituto Moreira Salles. No entanto, há de se reconhecer que o documento ora apresentado não se parece com qualquer uma das “Políticas de Preservação” até agora publicadas ou em elaboração. O desafio que encampamos foi o de equacionar a necessidade de estabelecer procedimentos e compromissos sustentáveis com a preservação do patrimônio documental digital e com a necessidade de reforçar e aparelhar a gestão documental sistêmica, de modo que o que está estabelecido neste texto deve ter igual validade para os procedimentos internos do APESP, bem como para a administração pública paulista em toda a sua imensa extensão.

Por fim, fica um agradecimento enfático a todos e todas servidoras do Arquivo Público do Estado de São Paulo que contribuíram com a realização desse

projeto, que enfrentaram o desafio de lidar com a transversalidade do problema do digital, superando as fronteiras do conhecimento da sua área de origem, enfrentando a sobrecarga de trabalho gerada pela própria importância estratégica que ganham esses novos saberes no mundo contemporâneo. Graças a vocês, no aniversário de 130 anos da instituição podemos comemorar não apenas o que foi feito até aqui, mas imaginar como será um porvir no qual o Arquivo Público continue cumprindo papel estratégico para o Estado em preservar e respeitar sua memória, bem com na criação de soluções para que os dados, documentos e informações possam ser usados visando o interesse público e o bem comum.

**Thiago Lima Nicodemo**
Coordenador do Arquivo Público do Estado de São Paulo

# 1 Introdução

Esta *Política de Gestão e Preservação de Documentos Digitais* sistematiza todo o trabalho técnico desenvolvido pela instituição. A partir dela, a instituição firma seu compromisso com a gestão, preservação e acesso aos documentos, dados e informações produzidos e armazenados em ambiente digital pelos órgãos e entidades estaduais no exercício de suas funções e atividades governamentais, bem como com a modernização, eficiência e transparência da Administração Pública Estadual e, também, com a expansão e aprimoramento do Programa "SP Sem Papel", instituído pelo Decreto nº 64.355/2019, que tem como objetivo assegurar a produção, gestão, tramitação, armazenamento, preservação, segurança e acesso aos documentos e informações arquivísticas em ambiente digital.

Este documento pretende conciliar e integrar os objetivos maiores do Sistema de Arquivos do Estado de São Paulo - SAESP com os desafios propostos pela política de gestão documental e de preservação digital. Assim, as normas, procedimentos e fluxos internos da instituição ganham capilaridade para alcançar também os órgãos e entidades estaduais que integram o SAESP.

Nesse sentido, os dois pilares desta Política - a **gestão** e a **preservação de documentos digitais** – foram tratados em capítulos específicos, mas pensados de forma articulada e em constante diálogo com outros temas transversais - a incorporação das TIC aos processos de produção, armazenamento e preservação de documentos, dados e informações, e a promoção do acesso à informação, bem como a proteção de dados.

Por outro lado, a instituição compromete-se com o grande desafio da contemporaneidade devidamente analisado no Capítulo sobre "Governança e gestão de dados públicos", que aponta a necessidade da integração e colaboração entre os diversos atores envolvidos no processo, bem como a clara definição de seus papéis e responsabilidades. A esse propósito, indica a função estratégica dos Arquivos Públicos, que têm a expertise na implementação de políticas arquivísticas, para colaborar também com a gestão e a preservação dos dados governamentais.

Por sua complexidade e extensão, as questões afetas à governança e gestão de dados foram abordadas em dois ângulos diferentes, porém complementares. Um deles ficou registrado no Capítulo sobre a "Política de dados abertos" no qual foi tratada a importância da abertura dos dados para o acompanhamento e controle das ações governamentais, bem como para o reuso e cruzamento de dados visando a realização de estudos e o desenvolvimento de novas ferramentas tecnológicas

e sistemas de informação. O outro foi abordado no Capítulo sobre "Proteção de dados pessoais", que apresenta a importância da definição de critérios técnicos e objetivos para o tratamento de dados pessoais, tal como proposto pela Lei Geral de Proteção de Dados (LGPD), mas de forma harmônica e integrada com as disposições da Lei de Acesso à Informação (LAI) e da Lei de Arquivos nº 8.159/1991.

O Capítulo sobre "Política estadual de arquivos e Tecnologias de Informação e Comunicação" (TIC) aponta a necessária integração entre as políticas arquivísticas e as TIC para dar suporte e segurança aos processos de transformação digital.

O "Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD) e Sistemas de Negócio" demonstra que o sucesso de um SIGAD depende, fundamentalmente, da implementação de uma política de gestão documental e da incorporação à ferramenta tecnológica de planos de classificação e de tabelas de temporalidade. Fica, portanto demonstrado, que a evolução tecnológica de um SIGAD deve espelhar necessariamente o aprimoramento, a expansão e a consolidação da política de gestão documental.

O APESP, no exercício de suas atribuições, tem enfrentado os desafios colocados pela dimensão digital da informação, que envolve a informação em si, contida em bancos de dados e documentos arquivísticos digitais, mas que abarca também atividades específicas, agentes especializados e tecnologias apropriadas. Para que esta instituição prossiga em sua missão arquivística plenamente adaptada ao governo digital, são necessários alguns requisitos indispensáveis para o bom desenvolvimento de suas competências.

Em primeiro lugar, as pessoas. Pensar a transformação digital depende da confluência de várias formações e de diversas competências. O APESP vem sendo um território fértil para o desenvolvimento e aprendizado, de modo que nossos atuais profissionais da instituição vêm se aprimorando em competências que envolvem saberes do campo da Arquivologia, da Ciência da Informação, da Biblioteconomia, das Humanidades, em particular, da História e das Ciências Sociais, bem como da Tecnologia da Informação e Comunicação (TIC), e têm dado o seu melhor ultrapassando não só seus limites, mas também fazendo a instituição avançar nessa seara tão disputada entre órgãos e entidades estaduais, que é a do controle da informação. Mesmo assim, apesar de todo arrojo e comprometimento desse pequeno grupo de pessoas, é necessário constituir uma equipe bem maior e mais bem remunerada - este último ponto é muito importante, pois o APESP tem se tornado, infelizmente, local de passagem para profissionais que saem em busca de oportunidades mais justas e compatíveis às suas atribuições.

Em segundo, a estrutura organizacional adequada. O APESP precisa estar preparado para o futuro, e no mundo digital o futuro é agora. Mesmo mantendo

suas atividades tradicionais de arquivo de documentos não digitais, a instituição precisa também orientar toda a administração paulista, bem como nosso parceiro tecnológico - a PRODESP - para a execução de ações de gestão e preservação digital, e ainda contribuir para a implementação e aprimoramento de ferramentas digitais, como o SP Sem Papel. Entre as ações estratégicas da maior relevância, no momento, é preciso assegurar que o APESP esteja vinculado às mais altas estruturas da Administração Paulista, como a Casa Civil ou a Secretaria de Governo, e desenvolver esforços para robustecer o seu organograma interno na área de serviços digitais voltados à Administração Pública e ao cidadão, fortalecendo também seu setor de tecnologia da informação a fim de responder às novas necessidades da instituição e do Estado.

Por fim, para que o APESP cumpra adequadamente sua missão institucional no âmbito de um governo digital, é necessário garantir à instituição os melhores e mais avançados recursos tecnológicos disponíveis, inclusive soluções colaborativas e *softwares* livres - não proprietários - seguros e recomendados. Dessa maneira, o APESP poderá responder às novas e desafiadoras demandas governamentais, orientar os servidores estaduais, e implementar políticas capazes de garantir a gestão, preservação e acesso aos documentos, dados e informações governamentais.

# 2 Contexto

Criado oficialmente em 1892, o Arquivo Público do Estado (APESP) é uma das instituições mais antigas do estado de São Paulo. Seu acervo permanente, com aproximadamente 11.000 metros lineares (m) de documentos textuais, bem como cerca de 2.600 metros lineares (m) de documentos cartográficos, e mais de 1.100 metros lineares (m) de documentos iconográficos, e pouco mais de 3.400 metros lineares (m) de acervo bibliográfico e hemerográfico (volumes de livros, títulos de jornais e revistas), além de cerca de 124 TB - Terabytes de representantes digitais recolhidos, aos quais somam-se ainda a 9.908 metros lineares (m) de acervo intermediário, constituído por documentos de órgãos e entidades da Administração Pública paulista, e por documentos privados de pessoas físicas ou jurídicas declarados de interesse público e social.

O APESP é a instituição arquivística do Poder Executivo paulista que atua como órgão central do Sistema de Arquivos do Estado de São Paulo (SAESP), criado pelo Decreto nº 22.789/1984, com competência para formular e implementar a política estadual de arquivos, por meio da gestão documental, da preservação de acervos de guarda permanente (ou históricos), da difusão do patrimônio documental e do acesso à informação.[3]

O Decreto que instituiu o SAESP visa promover a gestão documental, preservar o patrimônio arquivístico estadual e assegurar o direito de acesso aos documentos públicos estaduais, antecipando-se, de forma pioneira, à Constituição Federal de 1988, à Lei Federal de Arquivos nº 8.159/1991 e à Lei Federal de Acesso à Informação (LAI) nº 12.527/2011.

A Constituição Federal (BRASIL, 2022a) fortaleceu o SAESP e a política estadual de arquivos ao determinar a obrigação da administração pública em promover "a gestão da documentação governamental e as providências para franquear sua consulta a quantos dela necessitem" (§ 2º, art. 216). A Lei de Arquivos (nº 8.159/1991) regulamentou o dever do poder público de promover a "gestão documental e a proteção especial a documentos de arquivos, como instrumento de apoio à administração, à cultura, ao desenvolvimento científico e como elementos de prova e informação" (art. 1º); ainda, assegurou o direito de todos receberem dos órgãos públicos informações de seu interesse particular ou de interesse coletivo

3 Desde 2007 o APESP fez parte da estrutura da Casa Civil pelo Decreto nº 51.991. Em 2015 passou para estrutura da Secretaria de Governo pelo Decreto 61.035. Com o Decreto nº 64.998/2020, o Arquivo Público do Estado foi transferido da Secretaria de Governo para a Secretaria de Projetos, Orçamento e Gestão e, a seguir, pelo Decreto nº 66.017/2021, foi transferido para a Secretaria de Orçamento e Gestão, mantendo suas atribuições e estrutura organizacional definidas pelo Decreto nº 54.276/2009.

ou geral, contidas em documentos de arquivos (art. 4º). Mais recentemente, a LAI avançou ao definir mecanismos, procedimentos e prazos para efetivamente viabilizar o direito de acesso à informação.

Na administração pública estadual, a política arquivística também foi impulsionada pelo Decreto nº 48.897/2004, que orientou a elaboração de planos de classificação e de tabelas de temporalidade, e definiu normas para a avaliação, guarda e eliminação de documentos, independentemente do suporte de registro das informações. O Decreto nº 48.898/2004, atualizado pelo Decreto nº 63.382/2018, aprovou o Plano de Classificação e a Tabela de Temporalidade de Documentos da Administração Pública do Estado de São Paulo: Atividades-Meio, que consolidou uma metodologia de avaliação funcional e definiu critérios técnicos para a eliminação segura de documentos públicos.

A ampliação das atividades de implementação do SAESP demandou uma estrutura organizacional do APESP mais compatível para o desempenho das atribuições de órgão central. Por essa razão, sua estrutura interna foi ampliada e aprimorada pelos Decretos estaduais nº 50.659/2006, nº 50.941/2006, nº 54.276/2009 e nº 64.355/2019.

A necessidade de prestar orientação técnica aos órgãos integrantes do SAESP para a produção, gestão e preservação de documentos digitais, levou o APESP à realização de estudos e pesquisas que resultaram na publicação da Instrução Normativa APE/SAESP nº 1/2009, revista e atualizada pela Portaria UAPESP/SAESP nº 4/2020, considerada o marco regulatório do tema no âmbito da administração pública estadual.

A instituição vem se destacando nacionalmente por sua atuação normativa na formulação da política arquivística estadual, por seu programa de publicações técnicas e pela coordenação do funcionamento do SAESP, que inclui orientação técnica e capacitação permanente dos órgãos e entidades estaduais para a aplicação dos instrumentos de gestão documental, e para a realização das atividades de eliminação de documentos, transferências e recolhimentos.

O APESP teve e continua a ter um papel de vanguarda na implementação de ações rotineiras de monitoria e fiscalização da política arquivística, de assistência técnica às administrações municipais, na padronização de normas e procedimentos de protocolo, em conformidade com os requisitos arquivísticos, e na definição de uma metodologia ágil para a avaliação da massa documental acumulada (ARQUIVO PÚBLICO DO ESTADO, 2022a).

A instituição também é reconhecida por seu protagonismo no desenvolvimento, administração e implantação progressiva do Sistema Informatizado Unificado de Gestão Arquivística de Documentos, o SPdoc,[4] na regulamentação da

4 O SPdoc é uma aplicação web que permite a gestão de documentos, expedientes e processos produzidos em papel, em tramitação ou arquivados (Decreto nº 63.936/2018). Atualmente, o sistema está operação em 27 órgãos e entidades da administração pública estadual.

LAI, por meio da elaboração do Decreto estadual nº 58.052/2012, e na implantação do processo eletrônico no âmbito da administração pública estadual, por meio do Programa São Paulo Sem Papel, instituído pelo Decreto nº 64.335/2019. Este último decreto, inclusive, criou o Centro de Gestão e Preservação de Documentos Digitais na estrutura do APESP para apoiar o aprimoramento do sistema de produção e gestão de documentos digitais e torná-lo mais aderente às regras arquivísticas.

Para o SP Sem Papel, a ferramenta adotada foi o Sistema Integrado de Gestão Documental (SIGA-Doc), um *software* livre, com possibilidade de alteração, distribuição e modificação, desenvolvido pelo Tribunal Regional Federal da 2ª Região / RJ (TRF-2), por melhor atender ao arcabouço jurídico e normativo que constitui a Política Estadual de Gestão de Documentos e Acesso à Informação, pois permite o gerenciamento da produção, tramitação e arquivamento dos documentos digitais produzidos pelos órgãos e entidades estaduais no exercício de suas atividades.

Ao longo do tempo, o APESP buscou parcerias inusitadas que contribuíram para o seu fortalecimento institucional e para a implementação de ações e programas estratégicos. Nesse contexto, merecem destaque as cooperações técnicas, em especial aquelas firmadas com o Ministério Público Estadual no ano 2000, renovada em 2009, e com o Tribunal de Contas do Estado de São Paulo, no ano de 2018, visando à efetiva aplicação da legislação arquivística e de acesso à informação, bem como a defesa do patrimônio documental do Estado.

A propósito, o APESP passou a atuar como órgão técnico consultivo desses órgãos de controle externo, inclusive atendendo a eventuais requisições de perícias na área arquivística junto às administrações municipais. Dentre as ações mais exitosas dessas parcerias, merecem destaque os "Encontros Paulistas sobre Gestão Documental e Acesso à Informação", que se encontram em sua 26ª edição e a publicação conjunta do "Guia Técnico de Transparência Municipal" (ARQUIVO PÚBLICO DO ESTADO, TRIBUNAL DE CONTAS DO ESTADO, 2018a).

Na atualidade, a instituição está atenta e comprometida com as demandas desafiadoras trazidas pela transformação digital, pela utilização crescente das TIC para a execução de funções de atividades governamentais e para a prestação de serviços públicos.

Tais mudanças têm ocasionado sérios impactos na gestão pública, alterado rotinas, procedimentos administrativos e a forma de criação de documentos, dados e informações governamentais, doravante produzidos, geridos e armazenados em complexos ambientes digitais.

Por essa razão, o tema foi amplamente debatido por ocasião da elaboração do Plano Diretor do APESP (ARQUIVO PÚBLICO DO ESTADO, 2019) e vem sendo aprofundado no escopo do Programa "ArquivoDigital.SP", criado por meio da Portaria UAPESP/SAESP nº 2/2021, que instituiu Grupo de Trabalho – que conta com colaboração do AEL/UNICAMP - com o objetivo de planejar, desenvolver e

implementar ações de gestão, preservação e acesso de documentos, dados e informações digitais no âmbito da Administração Pública Estadual.

Por todo o exposto, o APESP apresenta esta *Política de Gestão e Preservação de Documentos Digitais*, que pretende proteger e preservar o patrimônio digital do Estado de São Paulo, garantindo sua autenticidade, integridade, confidencialidade e confiabilidade para o acesso imediato e futuro, visando promover as pesquisas públicas e a produção de conhecimento, assegurar o exercício de direitos dos cidadãos e ampliar a transparência da gestão pública.

# 3 Compromisso institucional

O APESP conta com um complexo arcabouço legal que regula suas atribuições e responsabilidades,[5] bastante ampliadas pelos desafios da governança digital. Também vem se destacando pela edição de normas e procedimentos técnicos sobre os mais variados aspectos da política arquivística, seguida de ações permanentes para a capacitação de servidores estaduais e municipais e para a disseminação ampla do conhecimento arquivístico.

Em decorrência dessas conquistas, o APESP vem realizando um amplo esforço institucional para assegurar a efetividade da política arquivística de documentos e informações por meio do exercício concreto de suas competências e a aplicação prática dessas normas técnicas pelos órgãos e entidades da administração pública estadual.

Nesse sentido, o APESP está comprometido em consolidar-se como instituição inovadora e de referência, imprescindível às decisões governamentais, ao exercício dos direitos dos cidadãos, à promoção da memória, eficiência e transparência da gestão pública, e à construção de uma ampla política de governança digital.

Por isso, a instituição assume o compromisso de desenvolver ações integradas com os demais órgãos e entidades da administração pública estadual e buscar intercâmbio e parcerias com outras instituições arquivísticas e de gestão de documentos e informações públicas, institutos de pesquisa, universidades, em âmbito nacional e internacional, para que:

- A legislação e as normas técnicas arquivísticas sejam conhecidas e aplicadas no âmbito da Administração Pública Estadual;

- A gestão e a preservação de documentos, dados e informações digitais sejam realizadas com responsabilidade por todos os órgãos e entidades estaduais;

- Sejam investidos os recursos necessários para apoiar a adequada gestão, preservação e segurança de documentos digitais, especialmente para garantir a infraestrutura tecnológica adequada e sua permanente atualização, bem como para promover a capacitação de servidores;

- Os documentos, dados e informações digitais sejam geridos e preservados no âmbito governamental de forma a garantir o seu

5 O Arquivo Público do Estado já publicou dez Portarias e quatro Instruções Normativas, e colaborou na elaboração de mais de vinte Decretos e de uma Lei. Estes atos legais estão disponíveis em: http://www.arquivoestado.sp.gov.br/uploads/publicacoes/livros/Politicas_Publicas_3ed.pdf . Acesso em: 22 dez. 2022.

contexto original de produção, sua autenticidade, integridade, confidencialidade, confiabilidade e acesso, ao longo do tempo;

- Os documentos, dados e informações digitais, no âmbito governamental, sejam acessíveis a todos, respeitando-se a legislação pertinente e os direitos dos indivíduos, produtores e usuários;

- Os documentos, dados e informações digitais sejam utilizados de modo a contribuir para o aprimoramento e implementação de políticas públicas, para a promoção de uma cidadania responsável, e para a produção de conhecimento científico;

- As políticas de gestão e preservação digital sejam consideradas políticas de Estado com garantia de continuidade e investimentos permanentes.

# 4 Objetivo

O objetivo da *Política de Gestão e Preservação de Documentos Digitais* é orientar ações permanentes para a implementação da gestão e preservação de documentos, dados e informações digitais, sejam eles nato-digitais ou digitalizados, mantendo sua autenticidade, integridade, confidencialidade e confiabilidade ao longo do tempo.

Para alcançar esse objetivo, é indispensável uma política de estado com planejamento estratégico, sustentação legal, mudança de cultura organizacional, investimento contínuo na infraestrutura tecnológica e educação continuada de servidores.

# 5 Princípios

A *Política de Gestão e Preservação de Documentos Digitais*, tem como fundamentos os parâmetros técnicos consagrados pela comunidade arquivística nacional e internacional. Por essa razão, o APESP segue as orientações do Projeto InterPARES, do Conselho Internacional de Arquivos (CIA) e do Conselho Nacional de Arquivos (CONARQ). As definições e procedimentos adotados estão em conformidade com as normativas específicas da política estadual de arquivos, em especial com a Instrução Normativa APE/SAESP nº 1/2009, atualizada pela Portaria UAPESP/SAESP nº 4/2020.

A propósito, o APESP entende que:

- uma política de Estado voltada para a gestão e preservação de documentos, dados e informações digitais é necessariamente multidisciplinar e multissetorial, e certamente tem maior eficácia se resultar de ações articuladas entre os vários atores governamentais envolvidos no processo de transformação digital;

- essa política possui custos progressivos e deve ser apoiada por investimentos governamentais de longo prazo que lhe permitam manter-se e conservar-se ao longo do tempo, com sustentabilidade financeira e institucional, atualização permanente da infraestrutura tecnológica e capacitação profissional continuada;

- a política estadual de arquivos e a articulação do APESP com os órgãos setoriais do SAESP é a base segura para a implementaçãoda gestão e preservação digital em âmbito estadual;

- a produção e a gestão de documentos digitais devem ser controladas por sistema informatizado de gestão arquivística de documentos e informações (SIGAD), em conformidade com a política estadual de arquivos;

- a preservação digital deve ser assegurada por custodiadores de confiança, capazes de garantir a autenticidade dos documentos, dados e informações digitais recolhidos em repositórios arquivísticos digitais confiáveis;

- a política de gestão e preservação digital deve contar com mecanismos que promovam o acesso às informações, visando a construção de uma administração pública mais eficiente, responsável e transparente.

# 6 Política Estadual de Arquivos e Tecnologias da Informação e Comunicação (TIC)

No mundo contemporâneo, as TIC têm um papel essencial na gestão pública na busca pela eficiência, eficácia, efetividade, economicidade, melhoria de processos de trabalho e de qualidade na prestação de serviços.

Nesse contexto, observa-se a progressiva incorporação das TIC na implementação de políticas arquivísticas, impondo desafios relacionados à segurança, produção, gestão e preservação da autenticidade, integridade, confidencialidade e confiabilidade de documentos, dados e informações digitais produzidos e armazenados ao longo do tempo.

Por isso, torna-se cada vez mais estratégica e necessária a atuação de instituições arquivísticas na definição de políticas, normas, procedimentos e requisitos arquivísticos, nos processos de produção, gestão, armazenamento, preservação, segurança e acesso ao patrimônio arquivístico digital.

No cenário nacional, o Conselho Nacional de Arquivos (CONARQ) publicou normativas específicas para orientar os órgãos integrantes do Sistema Nacional de Arquivos (SINAR) para realizar o tratamento de documentos digitais, em especial, as Resoluções CONARQ nº 20/2004, que dispõe sobre a inserção dos documentos digitais em programas de gestão arquivística de documentos dos órgãos e entidades integrantes do Sistema Nacional de Arquivos; nº 24/2006, que estabelece diretrizes para a transferência e recolhimento de documentos arquivísticos digitais para instituições arquivísticas públicas; nº 31/2010, que dispõe sobre a adoção das Recomendações para Digitalização de Documentos Arquivísticos Permanentes; nº 37/2012, que aprova as Diretrizes para a Presunção de Autenticidade de Documentos Arquivísticos Digitais; nº 38/2013, que dispõe sobre a adoção das "Diretrizes do Produtor - A Elaboração e a Manutenção de Materiais Digitais: Diretrizes Para Indivíduos" e "Diretrizes do Preservador - A Preservação de Documentos Arquivísticos Digitais: Diretrizes para Organizações"; nº 39/2014, que estabelece diretrizes para a implementação de repositórios arquivísticos digitais confiáveis

para a transferência e recolhimento de documentos arquivísticos digitais para instituições arquivísticas dos órgãos e entidades integrantes do Sistema Nacional de Arquivos (SINAR), alterada pela Resolução nº 43/2015; nº 48/2021, que estabelece diretrizes e orientações aos órgãos e entidades integrantes do Sistema Nacional de Arquivos quanto aos procedimentos técnicos a serem observados no processo de digitalização de documentos públicos ou privados; e nº 50/2022, que dispõe sobre a Versão 2 do e-ARQ Brasil, o Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos.

Em âmbito estadual, considerando a adoção progressiva de práticas digitais pela administração paulista, o APESP vem apoiando o governo na transição segura para uma administração sem papel, disponibilizando seus conhecimentos e experiências de órgão central do Sistema de Arquivos do Estado (SAESP) para assegurar sustentação legal e técnica ao processo, visando controlar os riscos decorrentes da degradação do suporte e da obsolescência tecnológica.

Apesar de ações anteriores direcionadas para a digitalização de acervos permanentes custodiados pelo APESP e do desenvolvimento de ferramentas informatizadas de controle de acervos, a primeira iniciativa da instituição para a incorporação dos documentos digitais à política estadual de gestão de documentos foi o trabalho de definição de diretrizes e procedimentos para a gestão, preservação e acesso contínuo aos documentos arquivísticos digitais da administração pública estadual direta e indireta, que resultou na Instrução Normativa APE/SAESP nº 1/2009, revista e atualizada pela Portaria UAPESP/SAESP nº 4/2020.

A Instrução Normativa APE/SAESP nº 1/2009 orienta os órgãos integrantes do SAESP para a utilização de programas, estratégias, ações e técnicas de preservação e segurança digital para garantir a manutenção e atualização contínua do ambiente tecnológico, define os requisitos a serem utilizados por sistema de gestão arquivística de documentos, e orienta a adoção de metadados para documentos digitais, a fim de apoiar sua identificação, indexação, presunção de autenticidade, preservação e interoperabilidade.

Importante destacar que, em seguida, foi realizado um importante esforço de aplicação prática daquela primeira Instrução Normativa no desenvolvimento do sistema SPdoc,[6] uma solução corporativa de governo, concebida inicialmente como protocolo único, adotada pela administração pública estadual para a gestão arquivística de documentos, expedientes e processos físicos.[7]

A partir de 2017, a instituição realizou testes para selecionar uma ferramenta gratuita para produção e gestão de documentos digitais que fosse a mais aderente possível aos parâmetros estabelecidos pela política estadual de arquivos, o que

6 As informações sobre o SPdoc estão disponíveis em: http://www.arquivoestado.sp.gov.br/web/gestao/sistema/spdoc. Acesso em: 12 dez. 2022.

7 O SPdoc está disponível em: www.sistema.spdoc.sp.gov.br. Acesso em: 12 dez. 2022.

resultou na adoção do Sistema Integrado de Gestão Documental (SIGA-Doc) para integrar o Programa SP Sem Papel, instituído em 2019. Desde então, o APESP vem atuando na implementação e capacitação de servidores, na análise de requisitos e na elaboração de regras de negócio, parametrização e aprimoramento tecnológico do sistema, mapeamento e modelagem de documentos.

Para orientar o uso do ambiente digital de gestão documental do Programa SP Sem Papel, o APESP publicou um manual por meio da Resolução SG nº 57/2019, atualizado pela Portaria UAPESP/SAESP nº 3/2020. Considerando as demandas dos usuários, o APESP também publicou a Portaria UAPESP/SAESP nº 6/2021 para definir procedimentos e orientar o mapeamento de documentos compostos e a modelagem de documentos digitais.

Em decorrência das alterações promovidas nas leis federais nº 12.682/2012 e nº 13.874/2019, foi editada a Portaria UAPESP/SAESP nº 5/2021 para orientar sobre a digitalização de documentos públicos, a gestão e a preservação de seus representantes digitais para que produzam os mesmos efeitos legais de documentos originais.

Atualmente, o APESP vem realizando estudos bem como mantendo intercâmbio com diversas instituições de pesquisa visando a construção de um repositório arquivístico digital confiável (RDC-Arq) capaz de manter autênticos, preservar e promover acesso aos documentos digitais de guarda permanente. Na condição de órgão central do SAESP, a instituição também precisa se preparar para realizar a avaliação ou certificação de sistema de gestão arquivística de documentos (SIGAD), de sistemas de negócio, de repositórios arquivísticos digitais confiáveis (RDC-Arq) e de plataformas de acesso de documentos, dados e informações digitais.

Em consonância com as recomendações de organismos nacionais e internacionais, bem como em suas experiências acumuladas, o APESP consolidou o entendimento de que o uso das TIC nas práticas arquivísticas deve ser monitorado e orientado por políticas, estratégias, procedimentos e técnicas de preservação e segurança de documentos, dados e informações digitais.

Da mesma forma, os sistemas informatizados e sua utilização devem ser objetos de contínua melhoria da infraestrutura e de atualização tecnológica, para assegurar a gestão, preservação e acesso dos documentos digitais pelo tempo necessário. Nesse sentido, o desenvolvimento ou a adequação de sistemas informatizados para a produção ou captura, gestão, preservação e acesso a documentos, dados e informações digitais deverá:

- Estar em conformidade com as políticas de gestão e preservação de documentos digitais institucionalizadas;

- Incorporar um conjunto mínimo de requisitos e metadados indispensável à segurança, produção, gestão, preservação e acesso para garantir sua autenticidade, integridade, confidencialidade e confiabilidade;

- Promover a integração e interoperabilidade com sistemas legados, sistemas de negócio ou outros sistemas de informação;

- Assegurar a integração e interoperabilidade dos sistemas de produção e gestão com os sistemas de preservação e acesso, visando à manutenção da integridade da cadeia de custódia;

- Promover o uso racional dos recursos tecnológicos, tanto em relação à infraestrutura, quanto em relação à produção de dados e informações digitais, estejam eles registrados em documentos ou em outros sistemas e/ou bases de dados.

# 7 Ambientes arquivísticos digitais confiáveis

A administração pública tem o dever de promover a gestão documental visando assegurar o direito de acesso à informação. O cumprimento desse dever implica na responsabilidade jurídica dos órgãos e entidades estaduais pela custódia legítima e segura de documentos, dados e informações governamentais na condição de custodiadores confiáveis.

Cabe aos custodiadores confiáveis, sejam produtores ou preservadores, temporária ou definitivamente, o encargo de gerir e preservar os documentos, dados e informações governamentais e protegê-los de sua corrupção, adulteração ou destruição ao longo do tempo, garantindo a sua confiabilidade.

Esta *Política de Gestão e Preservação de Documentos Digitais* estabelece diretrizes e estratégias que devem ser implementadas de forma controlada e documentada, desde a produção dos documentos até sua destinação final e preservação, visando assegurar:

- A acurácia, precisão, correção, verdade e ausência de erros nos dados dos documentos (segundo o item *Definições* de INTERPARES, 2010a e INTERPARES, 2010b); e

- A credibilidade dos documentos enquanto documento (autenticidade, segundo a Instrução Normativa APESP/SAESP nº 1/2009, art. 2º, V), por meio do registro dos atributos que caracterizam cada documento como único e o diferencia de outros documentos arquivísticos (identidade, segundo CONARQ, 2020), e da garantia de que os documentos se encontram completos e que não sofreram nenhum tipo de corrupção ou alteração não autorizada nem documentada (integridade, segundo CONARQ, 2020).

Para a manutenção da confiabilidade ao longo do ciclo de vida dos documentos digitais é indispensável que a acurácia e a autenticidade não sejam comprometidas.

Toda operação que incidir sobre os documentos digitais, em qualquer etapa de sua existência, deve ser documentada, constituindo um conjunto de registros (controle de acesso, registro de metadados, protocolos de segurança, *logs)*, que possibilitem a auditoria dos procedimentos adotados.

Cabe ao APESP, enquanto órgão de preservação dos documentos de guarda permanente do Governo do Estado, fornecer orientação sobre a produção e manutenção dos documentos digitais, reforçando os requisitos e cuidados nos

procedimentos de preservação, como conversão ou migração, quando necessários, e nos procedimentos de transmissão, seja na esfera de um mesmo custodiador ou na sucessão dessa responsabilidade, considerando que durante a transmissão os documentos deixam um sistema presumidamente confiável e ficam vulneráveis até ingressarem em outro sistema seguro.

Cabe aos custodiadores adotarem as medidas de segurança preconizadas pelas normas de preservação para o processo de transmissão, de forma a reduzir os riscos de corrupção ou alteração.

Constitui também procedimento obrigatório documentar a sucessão de responsabilidades entre as entidades ou órgãos custodiadores dos documentos, dados e informações digitais.

A política integrada de gestão e preservação digital visa assegurar que a cadeia de preservação, um "sistema de controles que se estende por todo o ciclo de vida dos documentos, a fim de assegurar sua autenticidade ao longo do tempo" (segundo CONARQ, 2020), não seja quebrada, mantendo um criterioso sistema de controles, inclusive no momento de sucessão da custódia.

No sistema de controles, as ações que integram a cadeia de preservação digital são interdependentes e caso um elo da cadeia se rompa, por omissão, não conformidade, falha na execução de alguma atividade ou no registro de algum procedimento, a confiabilidade e a preservação dos documentos digitais ficam prejudicadas.

Para se conferir o maior grau de presunção de autenticidade aos documentos digitais, faz-se necessário que produtores e preservadores envidem todos os esforços para que não haja interrupção na cadeia de preservação e na cadeia de custódia, assegurando um ambiente arquivístico digital confiável, em conformidade com a política estadual de preservação digital.

# 8 Gestão de documentos digitais

O APESP, na condição de órgão central do Sistema de Arquivos do Estado de São Paulo (SAESP), é a instituição responsável por propor, orientar e promover a política estadual de arquivos e gestão de documentos (art. 7º do Decreto nº 48.897/2004). Sua implementação cabe aos órgãos e entidades por meio de suas Comissões de Avaliação de Documentos e Acesso (CADA).

No âmbito estadual, a Instrução Normativa APESP/SAESP nº 1/2009, atualizada pela Portaria UAPESP/SAESP nº 4/2020, estabeleceu diretrizes e procedimentos para gestão, preservação e acesso contínuo aos documentos arquivísticos digitais, em conformidade com as orientações da Versão 2 do e-ARQ Brasil, o Modelo de requisitos para sistema informatizados de gestão arquivística de documentos, elaborado pela Câmara Técnica de Documentos Eletrônicos do Conselho Nacional de Arquivos (CONARQ, 2022a e 2022b). Em âmbito nacional, merece destaque, ainda, a Resolução CONARQ nº 20/2004, que dispõe sobre a inserção dos documentos digitais em programas de gestão arquivística de documentos dos órgãos e entidades integrantes do Sistema Nacional de Arquivos (CONARQ, 2004).

A gestão de documentos é constituída por um conjunto de procedimentos e operações técnicas referentes à sua produção, classificação, avaliação, tramitação, uso, arquivamento e reprodução, que assegura a racionalização e a eficiência dos arquivos (art. 8º do Decreto nº 48.897/2004). São instrumentos básicos da gestão de documentos os planos de classificação, as tabelas de temporalidade, as normas e os procedimentos de protocolo e os sistemas informatizados de gestão arquivística.

A política de gestão documental é aplicável independentemente da forma ou do suporte, em ambientes não digitais, digitais ou híbridos em que os documentos, dados e informações são produzidos e armazenados. Entretanto, os documentos digitais são produzidos ou capturados em ambientes tecnológicos complexos e possuem características específicas que precisam ser consideradas.

A gestão arquivística de documentos digitais, não digitais e híbridos deve ser realizada por sistema informatizado de gestão arquivística de documentos (SIGAD) que adota requisitos e metadados arquivísticos e promoverá, quando possível, a integração com sistemas legados de controle de documentos e outros sistemas de negócio, evitando-se a perda ou corrupção de dados e informações.

O avanço contínuo das TIC permite que os documentos digitais sejam facilmente produzidos, transmitidos, armazenados, reproduzidos e utilizados nos processos de trabalho e na prestação de serviços públicos. Porém, essa facilidade, inerente ao ambiente digital, representa um grande desafio para a segurança e preservação dos documentos, considerando a fragilidade dos suportes, a obsolescência tecnológica e a dependência de *hardwares*, *softwares* e sistemas informatizados proprietários.

Nesse sentido, a *Política de Gestão e Preservação de Documentos Digitais* deve prever a adoção de um conjunto de medidas preventivas resultante de estudos e pesquisas promovidas por organismos nacionais e internacionais amplamente reconhecidos. A propósito, o APESP adota as orientações do *International Researchon Permanent Authentic Records in Electronic Systems Project* (InterPARES) para a definição de estratégias, procedimentos e técnicas de preservação digital de forma contínua, desde o momento da produção dos documentos, a fim de garantir sua autenticidade, integridade, confidencialidade e confiabilidade ao longo do tempo.

## 8.1. Produção de documentos digitais

De acordo com o Decreto nº 64.355/2019, que instituiu o processo eletrônico na administração pública estadual, os documentos nato-digitais assinados eletronicamente são considerados originais para todos os efeitos. A Portaria UAPESP/SAESP nº 2/2018, substituída pela Portaria UAPESP/SAESP nº 6/2021, definiu procedimentos para orientar a elaboração de modelos dos tipos documentais indicados nos planos de classificação, a fim de padronizar a sua produção no Sistema SP Sem Papel.

A produção de documentos digitais deve ser realizada em sistemas informatizados que incorporem requisitos e metadados arquivísticos, tanto aqueles de gestão arquivística de documentos (SIGAD), quanto aqueles que atendam a processos específicos dos órgãos e entidades (sistemas de negócio).

Em ambos os casos tais sistemas de produção de documentos digitais devem permitir em sua configuração requisitos e metadados de identidade e integridade que se mantenham associados aos documentos digitais, tais como a classificação de acordo com os planos de classificação; o prazo de guarda e a destinação de acordo com as tabelas de temporalidade; o encerramento por meio de procedimentos regulamentares e por usuários autorizados; a restrição de acesso; a verificação da validade da assinatura digital no momento da produção do documento; a consulta aos documentos encerrados por usuários autorizados; a integridade da relação hierárquica entre função, subfunção, atividade, série, documento, volume

e item documental em todos os momentos, independentemente de atividades de manutenção, ações do usuário ou falha de componentes do sistema.

Além disso, os sistemas informatizados que produzem documentos digitais devem impedir o acréscimo de novos documentos a processos ou expedientes encerrados e a eliminação de um documento digital ou de qualquer parte de seu conteúdo a não ser nos prazos determinados nas tabelas de temporalidade.

Para viabilizar a integração de sistemas de negócio ao SIGAD, bem como a presunção de autenticidade de documentos digitais neles produzidos é necessário o registro de seus metadados de identidade e integridade, e o cumprimento de requisitos de segurança e de preservação digital.

O SIGAD deve permitir a produção de documentos originalmente em ambiente digital (nato-digitais), a captura de documentos digitais produzidos em outros sistemas ou a captura de documentos não digitais que passaram pelo processo de digitalização (representantes digitais).

Documentos complexos ou não suportados pelos sistemas de produção e gestão de documentos devem ser armazenados em repositórios arquivísticos digitais confiáveis, preferencialmente vinculados ao SIGAD, que disponham no mínimo de controle de acesso por pessoas autorizadas, registro de alterações, controle de identificação e vínculo dos documentos, cópia de segurança e *backup*.

A captura de documentos não digitais pelo SIGAD deve ser realizada em formato PDF/A, mediante sua digitalização, de acordo com os requisitos e metadados previstos na Lei Federal nº 12.682/2012, no Decreto Federal nº 10.278/2020 e em atos legais federais e estaduais complementares.

Em âmbito nacional, o representante digital passou a ter equivalência jurídica ao documento original para todos os fins de direito, inclusive para atender ao poder de fiscalização do Estado, com a publicação da Lei nº 13.874/2019, que incluiu o art. 2º-A na Lei nº 12.682/2012. Entretanto, essa equivalência jurídica somente será assegurada se forem observados os padrões técnicos e metadados mínimos para a digitalização de documentos exigidos pelo Decreto Federal nº 10.278/2020.

Importante registrar que a matéria foi objeto da Resolução CONARQ nº 48/2021, que estabelece diretrizes e orientações aos órgãos e entidades integrantes do Sistema Nacional de Arquivos quanto aos procedimentos técnicos a serem observados no processo de digitalização de documentos públicos ou privados.

O APESP entende que a digitalização é um procedimento técnico integrado à política de gestão de documentos, por isso os documentos originais que não forem considerados históricos ou de guarda permanente poderão ser eliminados após sua digitalização, nos prazos estabelecidos nas tabelas de temporalidadade e que constatada a integridade dos documentos digitalizados.

Em decorrência das alterações promovidas nas leis federais nº 12.682/2012 e nº 13.874/2019, o APEPS publicou a Portaria UAPESP/SAESP nº 5/2021 para orientar os órgãos integrantes do SAESP sobre a digitalização de documentos públicos, a gestão e a preservação de seus representantes digitais para que produzam os mesmos efeitos legais de documentos originais e sejam preservados pelo tempo necessário.

Os órgãos e entidades responsáveis pela digitalização devem avaliar a conveniência, oportunidade e economicidade do serviço, considerando-se os prazos de guarda e a destinação final dos documentos, a frequência e a intensidade de consulta e o custo para captura da imagem, classificação, descrição, indexação, recuperação e armazenamento, incluindo o custo com mão de obra, infraestrutura lógica e física.

Para a eventual contratação de serviços de digitalização é necessário definir as especificações técnicas do trabalho para que as normas e procedimentos sejam adequadamente cumpridas na execução do contrato com base na Portaria UAPESP/SAESP nº9/2022, que acrescenta as "Especificações técnicas para contratação de serviços de digitalização de documentos públicos estaduais" à Portaria UAPESP/SAESP nº 1/2018, que dispõe sobre diretrizes para a contratação de serviços arquivísticos visando à execução de atividades técnicas auxiliares.

Para que os representantes digitais preservem sua força probante e permaneçam disponíveis para o uso administrativo ou para a pesquisa pública, é necessário definir estratégias de preservação e segurança digital para a implementação de repositórios arquivísticos digitais confiáveis, obedecendo inclusive uma lógica que favoreça a otimização das infraestruturas de armazenamento de documentos, dados e informações digitais, em fase intermediária e permanente, e a disponibilização de portas de acesso ao cidadão preferencialmente unificadas.

## 8.2. Avaliação de documentos

A avaliação documental é um amplo processo de análise que se inicia com a identificação das funções e atividades exercidas pela administração pública e que são responsáveis pela produção de conjuntos de documentos das áreas meio e fim de seus órgãos e entidades. A avaliação permite a identificação dos valores dos documentos, independentemente do suporte de registro das informações, para fins da definição de seus prazos de guarda e de sua destinação.

Os documentos de guarda temporária podem ser eliminados após o cumprimento dos prazos determinados, sem prejuízo para a coletividade ou memória da administração, e aqueles de guarda permanente devem ser preservados como prova, garantia de direitos ou fonte de pesquisa.

O resultado desse processo deve ser sistematizado pelas Comissões de Avaliação de Documentos e Acesso (CADA) dos órgãos e entidades estaduais em planos de classificação e em tabelas de temporalidade de documentos, posteriormente aprovadas pelo APESP e publicadas pelas autoridades competentes (art. 19 do Decreto nº 48.897/2004).

O Plano de Classificação e a Tabela de Temporalidade de Documentos da Administração Pública do Estado de São Paulo: Atividades-Meio (ARQUIVO PÚBLICO DO ESTADO, 2018b) foram elaborados pelo APESP e oficializados pelo Decreto estadual nº 48.898/2004, atualizado pelo Decreto nº 63.382/2018. Atualmente, todos os órgãos da administração direta contam com seus planos de classificação e tabelas de temporalidade das atividades fim, elaborados de acordo com a metodologia funcional proposta pelo APESP.

A avaliação documental tem grandes repercussões na gestão pública, pois garante racionalidade na produção documental, agilidade no acesso a informações, economia de recursos com a eliminação criteriosa de documentos e redução de espaço de armazenamento. Ainda, esse trabalho orienta a preservação de documentos que são considerados importantes para a memória da administração pública.

A avaliação documental e a aplicação dos instrumentos de gestão devem incidir igualmente sobre os documentos digitais, a despeito de suas especificidades. Nesse sentido, é preciso analisar: a possibilidade de exportação e interoperabilidade dos metadados; a custódia, a integridade, a organização e a descrição arquivística que fundamentam a presunção de autenticidade dos documentos digitais; os formatos de arquivo dos documentos digitais; e a existência de mecanismos de restrição de acesso ao documento digital, como criptografia, senha ou qualquer outro tipo de proteção tecnológica que possa impedir acessos não autorizados.

Os documentos digitais produzidos em sistema informatizado de gestão arquivística são classificados e avaliados no momento de sua produção e, portanto, os modelos estão desde o início associados aos códigos de classificação, aos prazos de guarda e à destinação indicados nos planos de classificação e tabelas de temporalidade de documentos.

Entretanto, os documentos digitais produzidos em quaisquer sistemas informatizados que não dialogam com planos de classificação e tabelas de temporalidade são acumulados, ao longo do tempo, sem contexto e sem critérios definidores de prazos de guarda e de destinação, o que acarreta a formação de uma massa documental digital acumulada (MDDA).

A MDDA é constituída de enormes volumes de documentais digitais produzidos e armazenados desordenadamente, o que acarreta elevados custos para sua manutenção e posterior classificação, avaliação, descrição e acesso.

Por essa razão, a Portaria UAPESP/SAESP nº 4/2020 determinou que os órgãos e entidades estaduais providenciassem a adequação de seus sistemas de negócio aos requisitos e respectivos metadados de identidade e integridade, inclusive indicando a destinação de documentos de acordo com as tabelas de temporalidade.

Os conjuntos de documentos, dados e informações digitais produzidos por sistemas descontinuados, seja pelo advento de uma nova solução tecnológica, seja pela extinção dos órgãos ou de suas atividades, devem ser considerados MDDA, caso os sistemas não observem parâmetros arquivísticos mínimos de gestão documental.

A aplicação de critérios arquivísticos à MDDA impõe grandes desafios não apenas pelo volume a ser avaliado, mas também pelas características específicas de cada um dos sistemas de produção e armazenamento de documentos, dados e informações digitais. As novas tecnologias e o uso da inteligência artificial podem contribuir para o reconhecimento de modelos dos tipos documentais indicados nos planos de classificação e automação da aplicação de regras e procedimentos de gestão documental na avaliação de Massas Documentais Digitais Acumuladas (MDDA).

A avaliação da MDDA é fundamental para assegurar a preservação do patrimônio documental digital do governo do estado de São Paulo e exige investimentos públicos em tecnologia, bem como esforços conjugados dos órgãos produtores com o APESP para que a identificação dos documentos digitais que devem ser preservados seja realizada o mais cedo possível.

Os sistemas de negócio devem prever protocolos de interoperabilidade com o SP Sem Papel que deve ser permanentemente aprimorado para automatizar os procedimentos de avaliação e permitir a efetiva aplicação dos prazos de guarda e da destinação previstas nas tabelas de temporalidade.

Dessa forma, para uma avaliação da MDDA produzida e armazenada em sistemas de negócio, que não observam os requisitos da gestão documental arquivística, recomenda-se: 1) Analisar a finalidade de operação do sistema de negócio, a fim de identificar os seus objetivos e a área/função/subfunção em que são gerados e armazenados os documentos digitais; 2) indentificar qual(ais) o(s) principal(ais) documento(s) produzido(s) e armazenado(s) nos Sistemas de Negócio; 3) Classificar o(s) documento(s) identificado(s) em conformidade com os planos de classificação oficiais; 4) Verificar o cumprimento dos prazos de guarda do(s) documento(s) e sua destinação final, conforme as tabelas de temporalidade de documentos oficializadas.

Cabe ressaltar duas questões relativas a sistemas de negócio que não observam os requisitos da gestão documental, sendo a primeira referente à

operacionalização da avaliação da MDDA, e a segunda relacionada à revisão e estabelecimento de requisitos para automatização do processo de avaliação da massa documental digital acumulada.

A avaliação da MDDA possivelmente ocorrerá de forma não automatizada em um primeiro momento, visando a identificação dos sistemas de negócio e dos documentos digitais produzidos e armazenados.

Após a avaliação da MDDA de forma não automatizada, a atribuição do código de classificação e temporalidade dos documentos produzidos e armazenados nos sistemas de negócio, provavelmente exigirá uma revisão e estabelecimento de novos requisitos que contemplem metadados referentes à classificação, prazos de guarda e destinação final, considerando que os sistemas não foram desenvolvidos em conformidade com as diretrizes e procedimentos para a gestão dos documentos arquivísticos digitais. Entende-se, portanto, que a automatização do processo de avaliação se faz necessária para garantir a continuidade da operação sobre a massa documental digital acumulada.

Em suma, conclui-se que somente é possível realizar a gestão de documentos, dados e informações digitais produzidos e armazenados em sistemas de negócio após a avaliação da MDDA e da aplicação de um programa de gestão arquivística, com a construção de estratégias, procedimentos e técnicas que permitam o panejamento, a implantação e o controle dos documentos digitais.

## 8.3. Eliminação de documentos digitais

A eliminação de documentos consiste na destruição irreversível daqueles que foram considerados sem valor para a guarda permanente no processo de avaliação.

Na administração pública estadual, a eliminação de documentos decorre do trabalho de avaliação documental conduzido pelas Comissões de Avaliação de Documentos e Acesso (CADA) instituídas nos órgãos e entidades e deve ser efetuada nos prazos estabelecidos nas tabelas de temporalidade de documentos, aprovadas pelo APESP e oficializadas pela autoridade competente, nos termos do Decreto nº 48.897/2004 e da Instrução Normativa APE/SAESP nº 2/2010.

A eliminação de documentos que não constem das tabelas de temporalidade deve ser realizada pelas CADA do órgão ou entidade, mediante autorização do APESP.

Os documentos considerados de guarda permanente, mesmo que digitalizados, não podem ser eliminados, pois são considerados inalienáveis e imprescritíveis, em decorrência de seu valor histórico, probatório e informativo.

São considerados documentos de guarda permanente aqueles indicados nas tabelas de temporalidade, os produzidos até o ano de 1940 e os declarados de interesse público e social.

São também de guarda permanente os documentos selecionados como amostragem, por meio de critérios qualitativos e quantitativos, durante o processo de avaliação, nos termos do art. 5º da Instrução Normativa APE/SAESP nº 3/2015.

Documentos classificados como sigilosos, nos termos da Lei Federal nº 12.527/2011 e do Decreto Estadual nº 58.052/2012, podem ser eliminados após um ano de sua desclassificação, considerando os prazos de guarda e a destinação previstos nas tabelas de temporalidade.

No âmbito da administração do estado de São Paulo, o registro de documentos a serem eliminados deve ser efetuado por meio de "Relação de Eliminação de Documentos". As CADA devem publicar no Diário Oficial do Estado os "Editais de Ciência de Eliminação de Documentos", visando dar publicidade ao ato. O "Edital de Ciência de Eliminação de Documentos" deve consignar um prazo de 30 (trinta) dias para possíveis manifestações ou, quando for o caso, possibilitar às partes interessadas requererem o desentranhamento de documentos ou cópias de peças de processos ou expedientes. O registro das informações relativas à execução da eliminação deve ser efetuado por meio do "Termo de Eliminação de Documentos", cuja cópia deve ser encaminhada ao APESP para a consolidação de dados e a realização de estudos técnicos na área de gestão de documentos.

Esses procedimentos de eliminação aplicam-se igualmente aos documentos digitais, mesmo considerando suas especificidades. Para eliminar documentos digitais de forma irreversível devem ser utilizadas ferramentas que sobrescrevam o espaço utilizado pelo documento digital e qualquer outro objeto digital que compõe o documento digital. Na inviabilidade da eliminação por meio da sobrescrição, o órgão deve providenciar a destruição física dos dispositivos de armazenamento. Assim, deve-se garantir que a eliminação alcance todo o conteúdo do documento digital, incluindo cópias de acesso, cópias de segurança e memórias secundárias como pendrives. O órgão responsável deve também registrar os procedimentos e os *softwares* utilizados para eliminação de documentos digitais, garantindo sua irreversibilidade. Além disso, deve-se manter o registro dos metadados referenciais mínimos dos documentos digitais eliminados, a fim de permitir a localização de seu registro após a eliminação, caso seja necessário.

Após efetivada a eliminação, dentro dos critérios legalmente estabeleciodos, os documentos digitais não devem ser restaurados pelo sistema informatizado no qual foram produzidos, nem por meio de rotinas auxiliares do sistema operacional, nem por aplicações especiais de recuperação de dados. Os documentos não digitais, que não sejam de guarda permanente, podem ser eliminados após sua digitalização, desde que: a) a digitalização observe padrões técnicos e metadados mínimos definidos no Decreto federal nº 10.278/2020; b) seus representantes digitais cumpram os prazos determinados nas tabelas de temporalidade.

A eliminação de documentos originais, após sua digitalização, deve ser registrada nos modelos dos ANEXOS I, II e III do Decreto Estadual nº 48.897/2004, fazendo constar: "Migração de suporte de papel para digital, com fundamento na Lei Federal nº 12.682/2012, no Decreto Federal nº 10.278/2020 e no Decreto Estadual nº 48.897/2004. Os representantes digitais cumprirão os prazos de guarda e a destinação final determinados nas tabelas de temporalidade de documentos aprovadas pelo APESP".

Já a eliminação de representantes digitais após o cumprimento dos prazos de guarda determinados nas tabelas de temporalidade de documentos deve ser registrada nos modelos dos ANEXOS I, II e III do Decreto Estadual nº 48.897/2004, informando a quantidade e *bytes* dos arquivos eliminados em lugar da quantidade de caixas e metros lineares, e fazendo constar: "Representantes digitais que cumpriram os prazos de guarda determinados nas tabelas de temporalidade de documentos aprovadas pelo APESP".

Por fim, cabe esclarecer que poderão ser excluídos de forma irreversível os documentos digitais que permanecerem nos órgãos de origem após o procedimento formal de sua transferência ou recolhimento aos repositórios arquivísticos digitais confiáveis, que preservarão os documentos públicos digitais certificados. Do contrário, esses registros digitais duplicados remanescentes ocupariam espaço de armazenagem nos sistemas de forma desnecessária e onerosa.

# 9 Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD) e Sistemas de Negócio

O avanço das TIC, a partir dos anos 1990, mudou a forma de registro e gestão da informação nas instituições públicas e privadas e fez com que os documentos, produzidos no exercício das atividades dessas instituições, passassem a ser gerados em ambientes digitais e armazenados de forma digital.

Em decorrência, a gestão de documentos, tanto digitais quanto não digitais, começou a ser feita por meio de sistemas informatizados de gerenciamento de documentos. Entretanto, para assegurar que documentos arquivísticos digitais tenham presunção de auteticidade e se mantenham íntegros, confiáveis e acessíveis ao longo do tempo, é fundamental que tais sistemas informatizados incorporem os requisitos arquivísticos, evoluindo para atuarem como Sistemas Informatizados de Gestão Arquivística de Documentos (SIGAD). Esse tipo de Sistema é uma solução tecnológica composta por um único *software* ou pela integração de diversos *softwares*, que apoia a gestão arquivística de documentos.

O sucesso de um SIGAD depende, fundamentalmente, da implantação de uma política de gestão arquivística de documentos e da incorporação de seus instrumentos, os planos de classificação, as tabelas de temporalidade, processos de avaliação e as normas e procedimentos de protocolo. Sendo assim, a evolução tecnológica de um SIGAD deve espelhar o aprimoramento, a expansão e a consolidação da política de gestão arquivística. Além disso, o funcionamento de um SIGAD exige o desenvolvimento de funcionalidades aderentes às regras de negócios, bem como a revisão, adequação e ampliação da infraestrutura tecnológica.

O SIGAD é um ambiente informatizado de gestão de documentos, aplicável em ambientes que gerenciam documentos digitais, não digitais e híbridos. Portanto, deve controlar os documentos nas fases corrente e intermediária, e apoiar procedimentos de preservação. É recomendável que o tratamento e guarda de documentos já avaliados e em fase permanente sejam realizados por meio de solução tecnológica específica, independente do SIGAD, que garanta a

presunção de autenticidade e preservação de documenos digitais permanentes, com as características de um Repositório Arquivístico Digital Confiável (RDC-Arq), nos termos da Resolução CONARQ nº 43/2015.

O SIGAD realiza a gestão de documentos desde a sua produção, possibilitando a classificação na origem, a partir de planos de classificação, o que garante a manutenção da relação orgânica dos documentos entre si, bem como com as funções e atividades que representam. Nesse sentido, as operações inerentes à gestão documental devem ser implementadas e automatizadas no SIGAD, tais como: a contagem de prazos, o encerramento de processos e expedientes, e sua eliminação, de acordo com as tabelas de temporalidade. Ainda, deve ser capaz de promover a indexação e o acesso a documentos arquivísticos digitais, por meio de sua produção ou captura e armazenamento, zelando pela integridade dos metadados, indexadores e demais componentes digitais, que permitam a compreensão dos contextos jurídico-administrativo, de proveniência, de procedimentos documental e tecnológico.

Os requisitos e metadados arquivísticos de um SIGAD foram definidos pelo e-ARQ Brasil - Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (CONARQ, 2022a e 2022b), orientação válida para as instituições arquivísticas de todos os poderes e esferas de governo, a quem cabem a formulação e implementação de políticas de Estado capazes de assegurar a produção, gestão, armazenamento, preservação, segurança e acesso ao patrimônio arquivístico digital.

Na administração pública paulista, os requisitos e metadados a serem adotados pelo SIGAD foram definidos na Instrução Normativa APE/SAESP nº 1/2009, alterada pela Portaria UAPESP/SAESP nº 4/2020, em conformidade com o modelo de requisitos apresentado no e-ARQ Brasil (CONARQ, 2022a e 2022b).

Além do SIGAD, os sistemas de negócio também são utilizados para a produção de documentos digitais específicos. Embora menos complexos, tais sistemas devem observar um conjunto mínimo de requisitos arquivísticos que tornem possível sua integração com outros sistemas e o desenvolvimento de funcionalidades básicas de gestão arquivística de documentos.

A gestão arquivística de documentos digitais produzidos em sistemas de negócio pode ocorrer por meio da exportação dos documentos arquivísticos para o SIGAD, da integração entre esses sistemas ou da implementação de funcionalidades básicas de gestão arquivística nos próprios sistemas de negócio. Isso significa que o estado deve ser compromissado com a centralização da gestão da informação, a otimização dos fluxos e a facilitação das formas de controle em larga escala por meio da integração dos sistemas de negócio aos SIGAD.

## 9.1. Programa São Paulo Sem Papel

Para a adoção de um SIGAD, desde 2017 o Governo do Estado de São Paulo optou por analisar as opções de *softwares* livres e gratuitos disponíveis, mais aderentes à política estadual de arquivos, evitando-se custos com desenvolvimento e agilizando a implantação do processo eletrônico. Também foi considerada na análise a possibilidade de alteração e evolução do código fonte do sistema pelo Governo do Estado, possibilitando, assim, a customização e adaptação às suas necessidades próprias.

Para atender a esse objetivo, foi selecionado o Sistema Integrado de Gestão Documental (SIGA-Doc), desenvolvido pelo Tribunal Regional Federal da 2ª Região/RJ (TRF-2) e que também foi adotado pelo Conselho da Justiça Federal para o gerenciamento de seus processos e expedientes administrativos.

O SIGA-Doc foi incorporado ao Programa SP Sem Papel, instituído pelo Decreto nº 64.355/2019, para substituir a produção de documentos em papel pela produção de documentos digitais.

Na condição de órgão central do Sistema de Arquivos do Estado de São Paulo (SAESP), o APESP matém-se vigilante para garantir a aderência do SIGA-Doc à política estadual de arquivos e gestão documental, nos termos da Instrução Normativa nº 1/2009, atualizada pela Portaria UAPESP/SAESP nº 4/2021. Nesse sentido, a instituição apontou seis requisitos mínimos que a solução deve atender, de modo a permitir a produção segura e a gestão arquivística dos documentos digitais:

Captura de documentos externos ao sistema;

- Classificação obrigatória do documento no ato de sua produção ou de sua captura, quando se tratar de documento externo;
- Controle de documentos avulsos e compostos;
- Autuação de processos e outras rotinas de protocolo;
- Sinalização de que o documento foi encerrado (evento deflagrador para contagem de prazos de guarda);
- Automatização dos procedimentos de avaliação, arquivamento e eliminação.

Além de propor de alterações e evoluções do SP Sem Papel, o APESP atua para promover a padronização dos documentos produzidos pelo Sistema por meio da elaboração de modelos e do mapeamento de trâmite. Para tanto, o APESP conta com a colaboração das Comissões de Avaliação de Documentos e Acesso (CADA) e dos órgãos setoriais da Administração Pública Estadual.

O SP Sem Papel deve assegurar a proteção de autoria, autenticidade, integridade, disponibilidade e legibilidade de documentos digitais produzidos em conformidade com o art. 3º do Decreto nº 64.355/2019.

O APESP está comprometido com a expansão do Programa SP Sem Papel e plena adesão dos órgãos e entidades e, nesse sentido, tem atuado para a elaboração de planos de classificação e de tabelas de temporalidade das atividades fim pelos órgãos e entidades. Para atingir essa finalidade, a instituição se compromete com o pleno funcionamento do sistema nas seguintes frentes:

**1. Elaboração de regras de negócio**

No processo de implantação, coube ao APESP a tarefa de analisar o sistema, identificar as necessidades de melhorias, elaborar as regras de negócio - principalmente aquelas voltadas para a gestão de documentos digitais em fase corrente e intermediária – e homologar o seu desenvolvimento. Dentre as principais regras de negócio elaboradas pelo APESP para aprimorar o Sistema, destacam-se: Numeração de páginas de Processos e Expedientes, funcionalidade "Ciência", Protocolo de Acompanhamento, Incorporação, funcionalidade "Juntar", Encerramento, Arquivamento, Eliminação, Transferência, Recolhimento e Restrição de Acesso. Além de contribuir para o aprimoramento das regras de gestão documental, o APESP também contribui para melhorar a usabilidade do Sistema, como por exemplo, a reformulação da Mesa Virtual.

**2. Modelagem de documentos digitais**

Para promover o regramento da produção de documentos digitais no ambiente digital, o APESP aprovou a Portaria UAPESP/SAESP nº 2/2018, substituída pela Portaria UAPESP/SAESP nº 6/2021, que define procedimentos para orientar o mapeamento de documentos compostos e a modelagem de documentos digitais no Programa SP Sem Papel. Entende-se por modelagem de documentos digitais o desenvolvimento de modelos de documentos em sistema informatizado, considerando a sua forma e conteúdo. A modelagem de documentos torna a produção de documentos digitais mais intuitiva para o usuário, padroniza conteúdo e forma dos documentos, e agiliza a recuperação de informações nos campos descritores, por meio da funcionalidade "Pesquisar". Além dos descritores, os modelos apresentam conteúdos editáveis ou fixos, pré-determinados. Até o momento, o APESP elaborou 2.882 modelos de documentos digitais disponíveis no SP Sem Papel e pretende até o final de 2023 entregar mais 700 modelos.

### 3. Capacitação e orientação de usuários do sistema

Para a implantação do Programa SP Sem Papel o APESP elaborou o Manual de uso do sistema, aprovado pela Resolução SG-57/2019 e atualizado por meio da Portaria UAPESP/SAESP n. 3/2020, e vem atuando em parceria com a Fundação Carlos Alberto Vanzolini (FCAV), na capacitação permanente de usuários e na orientação técnica sobre procedimentos de protocolo e de classificação, permitindo o estabelecimento de novas rotinas e procedimentos internos, considerando as especificidades do ambiente digital.

### 4. Formalização de parcerias com órgãos de controle interno

O APESP vem propondo ações integradas e colaborativas com a Controladoria Geral do Estado e com a Subsecretaria de Tecnologia, Inovação e Serviços ao Cidadão, com a finalidade de facilitar a fiscalização e auditoria das informações registradas no sistema, bem como de avaliar as formas de produção e visualização de dados e metadados gerenciais que permitam outras formas de monitoramento sistêmico.

Ao Programa SP Sem Papel cabe garantir a proteção da autoria, da autenticidade, da integridade, da disponibilidade e da legibilidade de documentos digitais produzidos no ambiente digital de gestão documental do Programa SP Sem Papel, bem como assegurar a gestão, a preservação e a segurança de documentos ao longo do tempo, conforme art. 3º do Decreto nº 64.355/2019.

# 10 Governança e gestão de dados públicos

A governança de dados públicos pode ser entendida como o conjunto de políticas que o estado cria para proteger e utilizar os documentos, dados e informações para aprimoramento das suas políticas públicas, para promoção da transparência dos seus atos e para a qualidade dos serviços prestados, sempre atento ao princípio do interesse público. A governança de dados depende de uma matriz de responsabilidades e de papéis claros de órgãos estaduais comprometidos com o desenvolvimento de ações contínuas para sua produção, gestão, preservação e acesso. A gestão de dados se complementa, mas não se confunde, com os serviços digitais e desenvolvimento de tecnologias destinados para a melhoria dos serviços ao cidadão.

Nesse contexto, a gestão de documentos cumpre um papel estratégico para a gestão de dados governamentais (Lei de Arquivos, art. 3º), pois os dados e as informações, tanto quanto os documentos, integram os conceitos já consagrados e abrangentes de "arquivos" e de "arquivos públicos" (Lei de Arquivos, arts. 2º e 7º). Por essa razão, as diretrizes, normas e procedimentos definidos na política de gestão documental alcançam, igualmente, os documentos não digitais e digitais, as informações e os dados produzidos e armazenados no exercício de funções e atividades governamentais. Esses três objetos - documentos, dados e informações, ainda que exijam tratamentos técnicos ou tecnológicos específicos, são indissociáveis do ponto de vista de sua produção, da prática administrativa e da política arquivística, uma vez que resultam, igualmente, do exercício rotineiro de funções e atividades governamentais.

No campo jurídico, nota-se a equivalência de sentido entre os conceitos de "gestão de documentos" (Lei de Arquivos, art. 3º), "tratamento da informação" (Lei de Acesso à Informação - LAI, art. 3º, V) e "tratamento de dados" (Lei Geral de Proteção de Dados - LGPD, art. 5º, X), o que significa ter uma necessária complementaridade entre eles, na medida em que se preocupam com o estabelecimento de normas e procedimentos desde a sua produção até sua destinação final abarcando todo o seu ciclo de vida.

Nesse sentido, observa-se que as operações específicas relacionadas ao "tratamento da informação" e ao "tratamento de dados" são indicativas de especificidades da gestão de documentos quando aplicadas ao ambiente digital.

Por essa razão, a política arquivística deve, também, alcançar o tratamento de dados, a fim de garantir o seu contexto original de produção, organicidade, custódia e integridade. A manutenção dessas características é o que torna os dados confiáveis e úteis, tanto para a construção do conhecimento, quanto para a execução de políticas públicas, no momento presente e futuro.

Cabe esclarecer que os procedimentos para eliminação de documentos no setor público devem ser aplicados, também, aos dados e informações governamentais quando produzidos em ambiente digital, sem prescindir da necessária autorização das instituições arquivísticas públicas, nos termos do art. 9º da Lei de Arquivos nº 8.159/1991.

Portanto, há que se compatibilizar a LGPD com a legislação arquivística, pois mesmo que cumprida a finalidade primária que justificou a coleta de dados pessoais, estes podem estar registrados em documentos ou armazenados em bases de dados consideradas de guarda permanente e, nessa hipótese, não podem ser eliminados, por serem considerados "inalienáveis e imprescritíveis", nos termos do art. 10 da Lei nº 8.159/1991.

De forma similar à gestão de documentos, nota-se que a gestão de dados exige, igualmente, o trabalho de equipes multidisciplinares e ferramentas para seu tratamento de acordo com padrões e regras previamente definidas, visando sua segurança e acesso.

Na esfera federal, um passo importante para a transformação digital foi a implantação do processo eletrônico para a realização do processo administrativo por meio do Decreto nº 8.539/2015. A opção do Ministério do Planejamento à época foi pelo Sistema Eletrônico de Informações (SEI), desenvolvido pelo Tribunal Regional Federal da 4ª Região / RS (TRF-4), e que integra o Processo Eletrônico Nacional (PEN), uma iniciativa conjunta de órgãos e entidades de diversas esferas da administração pública, com o intuito de construir uma infraestrutura pública de processos e documentos administrativos eletrônicos. Diante das limitações apresentadas pela ferramenta, o Ministério da Economia propôs uma nova solução, o Sistema Único de Processo Eletrônico em Rede – SUPER.BR.

De forma mais ampla, a política de governança digital, em âmbito federal, foi instituída pelo Decreto nº 8.638/2016, atualizada pelo Decreto nº 10.332/2020 com metas e compromissos mais detalhados. Além disso, foram publicados outros decretos complementares com destaque para o Decreto nº 10.046/2019, que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.

Importante destacar que, em âmbito federal, a Controladoria Geral da União (CGU) é responsável, dentre outras competências, pela promoção da transparência

e do acesso à informação, exercendo o monitoramento dos Serviços de Informação ao Cidadão (SIC) e atuando como segunda instância recursal para as negativas dos pedidos de acesso à informação. Para assegurar efetividade da política de gestão de dados, a CGU atua como órgão de fiscalização.

No âmbito da administração pública estadual, o processo eletrônico foi implantado pelo Decreto nº 64.355/2019, que instituiu o Programa SP Sem Papel e criou o Comitê de Governança Digital, posteriormente extinto pelo Decreto nº 64.790/2020, que criou o Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo (CGGDIESP). Este Comitê, além de incorporar as atribuições do extinto Comitê de Governança Digital, tornou-se responsável pela Central de Dados do Estado de São Paulo (CDESP), repositório eletrônico de dados e informações, estruturados ou não, gerados ou coletados pela Administração Pública estadual, acessível pela Plataforma Única de Acesso (PUA), em fase de implantação. Esse colegiado é responsável por mapear e requisitar dados e informações dos órgãos e entidades da administração pública estadual, necessários à formulação, implementação e avaliação de políticas públicas do Estado. O Comitê editou a Deliberação Normativa CGGDIESP nº 1/2021, que institui a Política de Governança de Dados e Informações (PGDI), no âmbito da Administração Pública Estadual, e a Deliberação Normativa CGGDIESP nº 2/2021, que institui a Política de Proteção de Dados.

A implementação de uma política estadual de governança de dados, documentos e informações deve ser promovida por meio de ações integradas e colaborativas entre todos os órgãos estaduais diretamente envolvidos nesse processo, com responsabilidades e papéis bem definidos:

- O Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo (CGGDIESP), responsável pela política de governança de dados e informações no âmbito da administração pública estadual e pela Central de Dados do Estado de São Paulo (CDESP) (Decreto nº 64.790/2020);

- O APESP, instituição arquivística do Poder Executivo Estadual, que é o órgão central do Sistema de Arquivos do Estado de São Paulo (SAESP), responsável pela formulação da política estadual de gestão de documentos e acesso à informação (Decreto nº 22.789/1984, Decreto nº 48.897/2004, Decreto nº 54.276/2009 e Decreto nº 58.052/2012);

- O Conselho Estadual de Tecnologia da Informação e Comunicação (COETIC), órgão central do Sistema Estadual de Tecnologia da Informação e Comunicação (SETIC), responsável por analisar e aprovar políticas sobre o uso de tecnologias da informação e comunicação (Decreto nº 64.601/2019);

- A Subsecretaria de Inovação, Tecnologia e Serviços ao Cidadão da Secretaria de Governo, responsável pelas atividades de governança, planejamento, coordenação, organização, controle e monitoramento dos recursos de tecnologia da informação, comunicação e telecomunicação (Decreto nº 64.601/2019);

- A Companhia de Processamento de Dados do Estado de São Paulo (PRODESP) que tem como objetivo atuar como prestadora de serviços e fornecedora de produtos de tecnologia para desenvolvimento, produção, armazenamento, infraestrutura, manutenção, processamento e guarda de sistemas, dados, informações (Estatuto da PRODESP, DOE de 04/08/2021);

- A Controladoria Geral do Estado, criada pela Lei Complementar nº 1.361/2021e organizada pelo Decreto nº 66.850/2022, que tem por finalidade a defesa do patrimônio público, o controle interno, o combate à corrupção, e a promoção da ética e da transparência no âmbito da Administração Pública direta e indireta do Estado;

- A Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) e as Universidades Estaduais Paulistas para o desenvolvimento de pesquisa, inovação e capacitação na busca por soluções sustentáveis de longo prazo para os desafios relacionados à transformação digital.

## 10.1. Política de dados abertos

De forma geral, os documentos, dados e informações disponibilizados pelo setor público e as informações de transparência ativa são de livre utilização pelos Poderes Públicos e pela sociedade, ressalvadas as hipóteses legais de sigilo e das informações pessoais que devem ser protegidas, nos termos da LAI e LGPD.

A Política de Dados Abertos, instituída em âmbito federal pelo Decreto Federal nº 8.777/2016, alterado pelo Decreto nº 9.903/2019, determinou a publicação de dados primários e atualizados contidos em bases de dados dos órgãos e entidades federais, sob a forma de dados abertos e legíveis por máquinas, com a garantia de acesso irrestrito e de reuso.

Dados abertos são "dados acessíveis ao público, representados em meio digital, estruturados em formato aberto, processáveis por máquina, referenciados na internet e disponibilizados sob licença aberta que permita sua livre utilização, consumo ou cruzamento, limitando-se a creditar a autoria ou a fonte" (art. 2º, III).

Os dados abertos podem ser utilizados para o acompanhamento das ações dos órgãos públicos ou reutilizados em novos estudos e em cruzamentos com ou-

tras bases de dados para o desenvolvimento de ferramentas tecnológicas e outros sistemas de informação.

No Executivo federal, a gestão da Política de Dados Abertos é coordenada pela Controladoria-Geral da União (CGU), por meio da Infraestrutura Nacional de Dados Abertos (INDA). A CGU também é o órgão responsável pela implementação, monitoramento e fiscalização da LAI.

De acordo com o art. 6º do Decreto nº 8.777/2016, o atendimento de pedidos de abertura de bases de dados da administração pública federal deve observar os mesmos prazos e procedimentos previstos para o processamento de pedidos de acesso à informação, nos termos da LAI e de seu decreto regulamentador. Nesse sentido, o canal para recepção de pedidos de abertura de dados é o próprio Serviço de Informação ao Cidadão (SIC), considerando inclusive as mesmas instâncias recursais previstas na LAI, nos casos de negativas de acesso. Conclui-se, portanto, que essa integração da política de dados abertos à política de acesso à informação confere coerência e coesão para a política de transparência ativa em âmbito federal.

O governo federal conta com um Portal Brasileiro de Dados Abertos (https://dados.gov.br/) que disponibiliza 13.603 conjuntos de dados, conforme pesquisa realizada no dia 07/10/2022. Os Planos de Dados Abertos dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional devem ser elaborados e publicados em sítio eletrônico (art. 9º do Decreto nº 8.777/2016), devendo ser priorizada a abertura dos dados de maior interesse público, abaixo relacionados conforme o anexo do Decreto nº 8.777/2016, os quais deverão ser publicados em formato aberto:

- Textos das publicações do Diário Oficial da União;
- Ocupantes de cargos de gerência e direção em empresas estatais e subsidiárias;
- Dados relativos a servidores inativos e aposentados e relativos a empregados e servidores públicos das entidades da administração indireta de órgãos e entidades que não utilizam o Sistema Integrado de Administração de Pessoal (SIAPE);
- Dados do Sistema Integrado de Administração Financeira (SIAFI);
- Informações sobre o quadro societário das empresas, a partir do Cadastro Nacional de Pessoas Jurídicas (CNPJ);
- Dados relacionados ao Plano Plurianual, incluindo metas físicas;
- Bens móveis e de patrimônio registrados no Sistema Integrado de Administração de Serviços (SIADS);

- Dados relacionados ao Sistema Integrado de Administração de Serviços Gerais (SIASG/COMPRASNET);
- Dados referentes ao Portal do Sistema de Convênios (SICONV);
- Informações cadastrais e relacionadas ao controle da execução de emendas parlamentares;
- Propriedades e imóveis do Governo federal;
- Dados sobre nascimentos, casamentos, divórcios e óbitos - Sistema Nacional de Informações de Registro Civil (SIRC)

No estado de São Paulo, a Política de Dados Abertos foi inaugurada pelo Decreto Estadual nº 55.559/2010 que instituiu o Portal do Governo Aberto SP e dispôs sobre o livre acesso a dados e informações não sigilosos da Administração Pública Estadual. Em seguida, o Decreto Estadual nº 57.500/2011 criou o Portal da Transparência Estadual administrado à época pela Corregedoria Geral da Administração.

A política de dados abertos paulista foi complementada pelo Decreto nº 58.052/2012, que regulamentou a LAI, o qual dispôs que os órgãos e entidades da Administração Pública Estadual deveriam atualizar permanentemente os dados e informações que compõem o "Catálogo de Sistemas e Bases de Dados da Administração Pública do Estado de São Paulo (CSBD)", que deveria ser disponibilizado no Portal do Governo Aberto e no Portal da Transparência, com todos os elementos necessários para permitir sua utilização por terceiros, com a arquitetura das bases e o dicionário de dados.

Pelo Decreto Estadual nº 66.850/2022, o Conselho de Transparência da Administração Pública e o Comitê Gestor do Portal da Transparência Estadual passaram a integrar a estrutura da Controladoria Geral do Estado, que conta também com a Coordenadoria de Ouvidoria e Defesa do Usuário do Serviço Público, responsável por fomentar a transparência pública, assegurando o cumprimento dos dispositivos legais que regulam o acesso à informação e a proteção de dados pessoais (Decretos nº 58.052/2012 e nº 65.347/2020).

Nota-se que o Portal do Governo Aberto SP se propõe a disponibilizar para a sociedade, via Internet, as bases de dados digitais e as informações não sigilosas e de acesso irrestrito dos órgãos e entidades da Administração Pública Estadual (art. 1º do Decreto nº 55.559/2010). Com a mesma finalidade, o Portal da Transparência Estadual pretende divulgar de forma ativa dados relevantes para a promoção da transparência da gestão pública e do controle social (art. 43 do Decreto nº 57.500/2011).

A propósito, é necessário reconhecer que essa política de dados abertos, que mantém interlocução ampla com a sociedade, não se confunde com os

objetivos da Central de Dados do Estado de São Paulo (CDESP) criada para atender às necessidades gerenciais do próprio governo na formulação, implementação e avaliação de políticas públicas (art. 1º do Decreto nº 64.790/2020). Por essa razão, o acesso ao repositório da CDESP é restrito aos órgãos e entidades estaduais por meio de uma Plataforma Única de Acesso (PUA), mediante autorização do Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo (art. 3º do Decreto nº 64.790/2020).

## 10.2. Proteção de dados pessoais

Em âmbito nacional, a proteção de dados pessoais foi regulada pela Lei Federal nº 13.709/2018 (LGPD). A Lei dispôs sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

É importante destacar que a LGPD (art. 23, § 3º) determina a utilização dos mesmos prazos e procedimentos definidos na Lei de Acesso à Informação para proteger os direitos do titular de dados perante o Poder Público, sendo desnecessária a criação de mecanismos e procedimentos diversos o que, além de custos adicionais, poderiam também gerar insegurança jurídica.

O Decreto Federal nº 10.046/2019 avançou ao definir categorias de dados pessoais sensíveis, a serem protegidos: a) atributos biográficos - dados de pessoa natural relativos aos fatos da sua vida, tais como nome civil ou social, data de nascimento, filiação, naturalidade, nacionalidade, sexo, estado civil, grupo familiar, endereço e vínculos empregatícios; b) atributos biométricos - características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado; c) atributos genéticos - características hereditárias da pessoa natural, obtidas pela análise de ácidos nucleicos ou por outras análises científicas; d) dados cadastrais - informações identificadoras perante os cadastros de órgãos públicos.

A LGPD instituiu a Autoridade Nacional de Proteção de Dados (ANPD), com o objetivo de zelar pela proteção de dados pessoais e por regulamentar, implementar e fiscalizar o cumprimento da LGPD no Brasil. A Lei nº 14.460/2022 transformou a Agência Nacional de Proteção de Dados (ANPD) em Autarquia Especial, a fim de conferir a ela autonomia financeira e administrativa para o melhor cumprimento de sua finalidade. Essa mesma Lei alterou as Leis nº 13.709/2018 (LGPD) e nº 13.844/2019 (estrutura/órgãos da Presidência da República), e revogou dispositivos da Lei nº 13.853/2019, que havia alterado a LGPD.

Em âmbito estadual, o Decreto nº 58.052/2012, regulamentador da LAI, determinou o dever do poder público em promover a proteção dos documentos, dados e informações sigilosas e pessoais, por meio de critérios técnicos e objetivos, o menos restritivo possível. Esse decreto antecipou-se às orientações da LGPD uma vez que já previam os procedimentos referentes à produção ou coleta, gestão, tratamento e proteção de dados pessoais.

A regulamentação da LGPD em âmbito estadual se deu por meio do Decreto Estadual nº 65.347/2020, que também ampliou as atribuições do Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo, instituído pelo Decreto nº 64.790/2020, visando à elaboração e atualização da Política de Proteção de Dados Pessoais. De acordo com a Resolução SG nº 86/2020, cabe a esse Comitê definir diretrizes para o cumprimento da LGPD pelos órgãos e entidades da Administração Pública Estadual.

No exercício de suas atividades, o Comitê publicou a Deliberação Normativa CGGDIESP nº 2/2021, que institui a Política de Proteção de Dados Pessoais (PPDP) no âmbito da Administração Pública Estadual. Nessa Deliberação o APESP ficou responsável por orientar a definição de prazos para armazenamento e eliminação de dados considerando a finalidade específica do seu tratamento. A propósito, a temporalidade e a destinação dos documentos públicos estaduais já estão definidas nas tabelas de temporalidade de documentos das atividades meio e das atividades fim elaboradas pelas Comissões de Avaliação de Documentos e Acesso (CADA), instituídas em todos os órgãos e entidades estaduais, e aprovadas pelo APESP.

Por todo o exposto, a despeito do esforço já realizado para definir uma política de dados em âmbito estadual, ainda é necessário promover sua harmonização com as disposições da LAI e da Lei de Arquivos nº 8.159/1991, amplamente reguladas por dispositivos legais específicos em âmbito estadual.

# 11 Preservação de documentos digitais

Há pelo menos duas décadas, organismos internacionais vêm alertando sobre os riscos decorrentes da fragilidade e obsolescência inerentes ao mundo digital para a preservação do patrimônio arquivístico digital.

Em 2003, a UNESCO lançou a "Carta para a preservação do patrimônio arquivístico digital" (CONARQ 2005), com o tema central *Preservar para garantir o acesso*, a fim de promover políticas e ações para proteger o patrimônio arquivístico digital, em benefício das gerações atuais e futuras.

O Conselho Internacional de Arquivos (CIA) também lançou em 2010 a "Declaração universal sobre os arquivos" (CIA, 2010), estimulando os Arquivos Públicos a contribuírem para que os produtores de documentos criassem e mantivessem documentos arquivísticos fidedignos, autênticos, preserváveis e acessíveis ao longo do tempo.

Em âmbito internacional, desde a década de 1990 o governo estadunidense e governos da Comunidade Europeia vêm trabalhando para a definição de requisitos funcionais para a gestão de documentos digitais. Em 1997, o Departamento de Defesa dos Estados Unidos criou a Norma Do D 5015.2, que foi incorporada pela Administração Pública norte-americana e se tornou um padrão de referência nacional e internacional. Em 2002, um grupo de especialistas da União Europeia criou o MOREQ - Modelo de requisitos para a gestão, o acesso contínuo e a retenção de documentos pelo tempo necessário.

No Brasil, em 2006, foi lançada a 1ª versão do e-Arq Brasil, modelo de requisitos baseado na Norma DoD e no MOREQ, elaborada pela Câmara Técnica de Documentos Eletrônicos, aprovada pela Resolução CONARQ nº 25/2007, para orientar o desenvolvimento de Sistemas Informatizados de Gestão Arquivística de Documentos (SIGAD). A 2ª versão do e-Arq Brasil foi aprovada pela Resolução CONARQ nº 50/2022.

Quanto à preservação, merece destaque a iniciativa do governo dos EUA para a construção de repositórios digitais confiáveis. A NASA, agência aeronáutica norte-americana, desenvolveu ao longo de dez anos o modelo conceitual *Open Archival Information Sistems* (OAIS), ou Sistema Aberto de Arquivamento de Informação (SAAI), em colaboração com a comunidade científica internacional. Versões do documento inicial foram publicadas em 1999 e 2002, que, em 2003, transformou-se

na norma internacional ISO 14721:2003, uma das normas mais importantes para a construção de repositórios arquivísticos digitais confiáveis.

No Brasil, a norma OAIS foi publicada pela ABNT: NBR 15425: Modelo de referência para um Sistema Aberto de Arquivamento de Informação (SAAI). Em 2007, o Arquivo Nacional dos Estados Unidos (NARA), em consonância com o modelo OAIS, produziu um conjunto de critérios e um *checklist* (conhecido como TRAC) para a certificação de repositórios digitais confiáveis. Esse documento foi a base para a norma internacional ISO 16363:2012 (ISO, 2012).

Importante também destacar a importância do Projeto InterPARES (1998/2018) - *International Research on Permanent Authentic Records in Electronic Systems*, ou Pesquisa internacional sobre documentos arquivísticos permanentes autênticos em sistemas eletrônicos, coordenado pela Universidade de British Columbia, no Canadá, com o objetivo de produzir conhecimento teórico-metodológico visando a preservação de longo prazo de documentos arquivísticos digitais autênticos.

O Projeto de pesquisa InterPARES produziu requisitos para presunção de autenticidade de documentos, diretrizes para produção e preservação de documentos digitais autênticos e um conjunto de estratégias para a preservação de longo prazo. O Brasil participou das pesquisas do InterPARES, sob a coordenação do Arquivo Nacional. O APESP também integrou o projeto com estudo de caso sobre o sistema SPdoc, mediante termo de cooperação técnica com o Arquivo Nacional.

A última fase do projeto, InterPARES Trust (2013/2018), dedicou-se a apoiar os países na definição de políticas, regras, procedimentos e padrões para os documentos arquivísticos digitais armazenados na Internet. Os documentos gerados no âmbito do Projeto InterPARES vêm sendo traduzidos pela Câmara Técnica de Documentos Eletrônicos do CONARQ e disponibilizados no site do Projeto: Diretrizes para a presunção de autenticidade de documentos arquivísticos digitais (Resolução CONARQ nº 37/2012); Diretrizes do produtor e do preservador (Resolução CONARQ nº 38/2013); Diretrizes para a implementação de repositórios arquivísticos digitais confiáveis (Resolução CONARQ nº 43/2015, que alterou a Resolução CONARQ nº 39/2014).

No âmbito da administração pública estadual, o APESP elaborou em 2009 o documento base para uma política de preservação digital - a Instrução Normativa APE/SAESP nº 1/2009 - posteriormente atualizada pela Portaria APESP/SAESP nº 4/2021.

De fato, uma política de preservação de documentos digitais exige a definição de estratégias, procedimentos e técnicas de preservação digital com sustentação legal, bem como recursos financeiros, humanos e tecnológicos, que assegurem o armazenamento e segurança dos documentos digitais pelo tempo que for necessário.

A sustentabilidade da política de preservação também depende da manutenção e atualização permanente da infraestrutura tecnológica visando controlar os riscos decorrentes da degradação do suporte, da obsolescência tecnológica e da dependência de fornecedores ou fabricantes. Esses riscos podem ser controlados com condições ambientais e de armazenamento adequados, técnicas de preservação digital e utilização de soluções independentes e de padrões abertos de formatos de arquivo, de ampla aceitação por organismos oficiais e de recursos tecnológicos estáveis e consolidados no mercado.

As ações de preservação são contínuas e devem ser implementadas e monitoradas desde a produção dos documentos por sistemas informatizados confiáveis, tanto para realizar a sua gestão quanto para assegurar sua preservação e promover a sua difusão. Mesmo porque os documentos, dados e informações produzidos, coletados e armazenados no âmbito governamental apoiam as atividades dos órgãos públicos e servem também de evidência dessas atividades para todos os fins do direito.

Para que seja possível assegurar o valor probatório dos documentos, dados e informações governamentais, é necessário preservar seus atributos arquivísticos, em especial sua autenticidade, aferida por meio da relação orgânica que mantêm com as funções e atividades que lhes deram origem e com o conjunto do qual fazem parte, e a sua autenticidade. A autenticidade dos documentos não pode ser baseada unicamente em recursos tecnológicos, pois é necessário associar as soluções tecnológicas a políticas, procedimentos e informação (na forma de metadados), bem como levar em conta a reputação idônea e a credibilidade da entidade produtora e custodiadora.

Os especialistas também alertam para a necessidade de auditoria e certificação dos sistemas informatizados, tanto os de gestão quanto os de preservação, a fim de se verificar a sua conformidade com os padrões pré-estabelecidos e, consequentemente atestar a sua confiabilidade (BERNARDES, 2018).

Na cadeia de preservação todos os órgãos e entidades da Administração Pública Paulista que produzem, recebem ou acumulam documentos digitais no exercício de suas funções e atividades têm o dever de exercer a função de custodiador confiável e respondem pela implementação dos requisitos arquivísticos e técnicos nos sistemas de produção, gestão, armazenamento, preservação e disponibilização de documentos digitais sob sua responsabilidade.

Cabe aos custodiadores confiáveis assegurar a autenticidade dos documentos digitais ao longo do tempo, e implementar todos os requisitos técnicos e arquivísticos para a sua preservação: 1. Nos próprios sistemas de produção e gestão de documentos nato-digitais e híbridos, preferencialmente no Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD); 2. Em repositórios arquivísticos

digitais confiáveis de documentos intermediários; 3. Em repositórios arquivísticos digitais confiáveis de documentos de guarda permanente.

Cabe ao APESP propor critérios que orientem a definição da melhor forma de armazenamento das séries documentais em cada fase do ciclo de vida, considerando os prazos de guarda e destinação oficializados em tabelas de temporalidades e eventuais restrições de acesso.

A preservação segura de documentos em idade intermediária de longa duração ou permanente exigem investimentos contínuos em soluções tecnológicas complexas - os Repositórios Arquivísticos Digitais Confiáveis (RDC-Arq) - a serem implementados em conformidade com os requisitos técnicos e administrativos recomendados por diretrizes e normas nacionais e internacionais.

## 11.1. Repositório Arquivístico Digital Confiável (RDC-Arq)

O Arquivo Público do Estado vem utilizando como referência técnica para a implementação de repositório arquivístico digital confiável o modelo OAIS, as orientações do Projeto InterPARES, as recomendações do Conselho Internacional de Arquivos e do Conselho Nacional de Arquivos que tratou do tema na Resolução CONARQ nº 43/2015, que alterou a Resolução CONARQ nº 39/2014, que define diretrizes para a implementação de repositórios arquivísticos digitais confiáveis.

Os repositórios arquivísticos digitais confiáveis são constituídos por um conjunto de procedimentos normativos e técnicos, disciplinados por uma política de governança de dados e objetos digitais, que definem a gestão de processos, subsidiam a escolha de tecnologias e estabelecem uma matriz de responsabilidade para os órgãos e setores envolvidos na preservação digital.

A infraestrutura organizacional de um repositório arquivístico digital confiável é composta por:

- protocolos de tratamento e armazenamento de dados;
- protocolos de tratamento e armazenamento de objetos digitais, que compreendam aspectos físicos e lógicos;
- protocolos que padronizem a documentação de decisões, escolhas de soluções e processamentos que interfiram, direta ou indiretamente, nos dados e objetos digitais;
- elementos de *hardware*;
- elementos de *software*;

- rigoroso controle de acesso aos ambientes de armazenamento de preservação, tratamento e acesso.

Neste escopo, uma infraestrutura tecnológica robusta desempenha função capital no repositório arquivístico digital confiável. Embora o repositório não se resuma a qualquer solução informatizada para armazenamento, seja uma solução de *hardware* ou *software*, estes componentes são fundamentais para apoiar a confiabilidade do acervo nele mantido.

Após estudos e avaliações o Arquivo Público do Estado optou por utilizar duas soluções desenvolvidas em conformidade com as normas e requisitos arquivísticos e com o modelo OAIS: o *Archivematica* enquanto uma plataforma de microsserviços que apoiam a gestão do repositório, em especial os processos de admissão e arquivamento no ambiente de preservação, e o AtoM enquanto uma plataforma de acesso.

Os critérios que definem como é feito o armazenamento dos objetos digitais no repositório são elaborados em consonância com:

- a política de acesso, conforme legislação vigente;
- a política de cópias de segurança;
- a política de *backup*.

Para segurança do repositório a infraestrutura deve estabelecer ambientes distintos para funções específicas, instalados, preferencialmente, em dispositivos tecnológicos dedicados, na seguinte conformidade:

- Ambiente de quarentena: ambiente restrito de armazenamento temporário, destinado à verificação de erros e varredura de vírus em documentos digitais recebidos de órgãos e entidades externos à rede segura do repositório;
- Ambiente de produção: ambiente controlado que armazena informações, objetos digitais e dados referenciais, de documentos ainda em tratamento;
- Ambiente de preservação: ambiente com rigoroso controle de acesso, que armazena informações de conteúdo e de descrição de preservação que já passaram pelo tratamento mínimo exigido para o ingresso no ambiente de preservação. Neste ambiente são armazenadas as matrizes e derivadas de acesso;
- Ambiente de acesso: ambiente restrito que armazena as derivadas de acesso ostensivas. As derivadas são acessadas pelo público interessado por meio de um *software* de acesso. Este ambiente pode ser

instalado em servidor público para viabilizar a disponibilização da plataforma de acesso na internet.

A finalidade do repositório arquivístico digital confiável é manter autênticos, preservar e prover a disponibilização e acesso de longo prazo aos documentos, dados e informações digitais.

Os repositórios arquivísticos digitais confiáveis devem, para o efetivo alcance de resultados, estar integrados a uma política de gestão de documentos dados e informações que estabeleça estratégias sustentáveis de armazenamento, manutenção e tratamento arquivístico dos documentos digitais e suas respectivas informações de descrição em conformidade com os requisitos técnicos e administrativos recomendados por diretrizes e normas nacionais e internacionais.

Para ser arquivístico e confiável, um repositório arquivístico digital deve:

- Garantir a autenticidade dos documentos digitais desde a admissão, assegurando que não sejam manipulados, alterados ou falsificados;

- Ser estruturado com processos auditáveis e com estratégias que apoiem a presunção de autenticidade dos documentos digitais custodiados, tais como: a elaboração de manuais e o monitoramento de segurança de procedimentos de preservação; o registro, em metadados, das intervenções de preservação em cada documento; e o controle rigoroso do processo de submissão dos documentos digitais ao repositório;

- Assegurar a organização hierárquica e a recuperação dos documentos digitais, de forma a manter a relação orgânica entre eles;

- Garantir a independência do repositório de forma que seu funcionamento e o acesso aos documentos não dependam das aplicações que funcionam em conjunto com ele;

- Assegurar a conformidade com as normas e padrões estabelecidos, de forma a possibilitar níveis de interoperabilidade com outros repositórios digitais e sistemas informatizados que tratam de documentos arquivísticos;

- Assegurar a custódia ininterrupta dos documentos arquivísticos;

- Garantir que o conteúdo dos documentos arquivísticos e as anotações e elementos da forma documental não sofram alterações após a reprodução;

- Definir as responsabilidades das unidades administrativas e dos profissionais que nelas atuam que gerenciam os repositórios arquivísticos digitais confiáveis;

- Implantar sistemas de controle que incluam restrições de acesso físico a locais onde os computadores estão guardados, bem como restrições de acesso aos documentos digitais nos dispositivos de armazenamento, são requisitos indispensáveis à confiabilidade dos repositórios.

Cabe ao APESP propor um sistema confiável de preservação de documentos, dados e informações digitais que inclua a definição de um sistema de tratamento dos objetos digitais e de seus respectivos dados referenciais e de recuperação, além de regras e procedimentos para a produção, segurança e manutenção da acessibilidade de documentos digitais autênticos ao longo do tempo.

No que se refere à implementação de Repositórios Arquivísticos Digitais Confiáveis (RDC-Arq) e de plataformas de acesso, cabe ao APESP:

**1. Como órgão central do SAESP:**

- Definir normas e padrões para o armazenamento, segurança e preservação de documentos digitais considerados de valor permanente, conforme art.12, § 2º, do Decreto nº 64.355/2019;

- Orientar a implantação e manutenção de repositórios visando ao cumprimento dos requisitos tecnológicos e dos procedimentos do tratamento arquivístico, por meio de ações integradas de profissionais de arquivo e de TIC;

- Indicar parâmetros para garantir a autenticidade (identidade e integridade), confidencialidade, disponibilidade, acesso e preservação, tendo em vista a perspectiva da necessidade de manutenção dos acervos documentais por longos períodos ou permanentemente;

- Definir normas e procedimentos para a transferência e recolhimento de documentos digitais;

- Definir normas e procedimentos para o ingresso de documentos digitais privados de interesse público e social no repositório arquivístico digital confiável permanente do APESP;

- Propor metodologias para auditoria e certificação de sistemas de negócio, SIGAD e repositórios arquivísticos digitais confiáveis que considerem as expectativas de confiabilidade em conformidade com os requisitos técnicos e administrativos recomendados por diretrizes e normas nacionais e internacionais.

- Certificar os repositórios arquivísticos digitais confiáveis utilizados para o armazenamento de documentos digitais permanentes e intermediários de guarda longa.

**2. Como órgão custodiador confiável de documentos estaduais de guarda permanente e intermediária, conforme Decreto nº 54.276/2009:**

- Gerir o repositório arquivístico digital confiável de documentos permanentes e a plataforma de acesso ao acervo no exercício de sua atribuição legal de recolher, tratar arquivisticamente, preservar, dar acesso e difundir os documentos de guarda permanente;

- Gerir o repositório arquivístico digital confiável de documentos intermediários no exercício de sua atribuição legal de receber em transferência, tratar arquivisticamente, preservar e dar acesso aos documentos de guarda intermediária.

Os órgãos e entidades da Administração Pública Estadual responsáveis pela produção e acumulação de documentos digitais em outros sistemas de negócio, sejam eles SIGAD ou não, são responsáveis pela garantia da proteção da autoria, da autenticidade, da integridade, da disponibilidade e da legibilidade de documentos digitais, bem como por assegurar a gestão, preservação e segurança de seus documentos digitais pelos prazos de guarda definidos nas tabelas de temporalidade de documentos.

Quanto à preservação de documentos, é dever dos órgãos e entidades integrantes do Sistema de Arquivos do Estado de São Paulo (SAESP):

- Providenciar a adequação de sistemas de negócio em operação aos requisitos arquivísticos definidos pelo APESP;

- Preservar os documentos digitais intermediários e permanentes até sua transferência ou recolhimento ao repositório arquivístico digital confiável;

- Avaliar a conveniência e capacidade de desenvolvimento, implementação, gestão e manutenção de repositórios arquivísticos digitais confiáveis.

Os documentos digitais de guarda permanente devem ser preservados em repositórios arquivísticos digitais confiáveis dos órgãos e entidades estaduais ou recolhidos ao repositório arquivístico digital confiável do APESP.

## 11.2. Gestão do repositório arquivístico digital confiável e plano de preservação

O gerenciamento de documentos digitais em repositórios arquivísticos confiáveis deve ser realizado em consonância com o modelo OAIS, *Open Archival Information Sistems*, ou SAAI, Sistema Aberto de Arquivamento de Informação (ABNT, 2021), visando a garantia de sua confiabilidade.

Os procedimentos para execução de todas as funções do repositório devem ser normalizados e auditáveis, desde a submissão dos documentos digitais, até o planejamento da preservação, acesso e monitoramento de cópias de segurança, por meio de um Plano de Preservação Digital.

O Plano de Preservação Digital é o documento que define a governança institucional e estratégias sustentáveis de manutenção e preservação de documentos digitais e estabelece, entre outras coisas, a documentação técnica mínima que deve ser elaborada para assegurar a auditoria e avaliação periódica das soluções de preservação implementadas.

O APESP vem elaborando um Plano de Preservação Digital para regulamentar o funcionamento dos repositórios arquivísticos digitais confiáveis de documentos de guarda permanente e de guarda intermediária sob sua custódia.

Os órgãos e entidades que ficarem responsáveis por repositórios digitais também devem elaborar e publicar seus respectivos Planos de Preservação Digital em conformidade com as normas e recomendações do APESP, de modo a garantir confiabilidade aos documentos arquivísticos que armazenam e gerenciam.

Os Planos de Preservação Digital devem incluir:

- Estrutura organizacional e matriz de responsabilidades;
- Documentação de processos e transparência de procedimentos;
- Infraestrutura do repositório digital, protocolo de armazenamento e cópias de segurança;
- Rotinas de monitoramento e manutenção;
- Política de *backup*;
- Política de acesso.

## 11.3. Ingresso de documentos em Repositório Arquivístico Digital Confiável

Em âmbito nacional, esse tema foi objeto da Resolução CONARQ nº 24/2006, que estabelece diretrizes para a transferência e recolhimento de documentos arquivísticos digitais para instituições arquivísticas públicas. Em âmbito estadual a Instrução Normativa APE/SAESP nº 1/2009 definiu orientação geral para regular as transferências e recolhimentos de documentos digitais dos órgãos e entidades integrantes do SAESP para o APESP.

Cabe ao APESP estabelecer um padrão de metadados e os formatos de arquivos de preservação e de acesso para cada tipo de documento. Os documentos digitais com formatos de arquivos diferentes daqueles estabelecidos como padrão deverão ser normalizados ao ingressarem no repositório.

O APESP deve definir o procedimento e a tecnologia a ser utilizada na conversão dos arquivos para os formatos padronizados de preservação e acesso, bem como orientar os órgãos e entidades como deve ser feito o teste de conformidade e a documentação do processo.

Em casos excepcionais, podem ser aceitos documentos em formatos diferentes do padrão mediante avaliação de riscos; esta ação deve ser registrada no acordo de submissão.

Somente será autorizado o ingresso de documentos digitais e seus metadados aos repositórios arquivísticos digitais confiáveis caso os mesmos estejam sob a forma não criptografada e sem qualquer outro atributo tecnológico que impeça o acesso à informação.

São formas de ingresso de documentos nos repositórios arquivísticos digitais confiáveis:

- Transferência: passagem de documentos públicos do arquivo corrente para o arquivo intermediário. Os documentos intermediários que ainda aguardam o cumprimento de prazos de guarda prescricionais ou precaucionais podem ingressar no repositório arquivístico digital confiável de guarda intermediária, nos termos do artigo 16 do Decreto nº 54.276/2009.

- Recolhimento: passagem de documentos que foram considerados de guarda permanente no processo de avaliação, em função de seu valor informativo ou probatório, para o arquivo permanente. Os documentos destinados à guarda permanente podem ingressar no repositório arquivístico digital confiável de guarda permanente após o cumprimento dos prazos de guarda estabelecidos nas tabelas de temporalidade de documentos, nos termos do inciso I do art. 17 do Decreto nº 54.276/2009.

- Doação: incorporação de documentos privados de interesse público e social ao acervo do APESP. Os documentos privados de pessoas físicas ou jurídicas considerados de guarda permanente podem ingressar no repositório arquivístico digital confiável de guarda permanente, mediante declaração de interesse público e social do acervo e comprovação de que o doador dispõe do efetivo direito de posse, nos termos do inciso I do art. 17 do Decreto nº 54.276/2009.

As transferências e recolhimentos de documentos digitais também podem ocorrer no âmbito do próprio órgão ou entidade produtores desde que estejam assegurados formalmente a infraestrutura tecnológica, os recursos financeiros, corpo técnico, o Plano de Preservação publicado e a certificação do repositório arquivístico digital confiável.

Para plena implementação dos critérios de segurança, os documentos digitais de guarda intermediária e permanente devem ser admitidos e preservados em repositórios distintos, visando a melhor gestão e a redução de riscos.

Podem ingressar no repositório arquivístico digital confiável de guarda permanente:

- Documentos nato-digitais de guarda permanente recolhidos ou doados ao APESP, incluindo-se as amostragens;
- Representantes digitais de documentos não digitais de guarda permanente (matrizes e derivadas):
    - Cujos originais tenham sido recolhidos ao APESP;
    - Cujos originais tenham sido doados ao APESP;
    - Desacompanhados do original após avaliação de conveniência, oportunidade e capacidade de guarda e preservação; e
    - Digitalizados produzidos pela instituição a partir do acervo de guarda permanente por ela custodiado.

Podem ingressar no repositório arquivístico digital confiável de guarda intermediária:

- Documentos nato-digitais de guarda intermediária transferidos ao APESP, em especial os de longa guarda;
- Representantes digitais de documentos digitalizados passíveis de eliminação, conforme Portaria UAPESP/SAESP nº5/2021;
- Representantes digitais (matrizes e derivadas) de documentos originais em fase intermediária, cuja destinação final seja a guarda permanente.

Os documentos de guarda permanente podem ingressar nos repositórios arquivísticos digitais confiáveis de guarda permanente, diretamente do ambiente de produção do documento digital.

A definição do tipo de repositório apropriado para o armazenamento das diferentes séries documentais deve levar em consideração o seu uso pelo produtor durante a fase intermediária, seu tempo de guarda, seu volume e a infraestrutura disponível, bem como a capacidade de armazenamento no ambiente de produção.

## 11.4. Admissão

A admissão, compreendida de forma ampla, abrange todo o processo necessário ao ingresso de documentos, seus respectivos metadados e informações de descrição no repositório arquivístico digital confiável. Os processos dessa funcionalidade envolvem as tratativas e levantamento de informações junto ao produtor/custodiador, a preparação arquivística e computacional que antecede a extração e transmissão dos objetos digitais, o preparo e recebimento dos Pacotes de Submissão de Informação (PSI), a verificação da qualidade dos PSI e a geração dos Pacotes de Arquivamento de Informação (PAI), em conformidade com a formatação de dados e padrões de documentação estabelecidos pelo preservador.

### 11.4.1. Acordo de submissão

Assim como nos processos de recolhimento, transferência ou doação de documentos não digitais, o cumprimento de procedimentos definidos na política de gestão de documental estadual vigente deve preceder o ingresso de documentos ao APESP.

Os documentos arquivísticos digitais devem ser previamente identificados, classificados e avaliados, incluindo, no caso de documentos híbridos, os documentos não digitais que façam parte do conjunto a ser transferido ou recolhido, conforme o previsto em tabelas de temporalidade de documentos aprovadas pelo APESP e oficializadas, nos termos dos Decretos nº 29.838/1989 e nº 48.897/2004.

No caso de doação, o conjunto deve ser previamente analisado quanto à história arquivística, conteúdo, estrutura, teor informativo, condições de acesso e utilização, para fundamentar a declaração de interesse público e social dos documentos, além de ser constatado o efetivo direito de posse do doador para poder dispor dos documentos.

Após a análise de conformidade das séries documentais e o cumprimento dos prazos de guarda e destinação, as áreas técnicas farão a manifestação de interesse e conveniência, e procederão à análise dos objetos digitais e das informações de descrição associadas aos documentos digitais, para a formalização do Acordo de Submissão.

O Acordo de Submissão é o documento que reúne as informações necessárias à determinação da viabilidade de preservação e dimensionamento dos custos do ingresso, manutenção e disponibilização do acervo digital em questão.

Antes do preservador autorizar a transmissão ele deverá avaliar a capacidade de arquivamento, adequação dos recursos e infraestrutura para receber os documentos digitais. Caso haja necessidade, o ingresso de documento digital poderá ser condicionado ao aprimoramento operacional ou providência específica de infraestrutura.

O Acordo de Submissão deve prever:

- O diagnóstico da situação original, com as informações e características do conjunto sob análise incluindo:
    - A proveniência digital, sua cadeia de custódia e o histórico de modificações autorizadas. O órgão ou entidade deve registrar como foi realizada a produção, armazenamento e manutenção dos documentos no produtor/custodiador e informar se os documentos em questão são nato-digitais ou representantes digitais de documentos originais em outro suporte;
    - A análise do sistema produtor e/ou do sistema de gestão, incluindo a identificação de dados e metadados disponíveis, identificação de aspectos computacionais, estrutura dos documentos digitais, formatos, entre outras informações;
    - A indicação para cada formato da quantidade de documentos digitais em número de itens e o respectivo volume em *bytes*, e
    - Informação sobre existência de inibidores. Indicar se os documentos são criptografados, possuem certificação digital, senha de acesso ou qualquer outro tipo de proteção tecnológica que possa impedir o acesso de longo prazo destes documentos.
- O instrumento de busca e demais informações de descrição disponíveis;
- A manifestação do órgão ou entidade produtores sobre:
    - As condições de acesso, possíveis restrições, sigilo ou limitações a respeito da transferência de direitos. A informação de restrição deve ser registrada também como informação de descrição para cada documento indicado no instrumento de busca;
    - Direitos, informações como *copyright*, licenças e permissões especiais; e
    - Nome da pessoa/cargo responsável pela transmissão e posterior eliminação das informações no órgão de origem após a emissão de atestado de validação aprovando o processo de recolhimento, transferência ou doação pelo APESP.

Quanto mais consistentes forem estas informações e metadados, mais precisa será a avaliação da viabilidade de preservação e mais forte será a presunção de autenticidade. Além disso, essas informações e metadados são importantes para nortear a necessidade de ações de preservação digital no momento do recebimento (como normalização) e no futuro (como migrações).

Quando a admissão se referir a representantes digitais de documentos de guarda permanente produzidos pelo próprio APESP, o Acordo de Submissão deve ser feito com o centro/núcleo detentor dos documentos originais e, também, com o setor responsável pela digitalização do conjunto.

### 11.4.2. Preparação, extração e transmissão

Com base no diagnóstico, o preservador, em parceria com o custodiador/produtor, deve definir, para cada conjunto, quais dados e quais metadados serão preservados e como será feita a extração dos objetos digitais. Para tanto deve ser analisada a estrutura lógica do conjunto a ser recebido, considerando, entre outras questões, o padrão de nomeação dos objetos digitais e relação hierárquica dos arquivos.

Todos os componentes digitais essenciais devem ser identificados e suas relações implícitas devem ser explicitadas nos metadados antes da transmissão, visando assegurar a extração adequada dos documentos digitais, seja do sistema no qual foram produzidos ou de um sistema de armazenamento secundário.

Para assegurar a verificação da autenticidade são imprescindíveis a transferência dos metadados de identidade e integridade, junto com seus respectivos documentos, preservando-se o vínculo entre eles, e, também, a documentação relevante sobre o ambiente técnico-administrativo em que foram produzidos e mantidos.

Os metadados descritivos armazenados em sistemas de bancos de dados já existentes, devem ser exportados em arquivo de formato consagrado e documentado em norma ISO, em arquivo de formato amplamente utilizado no mercado, ou exportado em arquivo de texto simples.

Nesse caso, deve conter definições quanto à separação de valores, delimitadores de texto e sistema de codificação de caracteres, tal como se encontravam no sistema – isto é, normalizados conforme banco de dados e, portanto, estruturados na forma de múltiplas tabelas de dados, relacionadas entre si por meio de chaves de identificação; além disso, devem estar acompanhados de documentação apropriada relativa aos próprios bancos de dados, tais como Diagramas Entidade-Relacionamento (DER) e dicionários de dados, que descrevem de forma estruturada o significado, origem, relacionamento e função de cada dado ou metadado a ser recebido pelo preservador.

Cabe ao preservador realizar a verificação de integridade dos objetos recebidos de forma a garantir que não houve alteração dos dados durante o processo de transmissão. Para viabilizar este procedimento de controle, o custodiador deve preparar antes da transmissão um manifesto (lista) do lote de objetos digitais, emitido de forma automatizada, e um arquivo contendo o resultado do algoritmo de soma de verificação (*checksum*) para cada item do lote a ser definido pelo APESP.

Cabe ao órgão ou entidade preparar o pacote de transmissão, reunindo toda documentação complementar relacionada à produção, identificação e acesso dos documentos digitais (manuais, protocolos, documentos técnicos, instrumentos de controle e descrição etc.).

A transmissão deve ser realizada prioritariamente via transferência eletrônica por canal seguro. Em situações excepcionais, esgotadas as possibilidades de

transferência eletrônica, será avaliada a viabilidade e, mediante justificativa, a autorização para o recebimento a partir de uma mídia submetida ao preservador.

Os objetos digitais e demais informações de descrição recebidos serão armazenados temporariamente no ambiente de quarentena, em equipamentos especialmente preparados para esta finalidade, com controle de qualidade que inclui a verificação de erros e varredura antivírus.

Cabe ainda ao preservador, em conformidade com o modelo OAIS, executar uma nova soma de verificação e efetuar a comparação com o *checksum* gerado pelo órgão produtor antes da transmissão. O objetivo do procedimento é testar e documentar a completude de cada sessão de submissão de dados, sendo garantido ao preservador o direito de questionar o custodiador/produtor sobre o conteúdo transmitido. Este segundo *checksum* deve integrar a documentação de preservação. Em caso de falha, a transmissão deve ser refeita.

### 11.4.3. Preparo de pacotes de informação para preservação

Em conformidade com o modelo OAIS, o preservador deve armazenar os documentos digitais por meio de pacotes de informação que reúnem de forma estruturada e padronizada todas as informações que são indispensáveis à correta representação dos documentos digitais, a saber:

- Informação de conteúdo, composta pelos objetos de dados (os objetos digitais) e sua informação de representação associada. As informações de representação mapeiam o objeto de dados e são necessárias para interpretar o objeto digital e torná-lo compreensíveis à comunidade;

- Informação de descrição de preservação, que se refere aos objetos digitais, necessária à sua preservação, pois os identifica, descreve sua proveniência, o contexto, direitos de acesso e protege sua fixidez, evidenciando alterações não documentadas;

- Informação de empacotamento, que identifica e relaciona as informações de conteúdo às de descrição de preservação, encapsulando-as; e

- Informação de descrição do próprio pacote de informação, necessária ao seu gerenciamento e recuperação.

Os pacotes de informação consistem em estruturas de dados por meio das quais documentos digitais e suas respectivas informações relacionadas são transportados criteriosamente no fluxo das funções de preservação, de forma a zelar pela integridade e autenticidade dos conjuntos

De acordo com a função a ser executada - submissão, preservação ou acesso - serão gerados diferentes tipos de pacotes: os Pacotes de Submissão de Informação (PSI), os Pacotes de Arquivamento de Informação (PAI) e os Pacotes de Disseminação de Informação (PDI).

O APESP deve definir a estrutura lógica dos pacotes, de forma a padronizar a organização das informações e estabelecer uma política de nomeação dos objetos digitais, visando facilitar a gestão e recuperação da informação. Ainda, deve orientar os órgãos e entidades estaduais a estruturar o pacote de transmissão de informação de acordo com o padrão do Pacote de Submissão de Informação (PSI). Caso seja necessário agregar informações de descrição complementares ou executar operações - como normalização de formatos de preservação ou geração de derivadas de acesso, renomeação de objetos, movimentação dos arquivos para estruturas de pastas favoráveis à execução da política de *backup*, embutir metadados, entre outras – o APESP poderá finalizar a preparação dos Pacotes de Submissão de Informação (PSI).

No caso de documentos nato-digitais provenientes do SIGAD ou de outros sistemas de negócio que atendam a requisitos arquivísticos, a preparação dos pacotes pode ser facilitada e automatizada por meio do desenvolvimento de uma camada de barramento tecnológico que promova a interoperabilidade entre o sistema de gestão e o repositório de preservação.

## 11.5. Arquivamento

O arquivamento compreende todo o processo necessário ao depósito do Pacote de Arquivamento de Informação (PAI) no ambiente de preservação, bem como sua manutenção e recuperação. Inclui o gerenciamento da hierarquia de armazenamento, o monitoramento de erros, o processo de substituição de mídias de armazenamento, o processo de recuperação de desastres e a disponibilização de informações para disseminação.

### 11.5.1. Ambiente de preservação

O repositório arquivístico digital confiável deve adotar tecnologias de *hardware* e *software* apropriadas para os serviços prestados pelo preservador e estabelecer protocolos de armazenamento que definam aspectos físicos e lógicos, bem como uma política de *backup* capazes de manter autênticos os materiais digitais, preservá-los e prover a disponibilização e acesso de longo prazo aos documentos.

O preservador deve garantir que a informação a ser preservada possa ser acessada e compreendida. Para apoiar a preservação digital, deve também, asse-

gurar condições ambientais adequadas de temperatura e umidade, além de questões de segurança predial, em especial das instalações elétricas.

A organização dos Pacotes de Arquivamento de Informação (PAI) no ambiente de preservação do repositório é indispensável para o controle, recuperação e acesso aos documentos, dados e informações.

Verificada a presunção de autenticidade e adequação do PAI, os objetos digitais são depositados no ambiente de preservação do repositório digital e o preservador assume a responsabilidade de garantir a confiabilidade e autenticidade dos documentos ao longo do tempo. Caso não seja possível ao preservador garantir a autenticidade do documento, o fato deveder registrado na documentação técnica do conjunto.

O ambiente de armazenamento de preservação é rigorosamente restrito. A permissão para executar ações é autorizada somente para os administradores do repositório, contribuindo para incrementar a segurança e elevar a confiabilidade ao processo de preservação.

O preservador deve planejar a capacidade de processamento e armazenamento do repositório prevendo, no mínimo, o crescimento do acervo digital para quatro anos, incluindo os documentos digitais a serem incorporados e os representantes digitais produzidos internamente.

A proteção do ambiente de armazenamento de preservação e o acesso aos documentos digitais são assegurados por meio do fornecimento de cópias de acesso disponibilizadas via ambiente de difusão, prioritariamente, pela plataforma de disseminação de acervo.

Recomenda-se como estratégia de reforço da política de preservação digital a utilização de plataforma informatizada que apoie o processamento de objetos digitais desde o ingresso até o acesso, em conformidade com o modelo funcional ISO-OAIS.

Por todas as razões expostas, o Arquivo Público do Estado adotou o *Archivematica* como plataforma de apoio ao gerenciamento do repositório digital.[8] Constituído como um conjunto integrado de ferramentas de *software* de código aberto, o *Archivematica* permite que os usuários monitorem e controlem microsserviços que automatizam processos de preservação através de um painel baseado na *web*.

Compatível com infraestrutura em uso no APESP e com as normas descrição e preservação arquivísticas, o *Archivematica* foi projetado para manter os dados baseados em padrões de preservação digital e utiliza o *Dublin Core, METS, PREMIS*, a especificação *BagIt* da *Library of Congress* norte-americana, entre outros. Além de subsidiar, via interface gráfica de usuário, operações de ingestão de pacotes para armazenamento e também de consulta e exportação de pacotes armazenados,

8 A plataforma *Archivematica* está disponível em: https://www.archivematica.org/pt-br/. Acesso em: 14 dez. 2022.

oferece recurso de confirmações independentes como condição necessária à exclusão de pacotes armazenados e dispõe de microsserviços de processamento e verificação de objetos digitais submetidos à preservação, tais como conversão de formatos de arquivos e varredura antivírus, podendo estas tarefas serem pré-programadas em sequência operacional customizável. Outra característica desejável atendida pelo *Archivematica* é o fato de ser interoperável com outros sistemas de gerenciamento e armazenamento seguro de objetos digitais, dentre eles o AtoM e de dispor de comunidade *online* para suporte e desenvolvimento contínuos.

### 11.5.2. Estratégias de manutenção, preservação e recuperação de desastres

A preservação do acervo digital, em especial dos pacotes de informação prevê a implementação de estratégias de manutenção, preservação e recuperação de desastres. O uso de padrões amplamente disponíveis e testados é uma importante estratégia de preservação, pois aumenta a estabilidade e pode facilitar estratégias futuras de preservação.

O preservador deve limitar os formatos autorizados para ingresso de documento no repositório e/ou realizar a conversão dos documentos recebidos para os formatos padronizados. Os formatos definidos para a preservação também devem ser atualizados pelo preservador de acordo as inovações tecnológicas. Cabe ao preservador propor rotinas de monitoramento, visando identificar a necessidade de migração ou refrescamento para novos formatos.

Em caso de migração o arquivo original deve ser mantido como medida de segurança e o processo de migração deve ser documentado para permitir a avaliação de sua qualidade e para apoiar a presunção de autenticidade.

O uso de padrões deve ser adotado também para diversos aspectos da preservação como métodos de codificação, meios físicos de armazenamento, visando entre outras coisas administrar os riscos e subsidiar a superação da obsolescência tecnológica manifestada sobre os suportes de armazenamento, os formatos de arquivo e o conhecimento da comunidade de usuários.

Nenhum componente do pacote de arquivamento pode ser corrompido. Para manutenção da integridade, o preservador deve implementar um processo de verificação de erros, para tanto todos os procedimentos executados devem fornecer notificações na forma de registros padronizados (*logs*), subsidiando a avaliação dos responsáveis pelo repositório e a adoção das medidas corretivas cabíveis.

O processo de recuperação de desastres fundamenta-se prioritariamente na adoção de estratégias de cópia de segurança, *backup* e armazenamento externo, em endereço geograficamente distinto.

## 11.6. Disseminação

A disseminação compreende todos os serviços e processos que possibilitam ao usuário encontrar informações sobre o documento digital em um repositório e visualizar seu conteúdo.

A acessibilidade contínua é um dos principais objetivos do processo arquivístico.

O preservador deve garantir a acessibilidade contínua dos documentos digitais com a maior responsabilidade, em conformidade com a legislação vigente, pois facultar o acesso seguro é um componente essencial da cadeia de preservação.

O ambiente de armazenamento de preservação é rigorosamente restrito. Por esta razão o acesso do usuário não deve colocar em risco o ambiente de preservação e os pacotes de arquivamento de informação (PAI) devem permanecer protegidos.

Os Pacotes de Disseminação de Informação (PDI) devem conter as informações necessárias ao acesso, em especial documentos em formatos que facilitem a compreensão pela comunidade de usuários e informações de descrição produzidas em conformidade com a Norma Internacional de Descrição Arquivística (ISAD) (CIA, 2000) e outras normas complementares adotadas pelo APESP, visando potencializar o compartilhamento e aproveitamento das informações e do acervo disponibilizado.

Cabe ao custodiador garantir o acesso e respeitar as restrições nos termos da lei. O repositório arquivístico digital confiável estruturado conforme o modelo OAIS contribui com o cumprimento das exigências da LAI, LGPD e demais normativas, mantendo a restrição nos casos cabíveis ao mesmo tempo que facilita o acesso aos documentos ostensivos.

Cabe ao APESP estabelecer diretrizes para viabilizar a disseminação dos documentos digitais preservados como cópias autênticas do original ou rastreáveis até o original, apontando para o pacote de informação originalmente submetido, comprovando sua autenticidade.

O APESP deve estabelecer um procedimento para marcar cópias digitais fornecidas ou mantidas nas entidades e órgãos produtores com o objetivo de evitar que o conjunto ingresse novamente no repositório do APESP.

O APESP deve regulamentar o acesso de seus usuários aos repositórios arquivísticos digitais confiáveis sob sua reponsabilidade, estabelecendo perfis e permissões de acesso criteriosas.

Além de uma plataforma informatizada que apoie o processamento de objetos digitais, recomenda-se também como estratégia de reforço da política de preservação digital, a utilização de plataforma informatizada de acesso que apoie os serviços de disseminação do acervo de forma criteriosa.

Pelas razões expostas, o Arquivo Público do Estado adotou, como plataforma de acesso, o AtoM (*Access to Memory*).[9] Trata-se de um *software* de uso livre e de código aberto, compatível com a infraestrutura em uso no APESP e com as normas descrição arquivística.

O AtoM possibilita a renderização de representantes digitais, a importação de dados e objetos por linha de comando e oferece possibilidade de exportação de dados por interface de usuário. Além destas funcionalidades, o AtoM facilita a integração da descrição e pesquisa para diferentes tipos de acervo; possui arquitetura compatível com necessidades especiais de acessibilidade; e dispõe de comunidade online para suporte e desenvolvimento contínuos. Desenvolvido em linguagem de programação e linguagem de Sistema de Gerenciamento de Banco de Dados (SGBD) amplamente difundidas, o AtoM é interoperável com aplicações de *Business Intelligence* (BI), fornece interface multilíngue facilmente customizável e, também, dispõe de funcionalidade de descrição multirepositorial.

## 11.7. Armazenamento, cópias de segurança e *backup*

O avanço crescente das TIC traz como consequências a redução relativa dos custos de produção de dados e arquivos digitais, bem como a facilidade com que podem ser replicados e transferidos de um equipamento ou sistema a outro. Isto, todavia, não se reflete diretamente no barateamento dos custos de armazenamento, especialmente quando se trata de preservação arquivística de documentos digitais.

Primeiro porque a facilidade de produção tem provocado um aumento vertiginoso dos dados e arquivos digitais sujeitos a armazenamento, e, segundo, pelo alto investimento que deve ser feito para a garantia do armazenamento seguro de tais dados e arquivos, o que inclui não apenas observância à capacidade de armazenamento, mas também ao acompanhamento do processo contínuo de inovação tecnológica, que exige a renovação, aprimoramento e ampliação periódica de toda a infraestrutura.

No contexto da política de preservação digital as cópias de segurança e os *backups* devem preservar os documentos e as suas informações relacionadas para o caso de necessidade de recuperação em decorrência da perda provocada por danos ou desastres e devem ser implementadas como complemento indispensável das atividades de preservação.

Como a simples duplicação dos objetos digitais não garante a preservação, as cópias de segurança e os *backups* devem priorizar sempre que possível os pacotes de arquivamento de informações. Para tanto o APESP deve propor uma estrutura

9 A aplicação AtoM está disponível em: https://www.accesstomemory.org/pt-br/. Acesso em 14 dez. 2022.

de armazenamento que compatibilize a estrutura dos pacotes de informação de preservação com a política e rotinas de *backups*, racionalizando o trabalho de processamento e otimizando capacidade de guarda.

Cabe ao preservador garantir o armazenamento do conjunto primário - constituído pelos documentos nato-digitais e representantes digitais originais - separado das cópias de segurança e *backup*, além de dispor de estratégias adicionais como armazenamento não-digital e o armazenamento externo, e garantir investimento contínuo no planejamento, aquisição e gestão da infraestrutura.

### 11.7.1. Armazenamento do acervo digital primário

O armazenamento do acervo digital primário, composto por documentos nato-digitais e representantes digitais originais, é prioritário e condição necessária à preservação do acervo digital, e por esta razão deve ser feito em dispositivo de alta capacidade, dedicado, instalado localmente e disponível online, ou seja, acessível por equipamentos na rede interna da instituição, com rigoroso controle de acesso.

O preservador deve providenciar a redundância do acervo digital primário por meio de cópias de segurança e *backup*, pois mesmo atendendo a todos os requisitos de preservação digital, o armazenamento está sujeito a riscos, por ação intencional ou acidental, o que pode ocasionar perdas irreversíveis.

### 11.7.2. Produção, armazenamento e gestão de cópias de segurança

O preservador deve elaborar uma política de cópia de segurança que defina quais dados e objetos digitais serão copiados, a periodicidade de acordo com a frequência com que os objetos são atualizados ou requisitados para processamento e acesso, o local no qual as cópias de segurança serão armazenadas e os responsáveis pela rotina de cópia e recuperação em caso de necessidade.

Por cópias de segurança entende-se a cópia simples de acervo digital, não compactada, armazenada em dispositivo de alta capacidade, preferencialmente dedicado, instalado localmente e disponível *online* na rede interna da instituição, com permissão restrita de acesso. A cópia deve, preferencialmente, ser executada por processo automático e em área ou dispositivo dedicado, com permissão restrita de acesso.

A cópia de segurança dos ambientes de produção e quarentena deve ter uma periodicidade menor, considerando a alta frequência de alteração dos dados e objetos digitais em tratamento. A cópia de segurança do ambiente de preservação, por ser mais estável, pode ser feita com menor frequência.

A cópia por espelhamento pode também ser adotada de forma complementar, em especial para o ambiente de produção ou de acesso, com a finalidade de

disponibilizar em tempo real as alterações operadas sobre os arquivos. A cópia por espelhamento serve para garantir o acesso quando uma falha acontece no dispositivo principal de armazenamento.

### 11.7.3. Produção, armazenamento e gerenciamento de *backup*

O preservador deve elaborar uma política de *backup* que defina quais dados e objetos digitais são prioritários para criação de *backups*, o tipo de *backup* a ser adotado pela instituição, a periodicidade de acordo com a frequência com que os objetos são atualizados ou requisitados para processamento e acesso, o local de armazenamento e os responsáveis pela rotina de *backup*, de monitoramento para verificação de integridade e de recuperação, em caso de necessidade.

Entende-se por *backup* um método de armazenamento digital realizado por meio de compactação e, portanto, sem disponibilidade de acesso imediato, sendo geralmente mediado por um sistema dedicado, com funcionalidades próprias à execução e gerenciamento do processo de compactação e descompactação de arquivos.

O processo de geração de arquivos de *backup* deve, obrigatoriamente, ser executado e armazenado em área ou dispositivo dedicado, de alta capacidade, instalado localmente e disponível *online* na rede interna da instituição, com permissão restrita de acesso.

É recomendável também que o *backup* seja replicado em dispositivos de armazenamento fora da rede de computadores (*offline*) e fora da rede elétrica, como em fitas magnéticas de tecnologia de armazenamento de padrão aberto *Linear Tape-Open* (LTO).

Os *backups* em fitas magnéticas constituem uma forte estratégia de recuperação de desastres, por serem geralmente mais resistentes a choque do que as unidades de disco, por permitirem a portabilidade, viabilizando o transporte fácil para o armazenamento em local distinto ou até externo à instituição, além de não serem vulneráveis à propagação de vírus e flutuações no fornecimento de energia elétrica.

### 11.7.4. Armazenamento em suporte não-digital: alternativas ao *backup*

O armazenamento em suporte não-digital, como microfilmes, deve ser considerado como alternativa de preservação, considerando os custos de armazenamento seguro de acervos digitais de guarda permanente e as implicações da obsolescência e da inovação tecnológica contínuas.

A reprodução em suporte não-digital não deve comprometer:

- A disponibilidade de espaço, sendo preferível portanto a cópia em microfilme;

- As características dos acervos digitais originais, sendo, portanto, impraticável para acervos digitais com funcionalidades próprias, tais como arquivos com recursos interativos ou de animação;

A migração para suporte não-digital pode vir a comprometer a forma de apresentação dos acervos digitais originais quanto à cromia (no caso, conversão de padrão colorido para preto e branco). Esse comprometimento pode ser tolerado desde que isso não represente perda significativa de conteúdo.

A migração para suporte não-digital fica condicionada à identificação individual de cada imagem em planilha eletrônica, de modo que a digitalização do microfilme possa subsidiar facilmente o processamento para a geração digital de derivadas de acesso.

### 11.7.5. Armazenamento externo para cópias de segurança, *backup* e microfilmes

Como medida adicional de segurança, o acervo digital de guarda permanente pode ser replicado para fins de armazenamento externo, em endereço geograficamente distinto. O armazenamento externo constitui garantia em caso de sinistro tais como alagamentos, incêndios e desabamentos.

Tanto cópias de segurança, quanto *backups* e microfilmes, podem estar sujeitos a armazenamento externo, em outras instituições, desde que o acordo de cessão da guarda seja formalmente estabelecido em instrumento juridicamente válido, em conformidade com a legislação vigente, e especifique, obrigatoriamente: o direito de acesso por parte da instituição responsável pela cessão do acervo; as condições de armazenamento necessárias à preservação, a serem garantidas pela instituição responsável pela guarda das cópias; os deveres e responsabilidades das partes; restrições de acesso, uso e manuseio; além de estipular o prazo de validade, possibilidade de renovação ou suspensão, e condições de devolução.

Cabe ao APESP monitorar e avaliar a pertinência e a conveniência dos acordos para guarda externa de cópias de segurança ou *backups* visando a segurança e preservação de acervos digitais.

### 11.7.6. Planejamento, aquisição e gestão da infraestrutura

A infraestrutura reservada ao armazenamento deve ser objeto de especial atenção, além das medidas de segurança aplicadas aos acervos digitais propriamente ditos.

O preservador deve realizar inventário dos equipamentos existentes, identificando modelo, fabricante, data de aquisição, capacidade de armazenamento, conteúdo geral armazenado, permissões de acesso, prazo de garantia e previsão de descomissionamento. O inventário deve ser acompanhado por diagramas

referentes às conexões de rede e aos circuitos elétricos implicados, de acordo com padrões de notação e símbolos consagrados e documentados.

O planejamento da infraestrutura deve contar com plano e infraestrutura de contingência, com garantia de fornecimento contínuo de energia elétrica; protocolo de respostas a sinistros (tais como falhas catastróficas de equipamento); plano de investimento contínuo à necessária renovação periódica da infraestrutura; além de plano de gestão de contratos, de modo a assegurar a conformidade com prazos de garantia de equipamentos e disponibilidade da assistência técnica por parte de fornecedores.

O modelo OAIS subsidia a estruturação de uma política primordialmente preventiva, minimizando prejuízos operacionais e financeiros. Para sua implementação eficaz, o preservador deve considerar o contexto tecnológico no qual o RDC-Arq está inserido, e acompanhar continuamente as evoluções de *hardwares* e *softwares*.

## 11.8. Digitalização do acervo de guarda permanente

Em âmbito nacional, esse tema foi objeto da Resolução CONARQ nº 31/2010, que dispõe sobre a adoção das Recomendações para Digitalização de Documentos Arquivísticos Permanentes. Em âmbito estadual, a Instrução Normativa APE/SAESP nº 1/2009 definiu orientação geral para regular a digitalização de documentos dos órgãos e entidades integrantes do SAESP para o APESP, determinando que os documentos arquivísticos de guarda permanente não podem ser eliminados após a digitalização, devendo ser recolhidos ao APESP ou preservados definitivamente pelo órgão custodiador.

A digitalização é o processo por meio do qual documentos existentes em diferentes formatos e suportes considerados convencionais são capturados e convertidos em dados que são legíveis por computador.

Projetos responsáveis de digitalização de acervos permanentes exigem um alto investimento financeiro, seja com a aquisição ou locação de equipamentos, contratação de serviços ou armazenamento seguro, além do investimento em recursos humanos necessários para o preparo adequado no material a ser digitalizado. Devem também ser considerados a complexidade e o custo do tratamento posterior à digitalização.

Por estas razões cabe ao preservador avaliar criteriosamente a seleção dos conjuntos a serem digitalizados. Em arquivos permanentes, duas finalidades justificam a digitalização:

- No contexto da preservação – e, particularmente, da conservação –, a restrição do manuseio do documento original, contribuindo assim para a preservação do acervo;

- No contexto da difusão, a promoção do amplo acesso e disseminação dos documentos (e dos instrumentos de pesquisa a eles correspondentes), bem como o intercâmbio de acervos com instituições parceiras.

O APESP se propõe a elaborar um Plano Estratégico de Digitalização, com a definição de conjuntos prioritários a serem digitalizados e com a estimativa de ampliação em *bytes* do volume armazenado, visando subsidiar a escalabilidade da infraestrutura e o planejamento da aquisição de equipamentos, insumos e contratação de serviços.

O Plano deve prever o mapeamento do processo de digitalização e dos processos de tratamento posteriores, visando o estabelecimento de métricas de volume processado, tempo de processamento e pessoal empregado (não apenas quantitativamente, mas também quanto à composição técnica das equipes).

Para elaborar o Plano Estratégico de Digitalização, os preservadores devem:

- Avaliar a melhor técnica de reprodução considerando os objetivos específicos e a análise do caso concreto, em especial a fragilidade e estado de conservação dos documentos;

- Assegurar que o conjunto a ser digitalizado tenha passado por tratamento técnico (organização, identificação, classificação, avaliação, descrição, higienização etc.) ou, em casos específicos, considerar a digitalização como uma etapa facilitadora do fluxo de tratamento técnico;

- Considerar a frequência e intensidade de uso dos documentos, o estado de conservação, o grau de degradação e obsolescência do suporte original e sua relevância para a pesquisa;

- Priorizar, no caso de documentos seriados, a digitalização de séries documentais, e não de documentos isolados, levando-se em consideração o valor probatório ou informativo do conjunto;

- Avaliar a complexidade e os recursos necessários para o tratamento técnico prévio, captura, tratamento digital posterior à digitalização - que pode implicar em custos adicionais de pessoal, ferramentas de trabalho como a licença de aplicações proprietárias ou de serviços contratados de terceiros -, armazenamento e gestão dos acervos digitais;

- Adotar requisitos e procedimentos que assegurem a geração de representantes digitais com qualidade arquivística, fidelidade ao documento original e capacidade de interoperabilidade;

- Utilizar, preferencialmente, padrões e formatos abertos e/ou estáveis no mercado, em conformidade com as normas nacionais e internacionais, garantindo a possibilidade de interoperabilidade com diferentes aplicações e sistemas;

- Utilizar padrões estabelecidos pelo APESP para a captura digital de imagens, produção de matrizes e derivadas, identificação do representante digital (padrão de metadados) e controle de qualidade, em conformidade com normas nacionais e internacionais.

## 11.9. Automação digital

A automação é um processo por meio do qual uma ação, antes dependente de intervenção humana contínua, passa a ser realizada por meio de um sistema inteiramente autônomo (automático) ou apenas parcialmente dependente de intervenção humana (semi-automático).

A automação digital de processos - *Digital Process Automation (*DPA), ou simplesmente automação digital, compreende, portanto, o desenvolvimento e uso de sistemas de computação digital visando à implementação de processos semiautomáticos ou automáticos sobre dados e arquivos digitais.

A automação digital de processos em arquivos deve ser orientada à preservação, devendo garantir, de modo geral, a qualidade arquivística dos processos automatizados. A consecução deste objetivo dependente da observância dos seguintes princípios gerais:

- Auditabilidade, que implica na disponibilidade de documentação apropriada, tanto dos instrumentos da automação, quanto das operações que automatizam, compreendendo-se que a garantia da cadeia de preservação depende de automação documentada.

- Processualidade, segundo a qual o desenvolvimento de soluções com operacionalidade (propósito e utilidade) precede aquelas que possuam usabilidade apenas, compreendendo-se que soluções complexas evoluem de soluções mais simples, e não o inverso.

- Homogeneidade, o que significa que entre programas distintos deve haver consistência entre os problemas que se apresentam e as soluções que o resolvem, compreendendo-se que problemas análogos se resolvem com soluções análogas.

- Escalabilidade, que corresponde à capacidade de um programa em operar com lotes de arquivos variáveis quanto ao seu volume, e que implica em que parâmetros de execução quantitativos independam do código-fonte de um programa.

- Generalidade, que corresponde à capacidade de um programa em operar com lotes de arquivos variáveis quanto ao seu tipo, e que implica em que parâmetros de execução qualitativos independam do código-fonte de um programa.

- Singularidade, que corresponde à característica de um programa de realizar apenas uma tarefa, a ser executada sequencialmente, ou de apresentar-se como plataforma de microsserviços com sequência operacional pré-programável, compreendendo-se que a sequência operacional independa do código-fonte de um programa.

- Interoperabilidade, que corresponde à possibilidade de que um programa, desenvolvido para um propósito ou sistema, ou que os dados a partir dos quais opera ou que retorna, sejam compatíveis com outros programas, compreendendo-se que técnicas e dados (entrada/saída) independam da infraestrutura.

- Proporcionalidade, correspondente às dimensões e complexidade dos problemas, em relação à capacidade e aos custos das soluções que o resolvem, compreendendo-se que a capacidade da automação deva ser proporcional às condições existentes.

- Confiabilidade, que remete à garantia de integridade (e sigilo, quando for o caso) dos dados e arquivos submetidos a processamento automatizado, bem como à minimização de erro não intencional provocado por ação humana, compreendendo-se que automação orientada à preservação seja automação segura.

- Reversibilidade, que remete à possibilidade de reversão de dados e arquivos submetidos a transformações à sua condição original, compreendendo-se que a segurança depende da possibilidade de restauração ou recuperação de estados prévios.

- Governabilidade, que remete ao controle e acesso aos dados e arquivos envolvidos em automação digital de processos, quando este envolver terceiros, compreendendo-se que posse e acesso aos dados e arquivos independam de fornecedores e parceiros.

- Publicidade, que enfatiza a importância da adoção de ferramentas condizentes com os preceitos da tecnologia aberta, compreendendo-se que o compartilhamento favorece o desenvolvimento e o uso das ferramentas de automação digital.

Em termos gerais, a automação é realizada mediante programas, que são os instrumentos da automação, e correspondem a uma sequência de instruções

logicamente estruturadas a serem executadas pelo computador. Consideramos dois tipos principais de programas de automação digital:

- *Scripts*, que são desenvolvidos em linguagens de programação interpretadas e cuja execução depende de uma aplicação capaz de interpretar as instruções fornecidas;

- Aplicações (ou aplicativos), que são desenvolvidos em linguagens de programação compiláveis, gerando arquivos executáveis que independem de aplicativo interpretador.

Tais programas distinguem-se, ainda, quanto ao escopo de seu propósito:

- Programas de propósito único (*single purpose* ou *single task*), isto é, que realizam uma única tarefa e apenas uma;

- Programas de propósito múltiplo (*multipurpose* ou *multitask*), isto é, que integram múltiplas tarefas em uma única solução;

- Plataformas de automação digital, correspondentes a pacotes de microsserviços (subprogramas de propósito único) a serem combinados em sequências operacionais pré-programáveis.

As operações técnicas sujeitas à automação podem ser parcialmente ou inteiramente automatizáveis. Operações técnicas parcialmente automatizáveis incluem:

- Controle de dados gerenciais de processamento de acervo, digital e não-digital (registro de data e hora de início e conclusão do processamento, p.ex.);

- Captura digital de acervo para conversão em imagem digital, ou seja, trata-se do próprio processo de digitalização, parcialmente automatizável para o caso da digitalização de folhas, fotos ou de rolos de microfilme;

- Coleta de dados de identificação preliminar de acervo, digital e não-digital, para processamento posterior (número da página, data e local de publicação, p.ex.);

- Controle de dados de classificação, descrição e indexação de acervo, digital ou não-digital (tais como grupos e séries a que pertencem os acervos e suas dimensões e suporte, p. ex.);

- Controle de vocabulário para fins de indexação de acervo, digital e não-digital (produção de taxonomias em geral, tais como listas hierarquizadas, tesauros e listas de cabeçalho de assunto);

- Rastreamento de vocabulário controlado para fins de indexação de conteúdo de acervo digital (rastreamento de nomes, locais e assuntos, p.ex.);

- Rastreamento de imagem para fins de indexação de conteúdo de acervo digital (tais como o reconhecimento facial, de objetos retratados ou de padrões visuais repetitivos, possibilitando a identificação automática de sinaléticas de microfilme, p.ex.);

- Edição de conteúdo de acervo digitalizado (edição de imagem, áudio e vídeo, tais como recorte, alteração de brilho e contraste, correção de inclinação e abaulamento, p. ex.);

- Localização, substituição e extração de expressões regulares em cadeias de texto (expressões com códigos e sinais regulares, como CEP, RG e CPF, p. ex.);

- Localização e ocultação de dados sigilosos e anonimização de dados pessoais;

- Modelagem de dados de acervo, digital e não-digital, visando importação em sistemas de bancos de dados (isto é, a preparação de dados para que se adequem a bancos de dados).

- Cadastro, atualização cadastral e análise de dados de cadastro de consulentes, visando a produção de informação estatística conveniente ao planejamento das operações técnicas e a melhoria de serviços.

- Atendimento presencial e remoto de consulentes e registro e acompanhamento de solicitações, visando ao controle, transparência e eficiência dos serviços prestados ao cidadão, bem como o controle de dados e informações de caráter gerencial.

As operações inteiramente automatizáveis, muito embora possam envolver procedimentos manuais de preparação ou de inicialização a serem executados manualmente, incluem:

- Controle de dados gerenciais de processamento de acervo digital (registro de data e hora de início e conclusão do processamento, p.ex.);

- Tarefas específicas de manipulação de dados estruturados (tais como conversão de formatos de data, alteração de caixa alta para baixa, localização, substituição, combinação e segmentação de cadeias de texto, p. ex.);

- Listagem e controle de acervo digital armazenado, para fins de gestão ou processamento posterior (com caminho e nome do arquivo, p. ex);

- Preparação de pacotes de dados referenciais de arquivos digitais (arquivos de texto simples que contêm caminho e nome de arquivos, a serem lidos por outros programas, servindo assim de parâmetro para a sua execução);

- Renomeação, realocação, duplicação, exclusão e comparação de arquivos digitais;

- Edição de conteúdo de acervo digitalizado (edição de imagem, áudio e vídeo, tais como recorte, alteração de brilho e contraste, correção de inclinação e abaulamento, p. ex.), quando independem de verificação visual;

- Conversão de formato de arquivos digitais (entendido como extensão de arquivo, tais como .jpg, .tif e .pdf, .pdf/a, p. ex.);

- Combinação de arquivos diferentes em um único arquivo (combinação de arquivos de imagem ou de arquivos .pdf de página única em .pdfmulti-página, ou combinação de diferentes arquivos de planilha eletrônica em planilha única p. ex.);

- Reconhecimento Ótico de Caracteres (OCR), a ser embutido no próprio arquivo ou extraído para arquivo externo;

- Reconhecimento de voz (em áudio e vídeo) com conversão para texto, com ou sem tradução (ou seja, a transcrição de áudio);

- Reconhecimento de texto com conversão em áudio, com ou sem tradução (ou seja, a leitura em "voz alta" por vocalização pré-programada);

- Obtenção de metadados de sistema para diagnóstico simples de acervo digital (data de criação, formato do arquivo e permissões a ele associadas, p.ex.);

- Geração de soma de verificação de integridade mediante execução de algoritmo pré-programado (*checksum*/*hashcode)*;

- Importação e exportação de metadados embutidos (tais como as referências de equipamentos e programas empregados no processo de digitalização do acervo);

- Importação e exportação de metadados descritivos, de taxonomia, de objetos digitais em sistemas de gerenciamento eletrônico de documentos, sistemas de gerenciamento de documentos eletrônicos, sistemas de gerenciamento de repositório digital e sistemas de acesso e difusão de acervo;

- Controle de acervo digital e não-digital armazenado em depósito (identificação e localização de caixas de acervo não-digital e de dispositivos móveis de armazenamento de acervo digital);

- Geração e gestão de arquivos de *backup* (agendamento de ações para produção, atualização e exclusão de arquivos de *backup* e controle de arquivos de *backup* existentes, p. ex.);

- Transporte de acervo digital, via transmissão de dados por canal seguro, em substituição ao transporte físico de mídias de armazenamento móvel, sujeitas a extravio e dano.

- Acompanhamento e registro de acesso aos sistemas de difusão e acesso, visando à produção de informação estatística conveniente ao planejamento das operações técnicas e a melhoria de serviços.

# 12 Segurança da informação e gestão de riscos

Em âmbito nacional, o Decreto nº 9.637/2018, alterado pelo Decreto nº 10.641/2021, instituiu a política nacional de governança e segurança da informação, com previsão de fomento às atividades de pesquisa científica e de desenvolvimento tecnológico, aprimoramento do arcabouço legal e normativo, formação e qualificação de recursos humanos e fortalecimento da cultura de segurança da informação.

A política de segurança da informação é transversal e sistêmica e demanda ações contínuas de integração, cooperação, intercâmbio e prevenção com vistas a garantir a segurança, o tratamento e a proteção de documentos, dados e informações sigilosas e pessoais custodiados pela administração pública.

Esses conjuntos de documentos, dados e informações governamentais precisam permanecer confiáveis para proteger direitos coletivos e individuais, para subsidiar as ações necessárias à implementação de políticas públicas e para garantir a preservação de acervos permanentes.

Em âmbito estadual, o tema foi abordado pelo Arquivo Público do Estado em sua Instrução Normativa nº 1/2009 que definiu conceitos e orientações gerais para a segurança de documentos digitais, com a previsão de controles de acesso, trilhas de auditoria e procedimentos de segurança capazes de garantir a proteção dos documentos digitais contra perdas, acidentes e intervenções não autorizadas.

Mais recentemente, a Deliberação Normativa CGGDIESP nº 1, de 30 de dezembro de 2011 instituiu a Política de Governança de Dados e Informações - PGDI, no âmbito da Administração Pública Estadual. Merece destaque, contudo, observar que a segurança da informação nesse contexto normativo refere-se especificamente à elaboração e atualização da Política de Proteção de Dados Pessoais, sob responsabilidade do Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo, nos termos do art. 3º do Decreto nº 65.347, de 9 de dezembro de 2020.

A política de segurança da informação é um conjunto de diretrizes e ações necessárias para assegurar a autenticidade, integridade, confidencialidade e disponibilidade dos documentos, dados e informações digitais, para todos os fins administrativos e jurídicos

A autenticidade é a credibilidade de um documento enquanto documento, isto é, a qualidade de um documento ser o que diz ser e que está livre de

adulteração ou qualquer outro tipo de corrupção (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, V). A integridade é o estado dos documentos que se encontram completos e que não sofreram nenhum tipo de corrupção ou alteração não autorizada nem documentada (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XXXIX). A confidencialidade é a propriedade de certos dados ou informações que não podem ser disponibilizados ou divulgados sem autorização para pessoas, entidades ou processos (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XVI). A disponibilidade é a qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados (Decreto nº 58.052/2012, art. 3º, X).

O controle de acesso e a recuperação de documentos digitais e seus metadados devem ser implementados por meio de procedimentos de identificação de usuários, com base nas credenciais de segurança e por procedimentos que limitem aos responsáveis o acesso aos ambientes de armazenamento.

O controle de acesso aos documentos arquivísticos digitais sigilosos deve prever a classificação da informação quanto ao seu grau de sigilo, nos termos da lei, bem como a utilização de procedimentos adicionais de segurança, tais como assinatura e certificação digitais, criptografia ou mesmo a guarda de documentos fora da rede.

A assinatura e a certificação digitais devem utilizar infraestrutura de chaves públicas, nos termos da lei, observadas as disposições do Decreto Estadual nº 48.599/2004, que regula a contratação da prestação de serviços de certificação digital no âmbito da Administração Pública Estadual.

As intervenções ou tentativas de intervenções feitas nos documentos arquivísticos digitais ou no sistema computacional devem ser registradas de modo a permitir que possam ser rastreadas em trilhas de auditoria. As trilhas de auditoria devem estar disponíveis para inspeção e não podem ser excluídas antes dos prazos previstos nas tabelas de temporalidade de documentos oficializadas, mesmo que implique em transferir cópia da trilha para outro espaço de armazenamento com a subsequente liberação do espaço original.

As cópias de segurança de documentos arquivísticos digitais e seus metadados, bem como de parâmetros do sistema operacional, do gerenciador de banco de dados, do sistema informatizado de gerenciamento e do *software* aplicativo, devem ser realizadas regularmente e de acordo com as necessidades específicas, visando garantir a recuperação dos documentos, em caso de sinistro ou falhas nos sistemas computacionais. As cópias de segurança devem ser armazenadas em locais diferentes e fisicamente distantes.

A segurança da infraestrutura de instalações do acervo arquivístico digital e de sistemas gerenciadores deve levar em conta o controle de temperatura e umidade relativa do ar, a iluminação, o fornecimento estável de energia elétrica, a instalação

e manutenção de equipamentos contra incêndio e de para-raios, e o controle de acesso às salas de computadores servidores por profissionais credenciados.

Os sistemas informatizados que gerenciam ou armazenam documentos arquivísticos digitais devem observar requisitos de autoproteção definidos por organismos nacionais e internacionais de ampla aceitação e reconhecimento, bem como devem interagir com outros sistemas de proteção, tais como antivírus, *firewall*, *anti-spywere*.

Entretanto, não é possível garantir uma proteção total contra todas as ameaças (conhecidas ou não), sendo necessário implementar um processo para identificar, gerenciar e controlar as possíveis ameaças e vulnerabilidades dos sistemas e informações, e as contramedidas necessárias para reduzir o efeito destas ameaças para um nível aceitável por meio da aplicação de um processo conhecido como gestão de riscos.

Na gestão de riscos, os tipos de ameaça devem ser identificados. As ameaças naturais ocorrem por fenômenos da natureza, as involuntárias ocorrem por erros inconscientes e não propositais, e as voluntárias são causadas por agente humano de maneira consciente e proposital.

Além disso, é preciso identificar as vulnerabilidades, que podem ser: as instalações físicas fora do padrão; obsolescência, defeitos, manutenção, garantia de *hardware*; configuração, instalação, atualização, *bugs* em *softwares*; falta de treinamento, sabotagens e erros humanos; localização geográfica, e outros.

Essa análise é feita por meio de ferramentas de controle de prevenção, com as contramedidas recomendadas para mitigar as ameaças aos ambientes de produção e armazenamento, que podem colocar em risco a autenticidade, integridade, confidencialidade e disponibilidade dos documentos, dados e informações.

Os controles de prevenção são resultado de uma combinação de políticas, procedimentos, estrutura organizacional e mecanismos de medida física ou de *hardware* e *software*, e podem ser divididos em:

- preventivos, que buscam antecipadamente evitar o incidente, impedindo ou desencorajando as tentativas de violação da segurança. Medidas como os controles de acesso, encriptação e autenticação são exemplos de controles preventivos;

- detectáveis, que identificam as condições e indivíduos causadores da ameaça, notificando a violação ou tentativa de violação da segurança. São exemplo os sistemas de auditoria, métodos de deteção de intrusões, as somas de verificação (*checksums*) e outros; e

- corretivos, que evitam que novas ameaças aconteçam pela correção de problemas já identificados.

Os controles de prevenção variam de contexto organizacional para outro, pois cada organização é distinta das demais, dependente de recursos financeiros e humanos específicos, da sua história e competências.

Tendo em consideração a particularidade de cada instituição, podemos citar como exemplos de barreiras de segurança algumas medidas que visam, por exemplo, desencorajar, desmotivar e desestimular crimes ou atos de vandalismo, como as câmeras de vídeo, alarmes, campainhas e uniformes; dificultar o acesso indevido por meio de roletas, gaiolas com detectores de metal, portas com leitores de cartão magnético, senhas, certificados digitais, criptografia, *firewall*; discriminar, ou seja, cercar de recursos que permitam a identificação e o acesso, como perfil de usuário, permissões, limites, perímetros físicos, cotas de recursos (impressão, disco etc.); detectar, monitorar, auditar e alertar detecções de ameaças, como tentativa de invasão, descumprimento de normas de segurança, cópia ou envio de informações sigilosas, intrusos; deter e impedir que a ameaça atinja seu objetivo por meio de acionamento de barreira, acionamento de controle, punições, bloqueios de acesso físico e lógico; diagnosticar e mapear a falha para proposição de melhorias, analisar a ocorrência, identificar as causas.

Para consolidar a política de segurança da informação é necessário revisar e aprimorar os processos continuamente, com comprometimento das lideranças, conforme estabelece a norma NBR ISO/IEC 27001 (ABNT, 2013), estabelecer os objetivos da segurança da informação e incorporá-los à missão, visão e valores institucionais, e assegurar os recursos orçamentários necessários.

Do ponto de vista das experiências acumuladas pelo APESP, observa-se dois grandes riscos à segurança da informação. O primeiro deles, diz respeito aos perigos relacionados à infraestrutura tecnológica, à instabilidade da rede elétrica e à perda irreversível dos servidores. Para fazer frente a esses perigos, o APESP tem se empenhado para:

- Programar investimentos de longo prazo para a aquisição, expansão e renovação da infraestrutura;
- Realizar monitoramento sistêmico da infraestrutura tecnológica, com instalação de rede elétrica externa e de geradores;
- Exercer vigilância contínua em relação à obsolescência das máquinas, equipamentos e programas;
- Elaborar um plano de gestão de riscos, prevendo, inclusive, uma matriz de responsabilidades dos agentes envolvidos no processo;
- Elaborar um plano de migração de dados com planejamento de unidades de arquivamento.

O segundo grande risco à segurança dos documentos, dados e informações digitais diz respeito à invasão de agentes externos nos ambientes de armazenamento e aos acessos não autorizados. A esse respeito, é preciso considerar que a segurança da informação não se restringe apenas aos aspectos tecnológicos, pois a classificação de sigilo e o mapeamento de dados pessoais são considerados pressupostos lógicos para a efetividade de uma política de segurança da informação.

Nesse sentido, as soluções tecnológicas tornam-se insuficientes se não forem acompanhadas pelo tratamento de documentos, dados e informações digitais, de acordo com as orientações da política de gestão documental, com classificação de informação na origem e uma série de procedimentos rotineiros de controle durante todo o seu ciclo de vida. Ainda, é preciso fomentar a cultura da segurança, com treinamento dos profissionais e usuários, a fim de garantir a proteção necessária aos documentos, dados e informações digitais com restrição de acesso.

# 13 Acesso à informação

A Lei de Acesso à Informação nº 12.527/2011 (LAI) regulamentou dispositivos constitucionais, especialmente o art. 5º, inciso XXXIII da Constituição Federal, o qual prevê que "Todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que devem ser prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado" (BRASIL, 2022a).

A própria Constituição Federal reconhece que a gestão documental é condição necessária para a garantia do acesso à informação em seu art. 216, § 2º: "Cabem à administração pública, na forma da lei, a gestão da documentação governamental e as providências para franquear sua consulta a quantos dela necessitem" (BRASIL, 2022a).

Nesse aspecto, ressalte-se, também, que a Lei nº 8.159/1991, conhecida como a Lei de Arquivos, que regulamentou esse dispositivo constitucional, determina em seu art. 17 que "A administração da documentação pública ou de caráter público compete às instituições arquivísticas federais, estaduais, do Distrito Federal e municipais", deixando evidente o papel estratégico dos Arquivos Públicos para a garantia do direito de acesso a informações.

A principal diretriz definida na LAI é que o acesso é a regra e o sigilo é a exceção. De fato, a lei representa um grande avanço para a garantia do direito de acesso à informação, pois determinou a criação de Serviços de Informações ao Cidadão (SIC) em todos os órgãos públicos, definiu prazos para atendimento dos pedidos de acesso e exigiu a criação de instâncias recursais para avaliar as negativas de acesso à informação.

Na administração pública do estado de São Paulo a LAI foi regulamentada pelo Decreto nº 58.052/2012, que teve alguns de seus dispositivos alterados pelos Decretos nº 61.559/2015 e nº 61.836/2016. A regulamentação da LAI em São Paulo inovou ao integrar a política de arquivos à política de acesso à informação definindo um papel estratégico para o APESP na coordenação dos SIC, na gestão do Sistema SIC.SP - canal oficial do governo para registro e gerenciamento dos pedidos de acesso à informação - e na presidência da Comissão Estadual de Acesso à Informação (CEAI) instituída pelo Decreto nº 60.144/2014, que atua como última instância de recurso em âmbito administrativo.

É importante considerar que o acesso e o eventual sigilo previstos no Decreto Estadual nº 58.052/2012 referem-se, indistintamente, a "documentos, dados

e informações", produzidos em papel ou em ambiente digital. Para que os documentos digitais possam ser descritos, gerenciados, compreendidos, preservados e acessados ao longo do tempo, o decreto determinou a identificação de seus metadados e de seu contexto documental, com identificador único, instituição produtora, nomes, assunto, datas, código de classificação, tipologia documental, temporalidade, destinação, versão, documentos relacionados, idioma e indexação. O acesso também depende do contexto tecnológico em que os documentos foram produzidos, sendo necessário indicar metadados referentes ao formato e tamanho do arquivo, dependência de *hardware* e *software*, tipos de mídias, algoritmos de compressão (Decreto nº 58.052/2012, art. 3º, XVIII).

A informação armazenada em formato digital será assim fornecida, caso haja anuência do interessado. Se a informação solicitada estiver disponível ao público em formato impresso, eletrônico ou em qualquer outro meio de acesso universal, serão informados ao interessado, por escrito, o lugar e a forma pela qual se pode consultar, obter ou reproduzir a referida informação, procedimento esse que desonerará o órgão ou entidade pública da obrigação de seu fornecimento direto, salvo se o interessado declarar não dispor de meios para realizar por si mesmo tais procedimentos (Decreto nº 58.052/2012, art. 15).

O acesso a documentos digitais e bases de dados classificados como sigilosos ou com dados pessoais será permitido mediante credencial de segurança e cria a obrigação para aquele que as obteve de resguardar restrição de acesso, devendo ser responsabilizado por seu uso indevido (Decreto nº 58.052/2012, arts. 35, 36, e. 61 a 65).

Para ampliar o acesso à informação e promover a transparência ativa, a LAI determinou que os órgãos e entidades públicas devem promover, independentemente de requerimentos, a divulgação de informações de interesse coletivo ou geral por eles produzidas ou custodiadas, sendo obrigatória a divulgação em sítios oficiais da rede mundial de computadores (internet) (Decreto nº 58.052/2012, art. 8º).

Nesse sentido, no âmbito da administração estadual, para dar acesso público aos documentos digitais, aos representantes digitais de documentos digitalizados, ou às bases de dados, os sítios institucionais, o Portal da Transparência e do Governo Aberto, bem como outros canais com objetivo similar, devem atender aos seguintes requisitos: I- conter ferramenta de pesquisa de conteúdo que permita o acesso à informação de forma objetiva, transparente, clara e em linguagem de fácil compreensão; II - possibilitar a gravação de relatórios em diversos formatos eletrônicos, inclusive abertos e não proprietários, tais como planilhas e texto, de modo a facilitar a análise das informações; III - possibilitar o acesso automatizado por sistemas externos em formatos abertos, estruturados e legíveis por máquina;

IV - divulgar em detalhes os formatos utilizados para estruturação da informação; V - garantir a autenticidade e a integridade das informações disponíveis para acesso; VI - manter atualizadas as informações disponíveis para acesso; VII - indicar local e instruções que permitam ao interessado comunicar-se, por via eletrônica ou telefônica, com o órgão ou entidade detentora do sítio; e VIII - adotar as medidas necessárias para garantir a acessibilidade de conteúdo para pessoas com deficiência (Decreto nº 58.052/2012, art. 23).

Ainda, o Decreto regulamentador da LAI em São Paulo determinou a elaboração de um "Catálogo de Sistemas e Bases de Dados da Administração Pública do Estado de São Paulo - CSBD", sob a responsabilidade da Fundação SEADE, com as seguintes informações: I - tamanho e descrição do conteúdo das bases de dados; II - metadados; III - dicionário de dados com detalhamento de conteúdo; IV - arquitetura da base de dados; V - periodicidade de atualização; VI - *software* da base de dados; VII - existência ou não de sistema de consulta à base de dados e sua linguagem de programação; VIII - formas de consulta, acesso e obtenção à base de dados" (Decreto nº 58.052/2012, art. 26).

Tanto o "Catálogo" quanto as bases de dados da Administração Pública Estadual devem estar disponíveis no Portal do Governo Aberto e no Portal da Transparência, com todos os elementos necessários para permitir sua utilização por terceiros, como a arquitetura da base e o dicionário de dados (Decreto nº 58.052/2012, art. 26, § 3º).

O APESP tem atuado ao longo do tempo para que os SIGAD adotados na administração estadual (SPdoc e SP Sem Papel) tenham uma interface com o cidadão permitindo, ao menos, o acesso a documentos de seu interesse particular.

No SPdoc foi desenvolvida a interface "SPdoc Cidadão", que permite ao cidadão localizar e acompanhar seus documentos no sistema. No SP Sem Papel, é possível autorizar que interessados não usuários do sistema, como cidadãos e empresas privadas, acompanhem a tramitação de documentos. Cabe aos órgãos e entidades avaliar e autorizar a concessão desse acesso por meio da geração e envio de protocolo de acompanhamento ao interessado. O protocolo de acompanhamento permite ainda, facultativamente, franquear o acesso ao conteúdo de um documento, além da sua tramitação. Para tanto, no momento da produção de um documento deve-se utilizar modelo em que previamente foi definida essa possibilidade de acesso. Assim, torna-se possível ao responsável pela assinatura do documento autorizar ou não esse acesso por meio do protocolo de acompanhamento.

Segundo a Lei de Acesso à informação (LAI), o órgão ou entidade pública deve autorizar ou conceder o acesso imediato à informação disponível em qualquer suporte. Não sendo possível conceder o acesso imediato, o órgão ou entidade deve

comunicar a data, local e modo para se realizar a consulta, efetuar a reprodução ou obter a certidão, em até 20 dias (Lei nº 12.527/2011, art. 11).

O atendimento de pedidos de acesso à informação via SIC pode ser agilizado com emprego da digitalização de documentos, com certificação de que as cópias conferem com o original. Nesse caso, poderá ser cobrado o valor necessário do custo dos serviços de digitalização (Decreto nº 58.052/2012, arts. 16 e 17).

Embora o acesso seja a regra, a LAI e a LGPD determinam que informações digitais sigilosas ou pessoais devem ter o seu acesso restrito a pessoas autorizadas. Para proteger os documentos, dados e informações digitais sigilosas de acessos indevidos, o Decreto nº 58.052/2012 autorizou o uso de código, cifra ou sistema de criptografia para controlar sua produção e tramitação no âmbito da Administração Pública Estadual e de instituições de caráter público (arts. 40 a 51). A criptografia é definida no decreto como o "processo de escrita à base de métodos lógicos e controlados por chaves, cifras ou códigos, de forma que somente os usuários autorizados possam reestabelecer sua forma original" (art. 3º, V). Ainda, para assegurar a proteção de documentos sigilosos, os documentos digitais precisam contar com metadados de segurança, com indicação de grau de sigilo, informações sobre o sistema de criptografia adotado, assinatura digital e outras marcas digitais (art. 3º, XVIII).

O código, cifra ou sistema de criptografia também são considerados sigilosos e, por essa razão, devem ser submetidos a procedimentos especiais de segurança, com vistorias periódicas, elaboração de inventários do material criptografado, comunicação de anormalidades relativas ao sigilo e registro de indícios de violação, interceptação ou irregularidades na transmissão ou recebimento de documentos, dados e informações sigilosos criptografados (Decreto nº 58.052/2012, arts. 53 e 54). É responsabilidade do órgão que fez uso da criptografia de documentos, dados e informações digitais sigilosas providenciar a sua descriptação após a sua desclassificação de sigilo (art. 56). Importante observar que os documentos, dados e informações digitais sigilosas considerados de guarda permanente, somente podem ser recolhidos ao APESP e disponibilizados para acesso público após a sua desclassificação e descriptação, com exceção apenas de documentos permanentes de órgãos ou entidades extintas ou que cessaram suas atividades (art. 58).

Por outro lado, a restrição de acesso a documentos, dados e informações digitais relativos à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais deve ser assegurada por meio da anonimização ou pseudoanonimização. Segundo a Lei Geral de Proteção de Dados Pessoais (LGPD), a anonimização refere-se à utilização de meios técnicos razoáveis e disponíveis no momento do tratamento dos dados, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo (Lei nº 13.709/2018, art. 5º, XI).

O acesso a documentos digitais e a bases de dados por órgão de pesquisa para a realização de estudos de caráter histórico, científico, tecnológico ou estatístico deve ser autorizado, garantida sempre que possível, a anonimização de dados pessoais e de dados pessoais sensíveis (Lei nº 13.709/2018, arts. 7º e 11).

Importante também observar que o titular dos dados pessoais tem direito a requerer a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD (art.18). Cabe à Autoridade Nacional de Proteção de Dados dispor sobre padrões e técnicas utilizados em processos de anonimização (art. 12).

O compartilhamento de dados pessoais no âmbito do poder público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e entidades públicas, respeitados os princípios de proteção de dados pessoais previstos na LGPD.

No âmbito da administração estadual, a eventual autorização de acesso por terceiros a dados pessoais não anonimizados está condicionada à assinatura de um termo de responsabilidade, que dispõe sobre a finalidade e a destinação que fundamentaram sua autorização e sobre as obrigações a que se submeterá o requerente, responsabilizando-se por seu uso indevido (Decreto nº 61.836/2016, art. 15).

Para ter acesso aos acervos custodiados pelo APESP, o interessado deve se cadastrar no sítio da instituição. Em alguns casos o acesso ao acervo custodiado pelo APESP pode ser objeto de restrições. Na maioria desses casos o cidadão deve se identificar como parte interessada (titular ou herdeiro legal) ou justificar o acesso para fins de pesquisa científica. Por se tratar de documentação sensível, alguns fundos do APESP podem apenas ser acessados com autorização judicial ou da autoridade competente. Em todos os casos, deve-se garantir o cumprimento das obrigações de vinculação do uso dos dados à finalidade do estudo e a adoção de medidas de prevenção e segurança apropriadas ao tratamento, no termos da LGPD.

Já para reproduzir e eventualmente reutilizar acervos digitais ou digitalizados, o interessado deve assinar o Termo de Responsabilidade para Uso, Reprodução e Divulgação das Informações e Dados Pessoais Contidos em Documentos Custodiados pelo APESP, responsabilizando-se civil e criminalmente pelo seu uso. Cópias em alta resolução e o acesso à matriz são fornecidos mediante solicitação.

A LAI e a LGPD regulam a restrição de acesso a dados sigilosos e pessoais, mas não excluem as demais hipóteses legais de sigilo, de segredo de justiça e de segredo industrial, bem como as práticas de segurança previstas em regulamentos específicos e padrões éticos relacionados a estudos e pesquisas de caráter histórico, científico, tecnológico ou estatístico.

# 14 Glossário

## Legislação Estadual

**Acesso:** direito, oportunidade ou meios de localizar, recuperar e usar a informação (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, I).

**Acondicionamento:** embalagem ou guarda de documentos visando à sua preservação e acesso (Instrução Normativa APE/SAESP nº 2/2010, art. 3º, I).

**Amostragem documental:** fragmento representativo de um conjunto de documentos destinado à eliminação, selecionado para guarda permanente por meio de critérios qualitativos e quantitativos (Instrução Normativa APE/SAESP nº 2/2010, art. 3º, II).

**Arquivo digital:** conjunto de bits que formam uma unidade lógica interpretável por computador e armazenada em suporte apropriado (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, II).

**Arquivos públicos:** conjuntos de documentos produzidos, recebidos e acumulados por órgãos públicos, autarquias, fundações instituídas ou mantidas pelo Poder Público, empresas públicas, sociedades de economia mista, entidades privadas encarregadas da gestão de serviços públicos e organizações sociais, no exercício de suas funções e atividades (Decreto nº 58.052/2012, art. 3º, I).

**Arquivos públicos:** conjuntos de documentos produzidos, recebidos e acumulados por órgãos públicos, autarquias, fundações instituídas ou mantidas pelo Poder Público, empresas públicas, sociedades de economia mista, entidades privadas encarregadas da gestão de serviços públicos e organizações sociais, definidas como tal pela Lei Complementar nº 846, de 4 de junho de 1998, no exercício de suas funções e atividades (Decreto nº 48.897/2004, art. 1º).

**Assinatura digital:** modalidade de assinatura eletrônica, resultado de uma operação matemática que utiliza algoritmos de criptografia e permite aferir, com segurança, a origem e a integridade do documento. Os atributos da assinatura digital são: a) ser única para cada documento, mesmo que seja o mesmo signatário; b) comprovar a autoria do documento digital; c) possibilitar a verificação da integridade do documento; d) assegurar ao destinatário o "não repúdio" do documento digital, uma vez que, a princípio, o emitente é a única pessoa que tem acesso à chave privada que gerou a assinatura (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, III).

**Atividade:** ação, encargo ou serviço decorrente do exercício de uma função, que pode ser identificada como: I - atividade-meio, quando se refere a ação, encargo ou serviço que um órgão leva a efeito para auxiliar e viabilizar o desempenho de suas atribuições específicas e que resulta na produção e acumulação de documentos de caráter instrumental e acessório; II - atividade-fim, quando se refere a ação, encargo ou serviço que um órgão leva a efeito para o efetivo desempenho de suas atribuições específicas e que resulta na produção e acumulação de documentos de caráter substantivo e essencial para o seu funcionamento (Decreto nº 48.897/2004, art. 17).

**Atividade-fim:** ação, encargo ou serviço que um órgão leva a efeito para o efetivo desempenho de suas atribuições específicas e que resulta na produção e acumulação de documentos de caráter substantivo e essencial para o seu funcionamento (Instrução Normativa APE/SAESP nº 2/2010, art. 3º, IV).

**Atividade-meio:** ação, encargo ou serviço que um órgão leva a efeito para auxiliar e viabilizar o desempenho de suas atribuições específicas e que resulta na produção e acumulação de documentos de caráter instrumental e acessório (Instrução Normativa APE/SAESP nº 2, de 02/2010, art. 3º, III).

**Atualização:** técnica de migração que consiste em copiar os dados de um suporte para outro sem mudar sua codificação para evitar perdas de dados provocadas por deterioração do suporte (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, IV).

**Autenticidade:** credibilidade de um documento enquanto documento, isto é, a qualidade de um documento ser o que diz ser e que está livre de adulteração ou qualquer outro tipo de corrupção (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, V).

**Autenticidade:** qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema (Decreto nº 58.052/2012, art. 3º, II).

**Avaliação de documentos:** processo de análise que permite a identificação dos valores dos documentos, para fins de definição de seus prazos de guarda e de sua destinação (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, VI).

**Avaliação documental:** processo de análise que permite a identificação dos valores dos documentos, para fins da definição de seus prazos de guarda e de sua destinação (Decreto nº 48.897/2004, art. 19, parágrafo único).

**Avaliação documental:** processo de análise que permite a identificação dos valores dos documentos, para fins da definição de seus prazos de guarda e de sua destinação (Instrução Normativa APE/SAESP nº 2/2010, art. 3º, V).

**Classificação de documentos:** sequência das operações técnicas que visam a agrupar os documentos de arquivo relacionando-os ao órgão produtor, à função,

subfunção e atividade responsável por sua produção ou acumulação (Decreto nº 48.897/2004, art. 10, parágrafo único).

**Captura:** incorporação de um documento ao sistema de gestão arquivística, por meio do registro, classificação e arquivamento (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, VII).

**Certificação digital:** atividade de reconhecimento em meio eletrônico que se caracteriza pelo estabelecimento de uma relação única, exclusiva e intransferível entre uma chave de criptografia e uma pessoa física, jurídica, máquina ou aplicação. Esse reconhecimento é inserido em um certificado digital por uma autoridade certificadora (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, IX)

**Certificado de autenticidade:** declaração de autenticidade das reproduções dos documentos arquivísticos digitais, emitida pela instituição responsável por sua preservação (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, VIII)

**Certificado digital:** documento emitido e assinado digitalmente por uma autoridade certificadora, que contém dados que identificam seu titular e o relaciona à sua respectiva chave-pública (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, X).

**Checksum:** soma de verificação do resultado da execução de um algoritmo (função hash), que mapeia a sequência de bits de um documento digital com a finalidade de atestar a sua integridade e autenticidade (Portaria UAPESP/SAESP nº 10/2022, art. 2º, I).

**Classificação de documentos:** sequência de operações técnicas que visam agrupar os documentos de arquivo relacionando-os ao órgão produtor, à função, subfunção e atividade responsável por sua produção ou acumulação (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XI).

**Classificação de segurança:** atribuição de graus de sigilo a documentos ou às informações neles contidas, conforme legislação específica (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XII).

**Classificação de sigilo:** atribuição, pela autoridade competente, de grau de sigilo a documentos, dados e informações (Decreto nº 58.052/2012, art. 3º, III).

**Código de classificação da série documental:** referência numérica que a associa ao seu contexto de produção, é composto das seguintes unidades de informação: órgão produtor, função, subfunção, atividade, série documental (Decreto nº 48.897/2004, art. 13).

**Comissões de Avaliação de Documentos de Arquivo:** grupos permanentes e multidisciplinares instituídos nos órgãos da Administração Pública Estadual nos termos do artigo 2º do Decreto nº 29.838, de 18 de abril de 1989, responsáveis pela

elaboração e aplicação de Planos de Classificação e de Tabelas de Temporalidade de Documentos (Decreto nº 48.897/2004, art. 34).

**Comissão de Avaliação de Documentos de Arquivo:** grupo permanente e multidisciplinar instituído oficialmente nos órgãos e entidades, responsável pela elaboração e aplicação de Planos de classificação e de Tabelas de temporalidade de documentos de arquivo (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XIII).

**Completeza:** atributo de um documento arquivístico que se refere à presença de todos os elementos intrínsecos e extrínsecos exigidos pela organização produtora e pelo sistema jurídico-administrativo a que pertence, de maneira a ser capaz de gerar consequências (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XIV).

**Confiabilidade:** credibilidade de um documento arquivístico enquanto uma afirmação do fato. Existe quando um documento arquivístico pode sustentar o fato ao qual se refere, e é estabelecida pelo exame da completeza da forma do documento e do grau de controle exercido no processo de sua criação (Instrução Normativa APE/SAESP nº 1/2009, art 2º, XV).

**Confidencialidade:** propriedade de certos dados ou informações que não podem ser disponibilizadas ou divulgadas sem autorização para pessoas, entidades ou processos (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XVI).

**Contexto tecnológico:** refere-se ao ambiente tecnológico (h*ardware*, *software* e padrões) que envolve o documento (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XVII).

**Conversão:** técnica de migração que pode se configurar de diversas formas, tais como: 1. conversão de dados: mudança de um formato para outro; 2. conversão de sistema computacional: mudança do modelo de computador e de seus periféricos (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XVIII).

**Cópia de segurança:** cópia feita de um arquivo ou de um documento que deve ser guardada sob condições especiais para a preservação de sua integridade no que diz respeito tanto à forma quanto ao conteúdo, de maneira a permitir a recuperação de programas ou informações importantes em caso de falha ou perda (Instrução Normativa APE/SAESP nº 1/2009, art. 2°, XIX).

**Correio eletrônico:** sistema usado para criar, transmitir e receber mensagem eletrônica e outros documentos digitais por meio de redes de computadores (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XX).

**Credencial de segurança:** autorização por escrito concedida por autoridade competente, que habilita o agente público estadual no efetivo exercício de cargo, função, emprego ou atividade pública a ter acesso a documentos, dados e informações sigilosas (Decreto nº 58.052/2012, art. 3º, IV).

**Credencial de segurança:** 1. um ou vários atributos associados a um usuário que definem as categorias de segurança segundo as quais o acesso é concedido; 2. autorização concedida por autoridade competente, que habilita o usuário a ter acesso a documentos, dados e informações sigilosos (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XXI).

**Criptografia:** método de codificação de dados segundo algoritmo específico e chave secreta de forma que somente os usuários autorizados podem restabelecer sua forma original (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XXII).

**Criptografia:** processo de escrita à base de métodos lógicos e controlados por chaves, cifras ou códigos, de forma que somente os usuários autorizados possam reestabelecer sua forma original (Decreto nº 58.052/2012, art. 3º, V).

**Custódia:** responsabilidade pela guarda de documentos, dados e informações (Decreto nº 58.052/2012, art. 3º, VI).

**Custódia:** responsabilidade jurídica de guarda e proteção de documentos de arquivo, independente de vínculo de propriedade (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XXIII).

**Dado público:** sequência de símbolos ou valores, representado em algum meio, produzido ou sob a guarda governamental, em decorrência de um processo natural ou artificial, que não tenha seu acesso restrito por legislação específica (Decreto nº 58.052/2012, art. 3º, VII).

**Desclassificação:** supressão da classificação de sigilo por ato da autoridade competente ou decurso de prazo, tornando irrestrito o acesso a documentos, dados e informações sigilosas (Decreto nº 58.052/2012, art. 3º, VIII).

**Descritor:** Palavra, expressão ou símbolo convencionados para expressar o conteúdo do documento e possibilitar sua recuperação de forma individualizada (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XXIV).

**Descritor:** palavra ou grupo de palavras retirados da composição do documento que indicam brevemente seu conteúdo, facilitando a recuperação da informação (Portaria UAPESP/SAESP nº 6/2021, art. 2º, I).

**Destinação:** decisão decorrente da avaliação de documentos, que determina o seu encaminhamento para eliminação ou guarda permanente (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XXV).

**Destinação:** decisão decorrente da avaliação documental, que determina o seu encaminhamento (Decreto nº 48.897/2004, art. 20, § 1º).

**Digitalização:** processo de conversão de um documento para o formato digital, por meio de dispositivo apropriado (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XXVI).

**Disponibilidade:** É a razão entre o tempo durante o qual o sistema está acessível e operacional e a unidade de tempo definida como referência (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XXVII).

**Disponibilidade:** qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados (Decreto nº 58.052/2012, art. 3º, X).

**Documento arquivístico digital:** documento arquivístico codificado em dígitos binários, produzido, tramitado e armazenado por sistema computacional, que pode ser produzido no contexto tecnológico digital (documentos nato-digitais) ou obtido a partir de suportes analógicos (documentos digitalizados) (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XXIX).

**Documento arquivístico:** documento produzido, recebido ou acumulado por um órgão ou entidade no exercício de suas funções e atividades (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XXVIII).

**Documento composto:** documento que, durante sua tramitação, acumula documentos simples ou avulsos de forma orgânica e relacional (Portaria UAPESP/SAESP nº 6/2021, art. 2º, III).

**Documento digital:** documento codificado em dígitos binários, acessível por meio de sistema computacional, que pode ser produzido no contexto tecnológico digital (objetos nato-digitais) ou obtido a partir de suportes analógicos (objetos digitalizados) (Instrução Normativa APE/SAESP nº1/2009, art. 2º, XXX).

**Documento digital:** documento codificado em dígitos binários, tramitado em sistema informatizado, que pode ser produzido no contexto tecnológico digital (documentos nato-digitais) ou obtido a partir de suportes analógicos (documentos digitalizados) (Portaria UAPESP/SAESP nº 6/2021, art. 2º, II).

**Documento digitalizado:** documento convencional convertido para um padrão de formato digital por meio de dispositivo apropriado (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XXXI).

**Documento intermediário:** documento com uso pouco frequente que aguarda prazos de prescrição e precaução nas unidades que tenham atribuições de arquivo nos órgãos ou entidades (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XXXII).

**Documento original:** documento não digital produzido em suporte papel (Portaria UAPESP/SAESP nº 5/2021, art. 1º, § 2º); ver verbete Representante digital.

**Documento permanente:** documento com valor histórico, probatório e informativo que deve ser definitivamente preservado (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XXXIII).

**Documento simples ou avulso:** documento formado por um único item documental (Portaria UAPESP/SAESP nº 6/2021, art. 2º, IV).

**Documento:** unidade de registro de informações, qualquer que seja o suporte ou formato (Decreto nº 58.052/2012, art. 3º, XI).

**Documentos correntes:** aqueles em curso ou que se conservam junto às unidades produtoras em razão de sua vigência e da frequência com que são por elas consultados (Decreto nº 48.897/2004, art. 4º, I).

**Documento de arquivo:** registro de informação, em qualquer suporte, inclusive o magnético ou óptico, produzido, recebido ou acumulado por órgão ou entidade da Administração Pública Estadual (Instrução Normativa APE/SAESP nº 2/2010, art. 3º, VI).

**Documentos de arquivo:** todos os registros de informação, em qualquer suporte, inclusive o magnético ou óptico, produzidos, recebidos ou acumulados por órgãos e entidades da Administração Pública Estadual, no exercício de suas funções e atividades (Decreto nº 58.052/2012, art. 3º, IX).

**Documentos de arquivo:** todos os registros de informação, em qualquer suporte, inclusive o magnético ou óptico, produzidos, recebidos ou acumulados pelos órgãos públicos, autarquias, fundações instituídas ou mantidas pelo Poder Público, empresas públicas, sociedades de economia mista, entidades privadas encarregadas da gestão de serviços públicos e organizações sociais, no exercício de suas funções e atividades (Decreto nº 48.897/2004, art. 3º).

**Documentos de guarda permanente:** I - os indicados nas Tabelas de Temporalidade de Documentos, que serão definitivamente preservados; II - os de arquivos privados de pessoas físicas ou jurídicas declarados de interesse público e social, nos termos da lei; III - todos os processos, expedientes e demais documentos produzidos, recebidos ou acumulados pelos órgãos da Administração Pública Estadual até o ano de 1940 (Decreto nº 48.897/2004, art. 31).

**Documentos intermediários:** aqueles com uso pouco frequente que aguardam prazos de prescrição e precaução nas unidades que tenham atribuições de arquivo nas Secretarias de Estado, ou na Seção Técnica de Arquivo Intermediário, do Arquivo do Estado (Decreto nº 48.897/2004, art. 4º, II).

**Documentos permanentes:** aqueles com valor histórico, probatório e informativo que devem ser definitivamente preservados (Decreto nº 48.897/2004, art. 4º, III).

**Documentos Pessoais:** aqueles relacionados à pessoa natural identificada ou identificável, relativas à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais (Decreto nº 58.052/2012, art. 27, II).

**Documentos Sigilosos:** aqueles submetidos temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado (Decreto nº 58.052/2012, art. 27, I).

**Eliminação:** destruição de documentos que na avaliação foram considerados sem valor permanente, por meio de fragmentação manual ou mecânica (Instrução Normativa APE/SAESP nº 2/2010, art. 3º, VII).

**Emulação:** utilização de recursos computacionais que fazem uma tecnologia funcionar com as características de outra, aceitando as mesmas entradas e produzindo as mesmas saídas (Instrução Normativa APE/SAESP nº 1/2009, inciso art. 2º, XXXIV)

**Encapsulamento:** técnica que permite preservar a integridade de dados durante o processo de transmissão (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XXXV).

**Espécie do documento:** configuração que assume um documento de acordo com a disposição e a natureza das informações nele contidas (Portaria UAPESP/SAESP nº 6/2021, art. 2º, V).

**Formato de arquivo:** especificação de regras e padrões descritos formalmente para interpretação dos bits constituintes de um arquivo digital. Pode ser: 1. aberto – quando as especificações são públicas (p.ex.: XML, HTML, ODF e RTF); 2. fechado – quando as especificações não são divulgadas pelo proprietário (p. ex.: DOC); 3. proprietário – quando as especificações são definidas por uma empresa que mantém seus direitos, sendo seu uso gratuito ou não (p.ex.: PDF, JPEG, DOC e GIF); 4. padronizado – quando as especificações são produzidas por um organismo de normalização, sendo os formatos abertos e não proprietários (p. ex.: XML) (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XXXVI).

**Fluxograma:** representação gráfica do processo de trabalho (Portaria UAPESP/SAESP nº 6/2021, art. 2º, VI).

**Função:** conjunto de atividades que o Estado exerce para a consecução de seus objetivos, pode ser identificada como: I - direta ou essencial, quando corresponde às razões pelas quais foram criados os diferentes órgãos, entidades ou empresas, caracterizando as áreas específicas nas quais atuam; II - indireta ou auxiliar, quando é a que possibilita a infraestrutura administrativa necessária ao desempenho concreto e eficaz de função essencial (Decreto nº 48.897/2004, art. 15).

**Gestão arquivística de documentos:** conjunto de procedimentos e operações técnicas referentes à produção, tramitação, uso, avaliação e arquivamento de documentos em fase corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XXXVII).

**Gestão de documentos:** conjunto de procedimentos e operações técnicas referentes à sua produção, classificação, avaliação, tramitação, uso, arquivamento e reprodução, que assegura a racionalização e a eficiência dos arquivos (Decreto nº 58.052/2012, art. 3º, XII).

**Gestão de documentos:** conjunto de procedimentos e operações técnicas referentes à sua produção, classificação, avaliação, tramitação, uso, arquivamento e reprodução, que assegura a racionalização e a eficiência dos arquivos (Decreto nº 48.897/2004, art. 8º).

**Higienização:** retirada, por meio de técnicas apropriadas, de poeira e outros resíduos, com vistas à preservação de documentos (Instrução Normativa APE/SAESP nº 2/2010, art. 3º, VIII).

**Indexação:** processo pelo qual se relacionam de forma sistemática descritores ou palavras-chave que permitem a recuperação posterior do conteúdo de documentos e informações (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XXXVIII).

**Integridade:** estado dos documentos que se encontram completos e que não sofreram nenhum tipo de corrupção ou alteração não autorizada nem documentada (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XXXIX).

**Item documental:** menor unidade de um documento fisicamente indivisível (Portaria UAPESP/SAESP nº 6/2021, art. 2º, VII).

**Informação:** dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato (Decreto nº 58.052/2012, art. 3º, XIII).

**Informação pessoal:** aquela relacionada à pessoa natural identificada ou identificável (Decreto nº 58.052/2012, art. 3º, XIV).

**Informação sigilosa:** aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado (Decreto nº 58.052/2012, art. 3º, XV).

**Integridade:** qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino (Decreto nº 58.052/2012, art. 3º, XVI).

**Mapeamento de documentos compostos:** identificação e análise de tipos documentais que registram a execução de funções e atividades do fluxo de trabalho (Portaria UAPESP/SAESP nº 6/2021, art. 2º, VIII).

**Marcação:** aposição de marca assinalando o grau de sigilo de documentos, dados ou informações, ou sua condição de acesso irrestrito, após sua desclassificação (Decreto nº 58.052/2012, art. 3º, XVII).

**Massa documental acumulada:** volume de documentos produzidos e recebidos no exercício de funções e atividades dos órgãos e entidades estaduais que foram acumulados ao longo do tempo sem a aplicação de Planos de Classificação e Tabelas de Temporalidade de Documentos (Instrução Normativa APE/SAESP nº 2/2010, art. 3º, IX).

**Mensagem de correio eletrônico:** Documento digital criado ou recebido via sistema de correio eletrônico, incluindo anexos que possam ser transmitidos com a mensagem (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XL).

**Metadados:** informações estruturadas e codificadas que descrevem e permitem gerenciar, compreender, preservar e acessar os documentos digitais ao longo do tempo. Os metadados referem-se a: 1. identificação e contexto documental (identificador único, instituição produtora, nomes, assunto, datas, local, código de classificação, tipologia documental, temporalidade, destinação, versão, documentos relacionados, idioma e indexação); 2. segurança (categoria de sigilo, informações sobre criptografia, assinatura digital e outras marcas digitais); 3. contexto tecnológico (formato de arquivo, tamanho de arquivo, dependências de *hardware* e *software*, tipos de mídias, algoritmos de compressão) e localização física do documento (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XLI).

**Metadados:** informações estruturadas e codificadas que descrevem e permitem gerenciar, compreender, preservar e acessar os documentos digitais ao longo do tempo e referem-se a: a) identificação e contexto documental (identificador único, instituição produtora, nomes, assunto, datas, local, código de classificação, tipologia documental, temporalidade, destinação, versão, documentos relacionados, idioma e indexação); b) segurança (grau de sigilo, informações sobre criptografia, assinatura digital e outras marcas digitais); c) contexto tecnológico (formato de arquivo, tamanho de arquivo, dependências de *hardware* e *software*, tipos de mídias, algoritmos de compressão) e localização física do documento (Decreto nº 58.052/2012, art. 3º, XVIII).

**Metadados de identidade e integridade:** dados estruturados que asseguram a autenticidade do documento digital, que o caracteriza como único, completo e livre de corrupção ou alteração não autorizada nem documentada (Portaria UAPESP/SAESP nº 4/2020, art. 2º, § 2º).

**Migração:** conjunto de procedimentos e técnicas para assegurar a capacidade dos documentos digitais serem acessados face às mudanças tecnológicas, que consiste na transferência de um documento digital: a) de um suporte que está se tornando obsoleto, fisicamente deteriorado ou instável para um suporte mais novo; b) de um formato obsoleto para um formato mais atual ou padronizado; c) de uma plataforma computacional em vias de descontinuidade para uma outra mais mo-

derna. A migração pode ocorrer por conversão, por atualização ou por reformatação (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XLII).

**Modelagem de documentos digitais:** desenvolvimento do modelo de documento digital em sistema informatizado (Portaria UAPESP/SAESP nº 6/2021, art. 2º, IX).

**Modelo:** representação do tipo documental, considerando sua forma e conteúdo (Portaria UAPESP/SAESP nº 6/2021, art. 2º, X).

**Nível de acesso:** limitador sistêmico que restringe o acesso ao documento a pessoas autorizadas: a) Público: acesso a todos os usuários, independentemente do órgão; b) Limitado entre Interessados: acesso a todas as unidades e/ou usuários dos órgãos por onde o documento tramitar; c) Limitado ao Órgão: acesso a todos os usuários do órgão, independentemente da unidade; d) Limitado entre Pessoas: acesso a quem produziu o documento e seu destinatário (Portaria UAPESP/SAESP nº 6/2021, art. 2º, XI).

**Órgão produtor:** instituição ou entidade juridicamente constituída e organizada responsável pela execução de funções do Estado (Decreto nº 48.897/2004, art. 14).

**Pacote de informação para transmissão**: conjunto estruturado de documentos digitais, constituído por seu conteúdo e respectivos metadados, *checksum* e demais informações relacionadas à sua produção, identificação e acesso (Portaria UAPESP/SAESP nº 10/2022, art. 2º, II).

**Patrimônio digital:** conjunto de documentos digitais que possuem valor suficiente para serem preservados a fim de que possam ser consultados e utilizados no futuro (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XLIII).

**Plano de classificação de documentos:** o instrumento utilizado para classificar todo e qualquer documento de arquivo (Decreto nº 48.897/2004, art. 10).

**Plano de classificação de documentos:** instrumento oficial utilizado para classificar todo e qualquer documento de arquivo, associando-o à função, subfunção e atividade que determinou a sua produção (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XLIV).

**Preservação digital:** conjunto de ações destinadas a manter a integridade e a acessibilidade dos documentos digitais ao longo do tempo, e que devem alcançar todas as suas características essenciais: físicas, lógicas e conceituais (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XLV).

**Presunção de autenticidade**: inferência da autenticidade de um documento arquivístico feita a partir de fatos conhecidos sobre a maneira como aquele documento foi produzido e mantido (Portaria UAPESP/SAESP nº 10/2022, art. 2º, III).

**Primariedade:** qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações (Decreto nº 58.052/2012, art. 3º, XIX).

**Programa de gestão arquivística de documentos:** conjunto de estratégias, procedimentos e técnicas que permite o planejamento, a implantação e o controle da gestão arquivística de documentos nos órgãos e entidades (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XLVI).

**Reclassificação:** alteração, pela autoridade competente, da classificação de sigilo de documentos, dados e informações (Decreto nº 58.052/2012, art. 3º, XX).

**Recolhimento:** entrada de documentos em arquivos permanentes (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XLVII).

**Recolhimento:** a) entrada de documentos em arquivos permanentes, com competência formalmente estabelecida; b) operação pela qual um conjunto de documentos passa do arquivo intermediário para o arquivo permanente (Instrução Normativa APE/SAESP nº 2/2010, art. 3º, X).

**Reformatação:** 1. técnica de migração que consiste na mudança da forma de apresentação de um documento para fins de acesso ou manutenção dos dados; 2. apagar todos os dados de uma unidade de armazenamento (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XLVIII).

**Repositório arquivístico digital confiável da UAPESP**: ambiente de preservação constituído pelo conjunto de procedimentos normativos e técnicos, a matriz de responsabilidades e a infraestrutura tecnológica com capacidade para preservar e dar acesso permanente aos documentos digitais recebidos pelo Arquivo Público do Estado (Portaria UAPESP/SAESP nº 10/2022, art. 2º, IV).

**Repositório digital confiável**: Repositório digital confiável é aquele que é capaz de manter autênticos, preservar e prover acesso a documentos digitais pelo tempo necessário (Portaria UAPESP/SAESP nº 4/2020, art. 3º, parágrafo único).

**Representante digital:** documento produzido a partir do processo de digitalização do documento original e seus metadados (Portaria UAPESP/SAESP nº 5/2021, art. 1º, § 1º); ver verbete Documento original.

**Requisitos funcionais:** conjunto de condições que se referem ao registro e captura, classificação, tramitação, avaliação e destinação, recuperação da informação, acesso e segurança, armazenamento e preservação de documentos (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, L).

**Requisitos não-funcionais:** conjunto de condições que se referem à utilização de padrões abertos, independência de fornecedor, integração com sistemas legados, conformidade com a legislação e os padrões de interoperabilidade do governo,

atendimento a usuários internos e externos, facilidade de utilização e desempenho (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, LI).

**Requisitos:** conjunto de condições a serem cumpridas pelo órgão ou entidade, pelo sistema de gestão arquivística de documentos e pelos próprios documentos a fim de garantir a sua confiabilidade e autenticidade, bem como seu acesso (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, XLIX).

**Rol de documentos, dados e informações sigilosas e pessoais:** relação anual, a ser publicada pelas autoridades máximas de órgãos e entidades, de documentos, dados e informações classificadas, no período, como sigilosas ou pessoais, com identificação para referência futura (Decreto nº 58.052/2012, art. 3º, XXI).

**Série documental:** conjunto de documentos do mesmo tipo documental produzido por um mesmo órgão, em decorrência do exercício da mesma função, subfunção e atividade e que resultam de idêntica forma de produção e tramitação e obedecem à mesma temporalidade e destinação (Decreto nº 48.897/2004, art. 12).

**Serviço ou atendimento eletrônico:** aquele prestado remotamente ou à distância, utilizando meios eletrônicos de comunicação (Decreto nº 58.052/2012, art. 3º, XXIII).

**Serviço ou atendimento presencial:** aquele prestado a presença física do cidadão, principal beneficiário ou interessado no serviço (Decreto nº 58.052/2012, art. 3º, XXII).

**Sistema de negócio:** sistema informatizado projetado e construído para atender a processo específico do órgão ou entidade (Portaria UAPESP/SAESP nº 4/2020, art. 2º, § 1º).

**Sistema informatizado de gestão arquivística de documentos (SIGAD):** conjunto de procedimentos e operações técnicas da gestão arquivística de documentos processado eletronicamente e aplicável em ambientes digitais ou em ambientes híbridos, isto é, documentos digitais e não digitais ao mesmo tempo (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, LII).

**Subfunção:** agrupamento de atividades afins, correspondendo cada subfunção a uma modalidade da respectiva função (Decreto nº 48.897/2004, art. 16).

**Suporte:** base física sobre a qual a informação é registrada (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, LIII).

**Tabela de documentos, dados e informações sigilosas e pessoais:** relação exaustiva de documentos, dados e informações com quaisquer restrições de acesso, com a indicação do grau de sigilo, decorrente de estudos e pesquisas promovidos pelas Comissões de Avaliação de Documentos e Acesso - CADA, e publicada pelas autoridades máximas dos órgãos e entidades (Decreto nº 58.052/2012, art. 3º, XXIV).

**Tabela de Temporalidade de Documentos:** instrumento resultante da avaliação documental, aprovado por autoridade competente, que define prazos de guarda e a destinação de cada série documental (Decreto nº 48.897/2004, art. 19).

**Tabela de temporalidade de documentos:** instrumento resultante da avaliação documental, aprovado por autoridade competente, que define os prazos de guarda e a destinação de cada série documental (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, LIV).

**Tipo documental:** configuração que assume um documento, considerando a disposição e a natureza das informações nele registradas, de acordo com a atividade que o gerou (Portaria UAPESP/SAESP nº 6/2021, art. 2º, XII).

**Transferência:** passagem de documentos do arquivo corrente para o arquivo intermediário (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, LV).

**Transferência:** passagem de documentos públicos do arquivo corrente para o arquivo intermediário (Instrução Normativa APE/SAESP nº 2/2010, art. 3º, XI).

**Tratamento da informação:** conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação (Decreto nº 58.052/2012, art. 3º, XXV).

**Trilhas de auditoria:** conjunto de informações registradas que permite o rastreamento de intervenções ou tentativas de intervenção feitas no documento arquivístico digital ou no sistema computacional (Instrução Normativa APE/SAESP nº 1/2009, art. 2º, LVI).

## Legislação Federal

**Agentes de tratamento:** o controlador e o operador (Lei nº 13.709/2018, art. 5º, IX).

**Anonimização:** utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo (Lei nº 13.709/2018, art. 5º, XI).

**Arquivo Público**: instituição do Poder Público com a função de implementar, acompanhar e supervisionar a gestão de documentos arquivísticos produzidos e recebidos pela Administração Pública em seu âmbito de atuação, e de promover a organização, a preservação e o acesso dos documentos de valor permanente ou histórico recolhidos dos diversos órgãos e entidades dos estados, do Distrito Federal e dos municípios (Resolução CONARQ nº 27/2008, art. 1º, parágrafo único).

**Arquivos correntes:** conjuntos de documentos em curso ou que, mesmo sem movimentação, constituam objeto de consultas frequentes (Resolução CONARQ nº 01/1995, art. 1º, § 2º).

**Arquivos do Distrito Federal:** são arquivos do Distrito Federal o arquivo do Poder Executivo, o arquivo do Poder Legislativo e o arquivo do Poder Judiciário (Lei nº 8.159/1991, art. 17, § 3º).

**Arquivos Estaduais:** são arquivos estaduais os arquivos do Poder Executivo, o arquivo do Poder Legislativo e o arquivo do Poder Judiciário (Lei nº 8.159/1991, art. 17, § 2º).

**Arquivos Federais:** são arquivos federais o Arquivo Nacional, do Poder Executivo, e os arquivos do Poder Legislativo e do Poder Judiciário. São considerados, também, do Poder Executivo os arquivos do Ministério da Marinha, do Ministério das Relações Exteriores, do Ministério do Exército e do Ministério da Aeronáutica (Lei nº 8.159/1991, art. 17, § 1º)

**Arquivos intermediários:** conjuntos de documentos que, não sendo de uso corrente nos órgãos produtores, aguardam sua eliminação ou recolhimento para guarda permanente (Resolução CONARQ nº 01/1995, art. 1º, § 3º).

**Arquivos Municipais:** são arquivos municipais o arquivo do Poder Executivo e o arquivo do Poder Legislativo (Lei nº 8.159/1991, art. 17, § 4º).

**Arquivos privados:** conjuntos de documentos produzidos ou recebidos por pessoas físicas ou jurídicas, em decorrência de suas atividades (Lei nº 8.159/1991, art. 11).

**Arquivos públicos dos Territórios:** os arquivos públicos dos Territórios são organizados de acordo com sua estrutura político-jurídica (Lei nº 8.159/1991, art. 17, § 5º).

**Arquivos públicos:** conjuntos de documentos produzidos e recebidos, no exercício de suas atividades, por órgãos públicos de âmbito federal, estadual, do Distrito Federal e municipal em decorrência de suas funções administrativas, legislativas e judiciárias (Lei nº 8.159/1991, art. 7º).

**Arquivos:** os conjuntos de documentos produzidos e recebidos por órgãos públicos, instituições de caráter público e entidades privadas, em decorrência do exercício de atividades específicas, bem como por pessoa física, qualquer que seja o suporte da informação ou a natureza dos documentos (Lei nº 8.159/1991, art. 2º).

**Autoridade nacional:** órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional (Lei nº 13.709/2018, art. 5º, XIX).

**Banco de dados:** conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico (Lei nº 13.709/2018, art. 5º, IV).

**Bloqueio:** suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados (Lei nº 13.709/2018, art. 5º, XIII).

**Consentimento:** manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (Lei nº 13.709/2018, art. 5º, XII).

**Controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (Lei nº 13.709/2018, art. 5º, IV).

**Dado anonimizado:** dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento (Lei nº 13.709/2018, art. 5º, III).

**Dado pessoal sensível:** dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (Lei nº 13.709/2018, art. 5º, II).

**Dado pessoal:** informação relacionada a pessoa natural identificada ou identificável (Lei nº 13.709/2018, art. 5º, I).

**Digitalização:** conversão da fiel imagem de um documento para código digital (Lei nº 12.682/2012, art. 1º, parágrafo único).

**Documento arquivístico digital:** documento arquivístico codificado em dígitos binários, produzido, tramitado e armazenado por sistema computacional. São exemplos de documentos arquivísticos digitais: planilhas eletrônicas, mensagens de correio eletrônico, sítios na internet, bases de dados e textos, imagens fixas, imagens em movimento e gravações sonoras, dentre outras possibilidades, em formato digital (Resolução CONARQ nº 20/2004, art. 1º, § 2º).

**Documento arquivístico:** informação registrada, independente da forma ou do suporte, produzida e recebida no decorrer das atividades de um órgão, entidade ou pessoa, dotada de organicidade e que possui elementos constitutivos suficientes para servir de prova dessas atividades (Resolução CONARQ nº 20/2004, art. 1º, § 1º).

**Documento digitalizado:** representante digital do processo de digitalização do documento físico e seus metadados. (Decreto Federal nº 10.278/2020, art. 3º, I).

**Documento público de valor permanente:** documento que deve ser preservado pelo seu valor histórico, probatório e informativo, estabelecido em tabela de

temporalidade elaborada pelas entidades mencionadas no art. 1º (empresas em processo de desestatização e às pessoas jurídicas de direito privado sucessoras de empresas públicas, detentoras de documentos públicos), ou, na sua ausência, de conformidade com as normas emanadas pelo CONARQ (Resolução CONARQ nº 19/2003, art. 2º, I).

**Documento público:** documentos produzidos ou recebidos por pessoas jurídicas de direito público interno ou por entidades privadas encarregadas da gestão de serviços públicos (Decreto Federal nº 10.278/2020, art. 3º, III).

**Documentos correntes:** aqueles em curso ou que, mesmo sem movimentação, constituam objeto de consultas frequentes (Lei nº 8.159/1991, art. 7º, § 1º).

**Documentos intermediários:** aqueles que, não sendo de uso corrente nos órgãos produtores, por razões de interesse administrativo, aguardam a sua eliminação ou recolhimento para guarda permanente (Lei nº 8.159/1991, art. 7º, § 2º).

**Documentos nato-digitais:** documentos produzidos originalmente em formato digital. (Decreto Federal nº 10.278/2020, art. 2º, parágrafo único, I).

**Documentos permanentes:** conjuntos de documentos de valor histórico, probatório e informativo que devem ser definitivamente preservados (Lei nº 8.159/1991, art. 7º, § 3º).

**Eliminação:** exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado (Lei nº 13.709/2018, art. 5º, XIV).

**Encarregado:** pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) (Lei nº 13.709/2018, art. 5º, VIII).

**Gestão arquivística de documentos:** conjunto de procedimentos e operações técnicas referentes à produção, tramitação, uso, avaliação e arquivamento de documentos em fase corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente (Resolução CONARQ nº 20/2004, art. 1º, § 3º).

**Gestão arquivística de documentos:** conjunto de procedimentos e operações técnicas referentes à produção, tramitação, uso, avaliação e arquivamento dos documentos em idades corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente (Resolução CONARQ nº 50/2022, art. 2º, § 1º).

**Gestão de documentos:** conjunto de procedimentos e operações técnicas referentes à produção, à tramitação, à avaliação, ao uso e ao arquivamento de documentos (Resolução CONARQ nº 19/2003, art. 2º, II).

**Gestão de documentos:** conjunto de procedimentos e operações técnicas referentes à sua produção, tramitação, uso, avaliação e arquivamento em fase corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente (Lei nº 8.159/1991, art. 3º).

**Gestão de documentos:** planejamento e o controle das atividades técnicas relacionadas à produção, classificação, tramitação, uso, arquivamento, avaliação e seleção dos documentos de arquivo, em fase corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente (Resolução CONARQ nº 01/1995, art. 1º, § 1º).

**Integridade:** estado dos documentos que não foram corrompidos ou alterados de forma não autorizada (Decreto Federal nº 10.278/2020, art. 3º, IV).

**Metadados:** dados estruturados que permitem classificar, descrever e gerenciar documentos (Decreto Federal nº 10.278/2020, art. 3º, II).

**Metadados:** informações estruturadas e codificadas que descrevem e permitem gerenciar, compreender, preservar e acessar os documentos digitais ao longo do tempo. Os metadados referem-se a: identificação e contexto documental (identificador único, instituição produtora, nomes, assunto, datas, local, código de classificação, tipologia documental, temporalidade, destinação, versão, documentos relacionados, idioma e indexação), segurança (categoria de sigilo, informações sobre criptografia, assinatura digital e outras marcas digitais), contexto tecnológico (formato de arquivo, tamanho de arquivo, dependências de *hardware* e *software*, tipos de mídias, algoritmos de compressão) e localização física do documento (Resolução CONARQ nº 20/2004, art. 3º, § 3º).

**Operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (Lei nº 13.709/2018, art. 5º, VII).

**Órgão de pesquisa:** órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico (Lei nº 13.709/2018, art. 5º, XVIII).

**Preservação de documentos:** tratamento de acervos documentais que permita a prevenção da deterioração física dos documentos, com vistas à recuperação da informação (Resolução CONARQ nº 19/2003, art. 2º, III).

**Processo de digitalização:** realizado de forma a manter a integridade, a autenticidade e, se necessário, a confidencialidade do documento digital, com o emprego de assinatura eletrônica (Lei nº 12.682/2012, art. 3º) .

**Recolhimento:** entrada de documentos para guarda permanente em instituições arquivísticas públicas (Resolução CONARQ nº 02/1995, art. 1º, § 2º).

**Relatório de impacto à proteção de dados pessoais:** documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco (Lei nº 13.709/2018, art. 5º, XVII).

**Requisitos:** conjunto de condições a serem cumpridas pela organização produtora/recebedora de documentos, pelo sistema de gestão arquivística e pelos próprios documentos a fim de garantir a sua confiabilidade e autenticidade, bem como seu acesso (Resolução CONARQ nº 50/2022, art. 2º, § 2º).

**Titular:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (Lei nº 13.709/2018, art. 5º, V).

**Transferência internacional de dados:** transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro (Lei nº 13.709/2018, art. 5º, XV).

**Transferência:** passagem de documentos de um arquivo corrente para o arquivo intermediário, onde aguardarão sua destinação final: eliminação ou recolhimento para guarda permanente (Resolução CONARQ nº 02/1995, art. 1º, § 1º).

**Tratamento:** toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (Lei nº 13.709/2018, art. 5º, X).

**Uso compartilhado de dados:** comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados (Lei nº 13.709/2018, art. 5º, XVI).

# Referências

ANDRADE, Rogério Ferraz Garcia. O cientista de dados arquivisticos: o encontro da arquivística com as ciências de dados. *In:* SIMPÓSIO INTERNACIONAL DE ARQUIVOS: **Arquivo, Documento e Informação em Cenários Híbridos, 2020. Arquivo, documento e informação em cenários híbridos*:*** anais do Simpósio Internacional de Arquivos. São Paulo: Eventus 8, 2021. Disponível em: https://even3.blob.core.windows.net/processos/f51c256d499f42b68b73.pdf. Acesso em: 28 abr. 2022

ARQUIVO PÚBLICO DO ESTADO (São Paulo). **Guia para a avaliação dinâmica da massa documental acumulada: eliminação rápida e segura de documentos de arquivo**. São Paulo: Arquivo Público do Estado, 2022a. Disponível em: http://www.arquivoestado.sp.gov.br/uploads/publicacoes/livros/guia_avaliacao_massa_documental_acumulada.pdf. Acesso em: 28 out. 2022

ARQUIVO PÚBLICO DO ESTADO (São Paulo); TRIBUNAL DE CONTAS DO ESTADO DE SÃO PAULO**. Guia técnico da transparência municipal**. São Paulo: Arquivo Público do Estado/Tribunal de Contas do Estado de São Paulo, 2018a. Disponível em: http://www.arquivoestado.sp.gov.br/site/assets/publicacao/anexo/guia_tecnico_de_transparencia_municipal.pdf. Acesso em: 28 abr. 2022

ARQUIVO PÚBLICO DO ESTADO (São Paulo). **Instrução Normativa APE/SAESP nº 01, de 10 de março de 2009.** Estabelece diretrizes e define procedimentos para a gestão, a preservação e o acesso contínuo aos documentos arquivísticos digitais da Administração Pública Estadual Direta e Indireta. São Paulo: Arquivo Público do Estado, 2009. Disponível em: http://www.arquivoestado.sp.gov.br/site/assets/legislacao/Instrucao%20Normativa_10_3_2009.pdf. Acesso em: 28 abr. 2022 (Ver a Portaria UAPESP/SAESP nº 04, de 23 de novembro de 2020)

ARQUIVO PÚBLICO DO ESTADO (São Paulo). **Instrução Normativa APE/SAESP nº 02, de 02 de dezembro de 2010**. Estabelece critérios para a avaliação da massa documental acumuladas e procedimentos para eliminação, transferência e recolhimento de documentos à Unidade do Arquivo Público do estado. São Paulo: Arquivo Público do Estado, 2010. Disponível em: http://www.arquivoestado.sp.gov.br/uploads/legislacao/instrucao_normativa_ape_saesp_2_de_02_12_2010.pdf. Acesso em: 06 set. 2022

ARQUIVO PÚBLICO DO ESTADO (São Paulo). **Instrução Normativa APE/SAESP nº 03, de 14 de setembro de 2015**. Estabelece critérios complementares à Instrução Normativa APE/SAESP nº 2, de 2-12-2010, para o recolhimento de documentos à Unidade do Arquivo Público do Estado, visando a efetiva aplicação do Decreto Estadual nº 60.145/2014. São Paulo: Arquivo Público do Estado, 2015.

Disponível em: http://www.arquivoestado.sp.gov.br/uploads/legislacao/instrucao_normativa_ape_saesp_3_de_14_09_2015.pdf. Acesso em: 06 set. 2022

ARQUIVO PÚBLICO DO ESTADO (São Paulo). **Manual de normas e procedimentos de protocolo para a Administração Pública do Estado de São Paulo**. São Paulo: Arquivo Público do Estado, 2013. Disponível em: http://www.arquivoestado.sp.gov.br/site/assets/publicacao/anexo/manual_de_normas_e_procedimentos_de_protocolo_para_a_administracao_publica_do_estado_de_sao_paulo.pdf. Acesso em: 30 set. 2022

ARQUIVO PÚBLICO DO ESTADO (São Paulo). **Modelo de plano de classificação e tabela de temporalidade de documentos do poder legislativo municipal (atividades fim e meio)**: por uma política pública de gestão documental nas câmaras municipais. São Paulo: Arquivo Público do Estado, 2018b. Disponível em: http://www.arquivoestado.sp.gov.br/site/assets/publicacao/anexo/Modelo_PC_TTD_Legislativo%20(2).pdf. Acesso em: 28 abr. 2022

ARQUIVO PÚBLICO DO ESTADO (São Paulo). **Plano Diretor** (Arquivo público do Estado). São Paulo: Arquivo Público do Estado, 2019. Disponível em: http://www.arquivoestado.sp.gov.br/web/institucional/quem_somos/plano_diretor. Acesso em: 28 abr. 2022

ARQUIVO PÚBLICO DO ESTADO (São Paulo). **Portaria UAPESP nº 02, de 16 de junho de 2021.** Institui o "ArquivoDigital.SP" na Unidade do Arquivo Público do Estado. São Paulo: Arquivo Público do Estado, 2021. Disponível em: http://www.arquivoestado.sp.gov.br/uploads/legislacao/portaria_uapesp_2_de_11_06_2021.pdf. Acesso em: 28 abr. 2022

ARQUIVO PÚBLICO DO ESTADO (São Paulo). **Portaria UAPESP/SAESP nº 01, de 04 de dezembro de 2018c.** Dispõe sobre diretrizes para a contratação de serviços arquivísticos visando à execução de atividades técnicas auxiliares São Paulo: Arquivo Público do Estado, 2018c. Disponível em: http://www.arquivoestado.sp.gov.br/uploads/legislacao/portaria_uapesp_saesp_1_de_4_12_2018.pdf. Acesso em: 28 abr. 2022

ARQUIVO PÚBLICO DO ESTADO (São Paulo). **Portaria UAPESP/SAESP nº 02, de 04 de dezembro de 2018d.** Dispõe sobre procedimentos para orientar a modelagem de documentos digitais. São Paulo: Arquivo Público do Estado, 2018d. Disponível em: http://www.arquivoestado.sp.gov.br/site/assets/legislacao/105_Portaria_UAPESPSAESP_2_de_04_12_2018.pdf. Acesso em: 28 abr. 2022

ARQUIVO PÚBLICO DO ESTADO (São Paulo). **Portaria UAPESP/SAESP nº 04, de 23 de novembro de 2020.** Substitui os Anexos I e II da Instrução Normativa APE/SAESP nº 1, de 10 de março de 2009, que definem os requisitos e metadados a serem adotados pelo ambiente digital de gestão documental ("Documentos Digitais") do SP Sem Papel e por outros sistemas autorizados de gestão arquivística de documentos. São Paulo: Arquivo Público do Estado, 2020. Disponível em: http://www.arquivoestado.sp.gov.br/site/assets/legislacao/2020_11_24_Portaria%20UAPESP_SAESP-4_23-11-2020-mesclado.pdf. Acesso em: 28 abr. 2022

ARQUIVO PÚBLICO DO ESTADO (São Paulo). **Portaria UAPESP/SAESP nº 05, de 05 de agosto de 2021.** Orienta os órgãos e entidades da Administração Pública Estadual sobre a digitalização de documentos públicos, a gestão e a preservação de seus representantes digitais para que produzam os mesmos efeitos legais de documentos originais. São Paulo: Arquivo Público do Estado, 2021. Disponível em: http://www. http://www.arquivoestado.sp.gov.br/uploads/legislacao/portaria_uapesp_saesp_5_de_05_08_2021.pdf. Acesso em: 06 set. 2022

ARQUIVO PÚBLICO DO ESTADO (São Paulo). **Portaria UAPESP/SAESP nº 09, de 18 de abril de 2022.** Acrescenta o ANEXO II à Portaria UAPESP/SAESP - 1, de 4-12-2018, com as especificações técnicas para contratação de serviços de digitalização de documentos públicos estaduais. São Paulo: Arquivo Público do Estado, 2022b. Disponível em: http://www.arquivoestado.sp.gov.br/uploads/legislacao/portaria_uapesp_saesp_9_de_18_4_2022.pdf. Acesso em: 28 abr. 2022

ARQUIVO PÚBLICO DO ESTADO (São Paulo). **Portaria UAPESP/SAESP nº 10, de 14 de dezembro de 2022.** Estabelece critérios e procedimentos complementares para a eliminação, transferência ou recolhimento de documentos digitais, produzidos e armazenados por órgãos e entidades integrantes do Sistema de Arquivos do Estado de São Paulo – SAESP, para os repositórios arquivísticos digitais confiáveis da Unidade do Arquivo Público do Estado – UAPESP. São Paulo: Arquivo Público do Estado, 2022c. Disponível em: http://www.arquivoestado.sp.gov.br/uploads/legislacao/portaria_uapesp_saesp_10_de_14_12_2022.pdf. Acesso em: 28 abr. 2022

ARQUIVO PÚBLICO DO ESTADO (São Paulo). **Procedimentos para recolhimento de documentos de guarda permanente.** Coleção Gestão Documental nº 1. São Paulo: Arquivo Público do Estado, 2014. Disponível em: http://www.arquivoestado.sp.gov.br/uploads/publicacoes/livros/procedimentos_para_recolhimento_de_documentos_de_guarda_permanente.pdf. Acesso em: 28 abr. 2022

ARQUIVO NACIONAL (Brasil). **AN digital**: Política de Preservação Digital (versão 2). Rio de Janeiro: Arquivo Nacional, 2016. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/portarias-federais/Politica_Preservacao_Digital_v2.pdf. Acesso em: 28 abr. 2022

ARQUIVOS NACIONAIS DA AUSTRÁLIA / NATIONAL ARCHIVES OF AUSTRALIA. **Digitalisation specifications for paper records in agencies**. Disponível em: https://www.naa.gov.au/information-management/capturing-information/digitisation-specifications-paper-records-agencies. Acesso em: 19 out. 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO 14721**: Sistemas espaciais de transferência de dados e de informação — Sistema Aberto de Arquivamento de Informação (SAAI) — Modelo de referência (Space data and information transfer systems - Open Archival Information System (OAIS) - Reference model). Rio de Janeiro: ABNT, 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27001**: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de

segurança da informação — Requisitos (Information technology — Security techniques — Information security management systems — Requirements). Rio de Janeiro: ABNT, 2013.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **A LGPD e o tratamento de dados pessoais para fins acadêmicos e para a realização de estudos por órgão de pesquisa** (Estudo Técnico - Texto para discussão nº 1/2022). Brasília: ANPD, 2022. Disponível em: www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_00261-000810_2022_17.pdf. Acesso em: 24 out. 2022

BERNARDES, Ieda Pimenta. **Como avaliar documentos de arquivo**. São Paulo: Arquivo do Estado, 1998 (Projeto Como Fazer, v. 1). Disponível em: file:///C:/Users/maria.p/Desktop/como_avaliar_documentos_de_arquivo.pdf. Acesso em: 28 abr. 2022

BERNARDES, Ieda Pimenta; DELATORRE, Hilda. **Gestão documental aplicada**. São Paulo: Arquivo Público do Estado, 2008. Disponível em: http://www.arquivoestado.sp.gov.br/site/assets/publicacao/anexo/gestao_documental_aplicada.pdf. Acesso em: 28 abr. 2022

BERNARDES, Ieda Pimenta. Gestão documental e direito de acesso: interfaces. **Acervo**, Rio de Janeiro (Arquivo Nacional), v. 28, nº 2, p. 164-179, 27 nov. 2015. Disponível em: https://revista.an.gov.br/index.php/revistaacervo/article/view/616/667. Acesso em: 28 abr. 2022.

BERNARDES, Ieda Pimenta. O impacto das políticas de gestão documental na implementação da Lei Geral de Proteção de Dados (LGPD). *In*: SIMPÓSIO INTERNACIONAL DE ARQUIVOS: Arquivo, Documento e Informação em Cenários Híbridos, 2020a (evento online). **Arquivo, documento e informação em cenários híbridos**: anais do Simpósio Internacional de Arquivos. São Paulo: Eventus 8, 2021. Disponível em: https://even3.blob.core.windows.net/processos/9b3aea-2b56a04797870b.pdf. Acesso em: 28 abr. 2022

BERNARDES, Ieda Pimenta. Os Arquivos e a construção da Democracia: 30 anos do Sistema de Arquivos do Estado de São Paulo – SAESP (1984-2014). *In*: **Arquivos, entre tradição e modernidade**, volume 1: conferências e trabalhos premiados com menção honrosa apresentados no XI Congresso de Arquivologia do Mercosul. Organização: Ana Célia Navarro de Andrade, Associação de Arquivistas de São Paulo. São Paulo: ARQ-SP, 2017 (Eventus, 1), p. 201-214. Disponível em: http://arqsp.org.br/wp-content/uploads/2017/09/XI-CAM-VOL.-1_e-book.pdf. Acesso em: 28 abr. 2022

BERNARDES, Ieda Pimenta. Os desafios da gestão e preservação de documentos arquivísticos digitais. **Revista do Arquivo**, São Paulo, Ano II, nº 6, p. 190 - 207, abril de 2018. Disponível em: http://www.arquivoestado.sp.gov.br/revista_do_arquivo/06/especial_seminario_apresentacao_01.php#inicio_artigo . Acesso em: 28 abr. 2022

BERNARDES, Ieda Pimenta; RIBEIRO, Camila Giovana; PEREIRA, Maria Elisa (organizadoras). **Política Pública de Arquivos e Gestão Documental do Estado de São Paulo**. 3ª ed. São Paulo: Arquivo Público do Estado, 2022. Disponível em: http://www.arquivoestado.sp.gov.br/uploads/publicacoes/livros/Politicas_Publicas_3ed.pdf. Acesso em: 28 out. 2022

BERNARDES, Ieda Pimenta. **Relatório final do Grupo de Estudos sobre Lei Geral de Proteção de Dados – LGPD do Conselho de Transparência da Administração Pública.** São Paulo: Conselho de Transparência da Administração Pública 2020b. Disponível em: http://www.transparencia.sp.gov.br/conselho/documentos/97/Relat%C3%B3rio%20Final%20do%20Grupo%20de%20Estudos%20da%20LGPD%20-%20Conselho%20da%20Transpar%C3%AAncia%202020.pdf

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil, de 1988**. Brasília: Presidência da República, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.htm. Acesso em: 28 abr. 2022

BRASIL. **Decreto nº 1.799, de 30 de janeiro de 1996.** Regulamenta a Lei nº 5.433, de 8 de maio de 1968, que regula a microfilmagem de documentos oficiais, e dá outras providências. Brasília: Presidência da República, 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/antigos/d1799.htm. Acesso em: 28 abr. 2022

BRASIL. **Decreto nº 8.539, de 8 de outubro de 2015.** Dispõe sobre o uso do meio eletrônico para a realização do processo administrativo no âmbito dos órgãos e das entidades da administração -pública federal direta, autárquica e fundacional. Brasília: Presidência da República, 2015. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/decreto/d8539.htm. Acesso em: 28 abr. 2022

BRASIL. **Decreto nº 9.637, de 26 de dezembro de 2018.** Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput , inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Brasília: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm. Acesso em: 14 dez. 2022

BRASIL. **Decreto nº 10.278, de 18 de março de 2020.** Regulamenta o disposto no inciso X do caput do art. 3º da Lei nº 13.874, de 20 de setembro de 2019, e no art. 2º-A da Lei nº 12.682, de 9 de julho de 2012, para estabelecer a técnica e os requisitos para a digitalização de documentos públicos ou privados, a fim de que os documentos digitalizados produzam os mesmos efeitos legais dos documentos originais. Brasília: Presidência da República, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10278.htm. Acesso em: 28 abr. 2022

BRASIL. **Decreto nº 10.641, de 2 de março de 2021.** Altera o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Brasília: Presidência da República, 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/D10641.htm. Acesso em: 14 dez. 2022

BRASIL. **Lei nº 5.433, de 08 de maio de 1968.** Regula a microfilmagem de documentos oficiais e dá outras providências. Brasília: Presidência da República, 1968. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L5433.htm. Acesso em: 28 abr. 2022

BRASIL. **Lei nº 8.159, de 09 de janeiro de 1991**. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. Brasília: Presidência da República, 1991. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L8159.htm. Acesso em: 28 abr. 2022

BRASIL. **Lei nº 9.610, de 19 de fevereiro de 1998**. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Brasília: Presidência da República, 1998. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9610.htm. Acesso em: 28 abr. 2022

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do artigo 5º, no inciso II do § 3º do artigo 37 e no § 2º do artigo 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 05 de maio de 2005, e dispositivos da Lei nº 8.159, de 08 de janeiro de 1991; e dá outras providências. Brasília: Presidência da República, 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.htm. Acesso em: 28 abr. 2022

BRASIL. **Lei nº 12.682, de 9 de julho de 2012**. Dispõe sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos. Brasília: Presidência da República, 2012a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12682.htm. Acesso em: 28 abr. 2022

BRASIL. **Lei nº 12.853, de 14 de agosto de 2013**. Altera os arts. 5º, 68, 97, 98, 99 e 100, acrescenta os arts. 98-A, 98-B, 98-C, 99-A, 99-B, 100-A, 100-B e 109-A e revoga o art. 94 da Lei nº 9.610, de 19 de fevereiro de 1998, para dispor sobre a gestão coletiva de direitos autorais, e dá outras providências. Brasília: Presidência da República, 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12853.htm. Acesso em: 28 abr. 2022

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 28 abr. 2022

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais – LGPD. Brasília: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 31 ago. 2022

BRASIL. **Lei nº 13.874, de 20 de setembro de 2019.** Institui a Declaração de Direitos de Liberdade Econômica; estabelece garantias de livre mercado; altera as Leis nos 10.406, de 10 de janeiro de 2002 (Código Civil), 6.404, de 15 de dezembro de 1976, 11.598, de 3 de dezembro de 2007, 12.682, de 9 de julho de 2012, 6.015, de 31 de dezembro de 1973, 10.522, de 19 de julho de 2002, 8.934, de 18 de novembro 1994, o Decreto-Lei nº 9.760, de 5 de setembro de 1946 e a Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943; revoga a Lei Delegada nº 4, de 26 de setembro de 1962, a Lei nº 11.887, de 24 de dezembro de 2008, e dispositivos do Decreto-Lei nº 73, de 21 de novembro de 1966; e dá outras providências. Brasília: Presidência da República, 2019a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13874.htm. Acesso em: 28 abr. 2022

BRASIL. **Medida Provisória nº 2.200-2, de 24 de Agosto de 2001.** Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Brasília: Presidência da República, 2001. Disponível em: http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm. Acesso em: 28 abr. 2022

BRASIL. **Medida Provisória nº 1.124, de 13 de junho de 2022**. Altera a Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais, transforma a Autoridade Nacional de Proteção de Dados em autarquia de natureza especial e transforma cargos em comissão. Brasília: Presidência da República, 2022b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/Mpv/mpv1124.htm . Acesso em: 24 out. 2022

BRASIL. CÂMARA DOS DEPUTADOS. **Ato da Mesa da Câmara dos Deputados nº 48, de 16 de julho de 2012**. Institui a Política de Preservação Digital da Câmara dos Deputados. Brasília: Câmara dos Deputados/Centro de Documentação e Informação, 2012b. Disponível em: https://www2.camara.leg.br/legin/int/atomes/2012/atodamesa-48-16-julho-2012-773828-normaatualizada-cd-mesa.pdf. Acesso em: 28 abr. 2022

BRASIL. MINISTÉRIO DA FAZENDA; BANCO CENTRAL DO BRASIL (BACEN). **Resolução nº 4.474, de 31 de março de 2016**. Dispõe sobre a digitalização e a gestão de documentos digitalizados relativos às operações e às transações realizadas pelas instituições financeiras e pelas demais instituições autorizadas a funcionar pelo Banco Central do Brasil, bem como sobre o procedimento de descarte das matrizes físicas dos documentos digitalizados e armazenados eletronicamente. Brasília: BACEN, 2016a. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes/resolucao-no-4-474-de-31-de-marco-de-2016. Acesso em: 19 dez. 2022

BRASIL. MINISTÉRIO DA JUSTIÇA E CIDADANIA; ARQUIVO NACIONAL. **Instrução Técnica AN DIGITAL Nº 01/2016**. Brasília: MJC/AN, 2016b. Disponível em: https://www.gov.br/arquivonacional/pt-br/servicos/gestao-de-documentos/orientacao-tecnica-1/it_an_digital_01_entrada_documentos_digitais.pdf. Acesso em: 5 de set. 2022.

BRASIL. MINISTÉRIO DA JUSTIÇA E CIDADANIA; ARQUIVO NACIONAL. **Recomendações para elaboração de política de preservação digital**. Brasília: MJC/AN, 2019b. Disponível em: https://www.gov.br/arquivonacional/pt-br/servicos/gestao-de-documentos/orientacao-tecnica-1/recomendacoes-tecnicas-1/politica_preservacao_digital.pdf. Acesso em: 5 de set. 2022.

BRASIL. MINISTÉRIO DO PLANEJAMENTO ORÇAMENTO E GESTÃO (MP); SECRETARIA DE LOGÍSTICA E TECNOLOGIA DA INFORMAÇÃO (SLTI). **Cartilha Técnica para Publicação de Dados Abertos no Brasil, v 1.0**. Brasília: MP/SLTI, s/d. Disponível em: https://wiki-dados-h.cgu.gov.br/CartilhaTecnicaparaPublica%C3%A7%C3%A3odeDadosAbertosnoBrasil.ashx?Code=1. Acesso em: 5 de set. 2022.

CAMPOS, Rogério Madeira de Moura; ESTRELLA, Leandro Teixeira; FARIAS, Aline Ribeiro de; QUEIROZ, Elisangela Mendes. Relato da experiência do Arquivo Público do Estado de São Paulo no Programa São Paulo Sem Papel – Documentos Digitais. **Manduarisawa**, Revista Eletrônica Discente do Curso de História da Universidade Federal do Amazonas – UFAM, Manaus, volume 4, nº 1, ano 4, 2020, p. 412-421. Disponível em: https://www.periodicos.ufam.edu.br/index.php/manduarisawa/article/view/7590. Acesso em: 28 abr. 2022

COMITÊ GESTOR DE GOVERNANÇA DE DADOS E INFORMAÇÕES DO ESTADO DE SÃO PAULO (CGGDIESP). **Deliberação Normativa CGGDIESP-1, de 30 de dezembro de 2021**. Institui a Política de Governança de Dados e Informações – PGDI, no âmbito da Administração Pública Estadual e dá providências correlatas. São Paulo: CGGDIESP, 2021a, (p. 1-33). Disponível em: http://www.coetic.sp.gov.br/anexos/Politicas_PGDI_PPDP_ESP_2021-12-30.pdf. (p. 1-33). Acesso em: 28 abr. 2022

COMITÊ GESTOR DE GOVERNANÇA DE DADOS E INFORMAÇÕES DO ESTADO DE SÃO PAULO (CGGDIESP). **Deliberação Normativa CGGDIESP-2, de 30 de dezembro de 2021**. Institui a Política de Proteção de Dados – PPDP no âmbito da Administração Pública Estadual e dá providências correlatas. São Paulo: CGGDIESP, 2021b, p. 34-63. Disponível em: http://www.coetic.sp.gov.br/anexos/Politicas_PGDI_PPDP_ESP_2021-12-30.pdf (p. 34-63). Acesso em: 28 abr. 2022

CONSELHO FEDERAL DE MEDICINA (CFM). **Código de Ética Médica**. Brasília: CFM, 2010. Disponível em: https://rcem.cfm.org.br/index.php/cem-atual. Acesso em: 24 out. 2022

CONSELHO FEDERAL DE MEDICINA (CFM). **Recomendação CFM nº 03/14**. Brasília: CFM, 2014. Disponível em: https://portal.cfm.org.br/images/Recomendacoes/3_2014.pdf. Acesso em: 24 out. 2022

CONSELHO INTERNACIONAL DE ARQUIVOS (CIA) / INTERNATIONAL COUNCIL ON ARCHIVES (ICA). **Declaração universal sobre os arquivos – DUA** (Universal

Declaration on Archives – UDA). Oslo: ICA, 2010. Disponível em: http://www.arquivoestado.sp.gov.br/site/assets/eventos/convite/Panfleto_Dia_Arquivo.pdf. Acesso em: 10 mai. 2022

CONSELHO INTERNACIONAL DE ARQUIVOS (CIA) / INTERNATIONAL COUNCIL ON ARCHIVES (ICA). **ISAD(G)**: Norma geral internacional de descrição arquivística: segunda edição, adotada pelo Comitê de Normas de Descrição, Estocolmo, Suécia, 19-22 de setembro de 1999, versão final aprovada pelo CIA. Rio de Janeiro (RJ): Arquivo Nacional, 2000. Disponível em: https://www.gov.br/conarq/pt-br/centrais-de-conteudo/publicacoes/isad_g_2001.pdf. Acesso em: 10 dez. 2022

CONSELHO NACIONAL DE ARQUIVOS (CONARQ); CÂMARA TÉCNICA DE DOCUMENTOS ELETRÔNICOS (CTDE). **Carta para a preservação do patrimônio arquivístico digital**. Rio de Janeiro: UNESCO/CONARQ/CTDE, 2005. Disponível em: https://www.gov.br/conarq/pt-br/centrais-de-conteudo/publicacoes/conarq_carta_preservacao_patrimonio_arquivistico_digital.pdf. Acesso em: 28 abr. 2022

CONSELHO NACIONAL DE ARQUIVOS (CONARQ); CÂMARA TÉCNICA DE DOCUMENTOS ELETRÔNICOS (CTDE). **Criação e desenvolvimento de Arquivos Públicos municipais: transparência e acesso à informação para o exercício da cidadania**. Rio de Janeiro: Arquivo Nacional, 2014c. Disponível em: https://www.gov.br/conarq/pt-br/centrais-de-conteudo/publicacoes/Cartilha_criacao_arquivos_municipais.pdf. Acesso em: 28 abr. 2022

CONSELHO NACIONAL DE ARQUIVOS (CONARQ); CÂMARA TÉCNICA DE DOCUMENTOS ELETRÔNICOS (CTDE). **e-ARQ Brasil**: Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos. Versão 2. Rio de Janeiro: Arquivo Nacional / CONARQ, 2022b. Disponível em: https://www.gov.br/conarq/pt-br/centrais-de-conteudo/publicacoes/EARQV205MAI2022.pdf . Acesso em: 16 mai. 2022.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ); CÂMARA TÉCNICA DE DOCUMENTOS ELETRÔNICOS (CTDE). **Glossário** - Documentos Arquivísticos Digitais. Rio de Janeiro: CONARQ/CTDE, 8ª Versão, 2020. Disponível em: https://www.gov.br/conarq/pt-br/assuntos/camaras-tecnicas-setoriais-inativas/camara-tecnica-de-documentos-eletronicos-ctde/glosctde_2020_08_07.pdf. Acesso em: 28 out. 2022

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Resolução nº 01, de 18 de outubro de 1995.** Dispõe sobre a necessidade da adoção de planos e ou códigos de classificação de documentos nos arquivos correntes, que considerem a natureza dos assuntos resultantes de suas atividades e funções. Rio de Janeiro: CONARQ, 1995a. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-1-de-18-de-outubro-de-1995. Acesso em: 28 abr. 2022

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Resolução nº 02, de 18 de outubro de 1995.** Dispõe sobre as medidas a serem observadas na transferência ou no recolhimento de acervos documentais para instituições arquivísticas públicas. Rio de Janeiro: CONARQ, 1995b. Disponível em: https://www.gov.br/conarq/

pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-2-de-18-de-outubro-de-1995. Acesso em: 28 abr. 2022

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Resolução nº 19, de 28 de outubro de 2003.** Dispõe sobre os documentos públicos que integram o acervo das empresas em processo de desestatização e das pessoas jurídicas de direito privado sucessoras de empresas públicas. Rio de Janeiro: CONARQ, 2003. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-19-de-28-de-outubro-de-2003. Acesso em: 28 abr. 2022

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Resolução nº 20, de 16 de julho de 2004.** Dispõe sobre a inserção dos documentos digitais em programas de gestão arquivística de documentos dos órgãos e entidades integrantes do Sistema Nacional de Arquivos. Rio de Janeiro: CONARQ, 2004. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-20-de-16-de-julho-de-2004. Acesso em: 28 abr. 2022

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Resolução nº 25, de 27 de abril de 2007.** Dispõe sobre a adoção do Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil pelos órgãos e entidades integrantes do Sistema Nacional de Arquivos - SINAR. Rio de Janeiro: CONARQ, 2007. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-25-de-27-de-abril-de-2007. Acesso em: 28 abr. 2022

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Resolução nº 27, de 16 de junho de 2008.** Dispõe sobre o dever do Poder Público, no âmbito dos Estados, do Distrito Federal e dos Municípios, de criar e manter Arquivos Públicos, na sua específica esfera de competência, para promover a gestão, a guarda e a preservação de documentos arquivísticos e a disseminação das informações neles contidas. Rio de Janeiro: CONARQ, 2008. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-27-de-16-de-junho-de-2008. Acesso em: 28 abr. 2022

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Resolução nº 31, de 28 de abril de 2010**. Dispõe sobre a adoção das Recomendações para Digitalização de Documentos Arquivísticos Permanentes. Rio de Janeiro: CONARQ, 2010a. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-31-de-28-de-abril-de-2010. Acesso em: 28 abr. 2022

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Resolução nº 32, de 17 de maio de 2010**. Dispõe sobre a inserção dos Metadados na Parte II do Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil. Rio de Janeiro: CONARQ, 2010b. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-32-de-17-de-maio-de-2010. Acesso em: 28 abr. 2022

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Resolução nº 36, de 19 de dezembro de 2012**. Dispõe sobre a adoção das Diretrizes para a Gestão arquivística

do Correio Eletrônico Corporativo pelos órgãos e entidades integrantes do Sistema Nacional de Arquivos – SINAR. Rio de Janeiro: CONARQ, 2012a. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-36-de-19-de-dezembro-de-2012. Acesso em: 28 abr. 2022

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Resolução nº 37, de 19 de dezembro de 2012**. Aprova as Diretrizes para a Presunção de Autenticidade de Documentos Arquivísticos Digitais. Rio de Janeiro: CONARQ, 2012b. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-37-de-19-de-dezembro-de-2012. Acesso em: 28 abr. 2022

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Resolução nº 38, de 9 de julho de 2013**. Dispõe sobre a adoção das "Diretrizes do Produtor - A Elaboração e a Manutenção de Materiais Digitais: Diretrizes Para Indivíduos" e "Diretrizes do Preservador - A Preservação de Documentos Arquivísticos digitais: Diretrizes para Organizações". Rio de Janeiro: CONARQ, 2013. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-38-de-9-de-julho-de-2013. Acesso em: 28 abr. 2022

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Resolução nº 39, de 29 de abril de 2014**. Estabelece diretrizes para a implementação de repositórios arquivísticos digitais confiáveis para o arquivamento e manutenção de documentos arquivísticos digitais em suas fases corrente, intermediária e permanente, dos órgãos e entidades integrantes do Sistema Nacional de Arquivos - SINAR. [Redação dada pela Resolução nº 43 de 04 de setembro de 2015]. Rio de Janeiro: CONARQ, 2014a. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-39-de-29-de-abril-de-2014. Acesso em: 28 abr. 2022

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Resolução nº 40, de 09 de dezembro de 2014** (alterada pela Resolução 44/2020). Dispõe sobre os procedimentos para a eliminação de documentos no âmbito dos órgãos e entidades integrantes do Sistema Nacional de Arquivos – SINAR. Rio de Janeiro: CONARQ, 2014b. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-40-de-9-de-dezembro-de-2014-alterada. Acesso em: 10 mai. 2022.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Resolução nº 43, de 04 de setembro de 2015**. Altera a redação da Resolução do CONARQ nº 39, de 29 de abril de 2014, que estabelece diretrizes para a implementação de repositórios digitais confiáveis para a transferência e recolhimento de documentos arquivísticos digitais para instituições arquivísticas dos órgãos e entidades integrantes do Sistema Nacional de Arquivos - SINAR. Rio de Janeiro: CONARQ, 2015. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-43-de-04-de-setembro-de-2015. Acesso em: 28 abr. 2022

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Resolução nº 48, de 10 de novembro de 2021**. Estabelece diretrizes e orientações aos órgãos e entidades

integrantes do Sistema Nacional de Arquivos quanto aos procedimentos técnicos a serem observados no processo de digitalização de documentos públicos ou privados. Rio de Janeiro: CONARQ, 2021. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-48-de-10-de-novembro-de-2021. Acesso em: 10 mai. 2022.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). **Resolução nº 50, de 06 de maio de 2022**. Dispõe sobre o Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos, e-ARQ Brasil, Versão 2. Rio de Janeiro: CONARQ, 2022a. Disponível em: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-50-de-06-de-maio-de-2022. Acesso em: 10 mai. 2022.

COSTA, M. et al. **Guia do usuário Archivematica.** Brasília: Instituto Brasileiro de Informação em Ciência e Tecnologia, 2016. Disponível em: https://livroaberto.ibict.br/bitstream/123456789/1063/4/Manual-Archivematica.pdf. Acesso em: 13.dez.2022

EUROPEAN ARCHIVES GROUP / GRUPO DE ARQUIVOS EUROPEUS. **Guidance on data protection for archive services**: EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector. Bruxelas (Bélgica): European Archives Group, 2018. Disponível em: https://ec.europa.eu/info/sites/default/files/eag_draft_guidelines_1_11_0.pdf. Acesso em: 28 out. 2022

GOUVEIA, Luís Borges. **Gestão da Segurança da Informação** - Conceitos básicos e introdução ao tema da Gestão da Segurança da Informação no contexto do digital e dos Sistemas e Tecnologias de Informação. Porto (Portugal): Repositório Institucional da Universidade Fernando Pessoa, 2016. Disponível em: https://bdigital.ufp.pt/bitstream/10284/5954/1/securv1_1_mar2016.pdf. Acesso em: 08 dez. 2022

FEITOSA, Eduardo Luzeiro. **Segurança em Sistemas de Informação**. Recife (PE): UFPE, 2005.

FLORES, Daniel; ROCCO, Brenda Couto de Brito; SANTOS, Henrique Machado dos. Cadeia de custódia para documentos arquivísticos digitais. **Acervo**, Rio de Janeiro (Arquivo Nacional), vol. 29, nº 2, p.117-132, 17 nov. 2016. Disponível em: https://revista.an.gov.br/index.php/revistaacervo/article/view/717/732. Acesso em: 28 abr. 2022

FUNDAÇÃO OSWALDO CRUZ – FIOCRUZ. **Programa de preservação digital de acervos da FIOCRUZ**. Rio de Janeiro: FIOCRUZ, 2020. Disponível em: https://www.arca.fiocruz.br/bitstream/icict/44220/4/Programa_Preservacao_Digital_Portugues. Acesso em: 28 abr. 2022

INNARELLI, Humberto Celeste. **Gestão da preservação de documentos arquivísticos digitais**: proposta de um modelo conceitual. 2015. Tese (Doutorado em Cultura e Informação) - Escola de Comunicações e Artes, Universidade de São Paulo, São Paulo, 2015. Disponível em: https://www.teses.usp.br/teses/disponiveis/27/27151/tde-27052015-101628/publico/HumbertoCelesteInnarelliVC.pdf. Acesso em: 19 dez. 2022

INARELLI, Humberto Celeste. Preservação digital e seus dez mandamentos. *In*: SANTOS, Vanderlei Batista dos. **Arquivística: temas contemporâneos**: classificação, preservação digital, gestão de conhecimento. Distrito Federal: SENAC, 2007, p. 21-75.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) / Organização Internacional para Padronização (ISO). **ISO 16363:2012**: Space data information transfer systems -- Audit and certification of trustworthy digital repositories. Genebra (Suíça): ISO, 2012.

INTERPARES. **Diretrizes do preservador**. A preservação de documentos arquivísticos digitais: Diretrizes para as organizações. Tradução e revisão do Arquivo Nacional e Câmara dos Deputados. Brasília: Editoração da Câmara dos Deputados, 2010a. Disponível em: http://www.interpares.org/ip3/display_file.cfm?doc=ip2_preserver_guidelines_booklet--portuguese.pdf. Acesso em: 07 dez. 2022

INTERPARES. **Diretrizes do produtor**. A elaboração e a manutenção de materiais digitais: Diretrizes para os indivíduos. Tradução e revisão do Arquivo Nacional e Câmara dos Deputados. Brasília: Editoração da Câmara dos Deputados, 2010b. Disponível em: http://interpares.org/ip3/display_file.cfm?doc=creator_guidelines_booklet--portuguese.pdf. Acesso em: 03 out. 2022

KLER, Evelyn Ruth; PRADO, Gelson. **Segurança de redes** - sistema de detecção de intrusão. Monografia (Especialização). Curso de Administração, com ênfase em análise de sistemas. Faculdade Internacional de Curitiba: Curitiba (PR), 2004.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Declaração Universal dos Direitos Humanos**. Paris (Fr): ONU, 1948. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 19 out. 2022

PARLAMENTO EUROPEU; CONSELHO DA UNIÃO EUROPEIA. **Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho de 23 de outubro de 2018**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) nº 45/2001 e a Decisão nº 1247/2002/CE. Estrasburgo (França): Jornal Oficial da União Europeia, 2018. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32018R1725&from=EN. Acesso em: 28 out. 2022

PLÁCIDO E SILVA, Oscar Joseph de. **Vocabulário Jurídico**. Rio de Janeiro: Editora Forense, 1980.

QUEENSLAND GOVERNMENT (AUSTRALIA). **Digitise physical records**. Disponível em: https://www.forgov.qld.gov.au/information-and-communication-technology/recordkeeping-and-information-management/recordkeeping/store-protect-and-care-for-records/digitise-physical-records. Acesso em: 19 out. 2022.

ROCHA, Claudia Lacombe. Repositórios para a preservação de documentos arquivísticos digitais. **Acervo**, Rio de Janeiro (Arquivo Nacional), v. 28, nº 2, p. 180-191,

27 nov. 2015. Disponível em: https://revista.an.gov.br/index.php/revistaacervo/article/view/608/669. Acesso em: 28 abr. 2022

ROCHA, Claúdia Lacombe; RONDINELLI, Rosely Curi. Gestão e preservação de documentos arquivísticos digitais. Revisitando alguns dos conceitos que as precedem. **Acervo**, Rio de Janeiro (Arquivo Nacional), v. 29, nº 2p. 61-73, 17 nov. 2016. Disponível em: https://revista.an.gov.br/index.php/revistaacervo/article/view/709/744. Acesso em: 28 abr. 2022

SÃO PAULO (Estado). **Decreto nº 30, de 10 de março de 1892.** Cria a Repartição da Estatística e do Arquivo do Estado. São Paulo: Assembleia Legislativa do Estado de São Paulo, 1892. Disponível em: https://www.al.sp.gov.br/repositorio/legislacao/decreto/1892/decreto-30-10.03.1892.html. Acesso em: 28 abr. 2022

SÃO PAULO (Estado). **Decreto nº 22.789, de 19 de outubro de 1984.** Institui o Sistema de Arquivos do Estado de São Paulo - SAESP. São Paulo: Assembleia Legislativa do Estado de São Paulo, 1984. Disponível em: https://www.al.sp.gov.br/repositorio/legislacao/decreto/1984/decreto-22789-19.10.1984.html. Acesso em: 28 abr. 2022

SÃO PAULO (Estado). **Decreto nº 48.897, de 27 de agosto de 2004.** Dispõe sobre os Arquivos Públicos, os documentos de arquivo e sua gestão, os Planos de Classificação e a Tabela de Temporalidade de Documentos da Administração Pública do Estado de São Paulo, define normas para a avaliação, guarda e eliminação de documentos de arquivo. São Paulo: Assembleia Legislativa do Estado de São Paulo, 2004a. Disponível em: https://www.al.sp.gov.br/repositorio/legislacao/decreto/2004/decreto-48897-27.08.2004.html. Acesso em: 28 abr. 2022

SÃO PAULO (Estado). **Decreto nº 48.898, de 27 de agosto de 2004**. Aprova o Plano de Classificação e a Tabela de Temporalidade de Documentos da Administração Pública do Estado de São Paulo: Atividades - Meio. São Paulo: Assembleia Legislativa do Estado de São Paulo, 2004b. Disponível em: https://www.al.sp.gov.br/repositorio/legislacao/decreto/2004/decreto-48898-27.08.2004.html. Acesso em: 26 dez. 2022

SÃO PAULO (Estado). **Decreto nº 54.276, de 27 de abril de 2009.** Reorganiza a Unidade do Arquivo Público do Estado, da Casa Civil, e dá providências correlatas. São Paulo: Assembleia Legislativa do Estado de São Paulo, 2009. Disponível em: https://www.al.sp.gov.br/repositorio/legislacao/decreto/2009/decreto-54276-27.04.2009.html. Acesso em: 28 abr. 2022

SÃO PAULO (Estado). **Decreto nº 58.052, de 16 de maio de 2012.** Regulamenta a Lei federal nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações, e dá providências correlatas. São Paulo: Assembleia Legislativa do Estado de São Paulo, 2012. Disponível em: https://www.al.sp.gov.br/repositorio/legislacao/decreto/2012/decreto-58052-16.05.2012.html . Acesso em: 28 abr. 2022

SÃO PAULO (Estado). **Decreto nº 60.145, de 11 de fevereiro de 2014.** Dispõe sobre o recolhimento de documentos de guarda permanente, produzidos e

acumulados pelos órgãos e entidades da Administração Pública estadual direta, indireta e fundacional, para a Unidade de Arquivo Público do Estado, da Casa Civil. São Paulo: Assembleia Legislativa do Estado de São Paulo (SP), 2014. Disponível em: https://www.al.sp.gov.br/repositorio/legislacao/decreto/2014/decreto-60145-11.02.2014.html. Acesso em: 28 abr. 2022

SÃO PAULO (Estado). **Decreto nº 61.836, de 18 de novembro de 2016.** Dispõe sobre a classificação de documento, dado ou informação sigilosa e pessoal no âmbito da Administração Pública direta e indireta. São Paulo: Assembleia Legislativa do Estado de São Paulo (SP), 2016. Disponível em: https://www.al.sp.gov.br/repositorio/legislacao/decreto/2016/decreto-61836-18.02.2016.html. Acesso em: 28 abr. 2022

SÃO PAULO (Estado). **Decreto nº 63.382, de 09 de maio de 2018.** Substitui os anexos do Decreto nº 48.898, de 27 de agosto de 2004, que aprova o Plano de Classificação e a Tabela de Temporalidade de Documentos da Administração Pública do Estado de São Paulo: Atividades-Meio, e dá providências correlatas. São Paulo: Assembleia Legislativa do Estado de São Paulo (SP), 2018. Disponível em: https://www.al.sp.gov.br/repositorio/legislacao/decreto/2018/decreto-63382-09.05.2018.html. Acesso em: 28 abr. 2022

SÃO PAULO (Estado). **Decreto nº 64.355, de 31 de julho de 2019.** Institui o Programa SP Sem Papel, seu Comitê de Governança Digital e dá providências correlatas. São Paulo: Assembleia Legislativa do Estado de São Paulo (SP), 2019a. Disponível em: https:// www.al.sp.gov.br/repositorio/legislacao/decreto/2019/decreto-64355-31.07.2019.html. Acesso em: 28 abr. 2022

SÃO PAULO (Estado). **Decreto nº 64.601, de 22 de novembro de 2019.** Reformula o Sistema de Tecnologia da Informação e Comunicação, reorganiza o Conselho Estadual de Tecnologia da Informação e Comunicação - COETIC, recria a Subsecretaria de Tecnologia e Serviços ao Cidadão, transfere e altera denominações de unidades da Secretaria de Governo e dá providências correlatas. São Paulo: Assembleia Legislativa do Estado de São Paulo (SP), 2019b. Disponível em: https://www.al.sp.gov.br/repositorio/legislacao/decreto/2019/decreto-64601-22.11.2019.html. Acesso em: 28 abr. 2022

SÃO PAULO (Estado). **Decreto nº 64.790, de 13 de fevereiro de 2020.** Institui a Central de Dados do Estado de São Paulo - CDESP, a Plataforma Única de Acesso - PUA e o Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo, e dá providências correlatas. São Paulo: Assembleia Legislativa do Estado de São Paulo (SP), 2020a. Disponível em: https://www.al.sp.gov.br/repositorio/legislacao/decreto/2020/decreto-64790-13.02.2020.html. Acesso em: 28 out. 2022

SÃO PAULO (Estado). **Decreto nº 66.017, de 15 de setembro de 2021**. Organiza a Secretaria de Orçamento e Gestão e dá providências correlatas. São Paulo: Assembleia Legislativa do Estado de São Paulo (SP), 2020b.

Disponível em: https://www.al.sp.gov.br/repositorio/legislacao/decreto/2021/decreto-66017-15.09.2021.html. Acesso em: 28 out. 2022

SÃO PAULO (Estado). CONSELHO DE TRANSPARÊNCIA DA ADMINISTRAÇÃO PÚBLICA. **Relatório final, Grupo de Estudos sobre a Lei Geral de Proteção de Dados – LGPD**. São Paulo: Conselho de Transparência da Administração Pública, 2021. Disponível em: http://www.transparencia.sp.gov.br/conselho/documentos/97/Relat%C3%B3rio%20Final%20do%20Grupo%20de%20Estudos%20da%20LGPD%20-%20Conselho%20da%20Transpar%C3%AAncia%202020.pdf . Acesso em 22 dez. 2022

SEMOLA, Marcos. **Gestão da Segurança da informação** - uma visão executiva. Rio de Janeiro (RJ): Campus, 2003.

UNIVERSIDADE ESTADUAL PAULISTA – UNESP. **Política de preservação digital para documentos de arquivo da UNESP**. São Paulo: UNESP, 2017. Disponível em: https://www2.unesp.br/portal#!/cppd/documentos/. Acesso em: 28 abr. 2022

Esta publicação utilizou em seu
projeto gráfico as fontes:
Roboto - Regular
Open Sans - Regular
Oswald - Extralight
O trabalho autoral da capa
contém documentos extraídos
do Acervo/APESP
e grafismos produzidos especialmente
para sua composição.

Arquivo Público
DO ESTADO DE SÃO PAULO
SÃO PAULO
GOVERNO DO ESTADO