



PLANO DE PRESERVAÇÃO DIGITAL

Realização:

Arquivo Público do Estado do Espírito Santo (APEES)
Instituto de Tecnologia da Informação e Comunicação do Estado do
Espírito Santo (Prodest)

Apoio:

Fundação de Amparo à Pesquisa e Inovação do Espírito Santo (FAPES)
Universidade Federal do Espírito Santo (Ufes)

RICARDO DE REZENDE FERRAÇO

Governador do Estado do Espírito Santo

MARCELO CALMON DIAS

Secretário de Estado de Gestão e Recursos Humanos

EDMAR MOREIRA CAMATA

Secretário de Estado de Controle e Transparência

MARCELO AZEREDO CORNÉLIO

Instituto de Tecnologia da Informação e Comunicação do Espírito Santo

CILMAR CESCO NETTO FRANCISCHETTO

Arquivo Público do Estado do Espírito Santo



Coordenação

Tânia Barbosa Salles Gava

Equipe técnica responsável pelo plano:

Alan Teixeira da Costa
Alex Pereira de Holanda
Ana Maria dos Santos Latgé
Daniel Brito de Oliveira Carvalho
Daniel Flores
Diana Vilas Boas Souto Aleixo
Eduardo Silva Guimarães
Érick Luiz do Valle Lopes
Felipe Mariano Matos
Gabriel Gatti
Gabriel Sena da Cunha
Gabriela De Grande Guerreiro
Guilherme José dos Santos
João Vitor Cosmo
José Márcio Moraes Dorigueto
Juliana Oliveira de Almeida
Jussara Teixeira
Kaio Silva Rosa
Michel Caldeira de Souza
Roberto Marconi de Macedo Filho
Marcos Tadeu de Araujo Torres
Vitor Estevão Silva Souza
Wagner Santana Bianchi
Wendel Luiz Castelan Celestino

Correções ortográficas realizadas:

Ana Maria dos Santos Latgé
Diana Vilas Boas Souto Aleixo
Gabriela De Grande Guerreiro

FICHA CATALOGRÁFICA

Dados Internacionais de Catalogação na Publicação (CIP)
Ana Carolina Medici Rocha – CRB 1151

P712 Plano de preservação digital / coordenação Tânia Barbosa Salles Gava. – Vitória,
ES: APEES ; PRODEST ; UFES ; FAPES, 2026.

1 recurso online (49 p.)

ISBN: 978-65-02-26336-5

1. Preservação digital. 2. Documentos arquivísticos digitais. 3. Repositórios arquivísticos confiáveis. 4. Governança arquivística. 5. Planos de preservação digital I. Gava, Tânia Barbosa Salles, coord. II. Título.

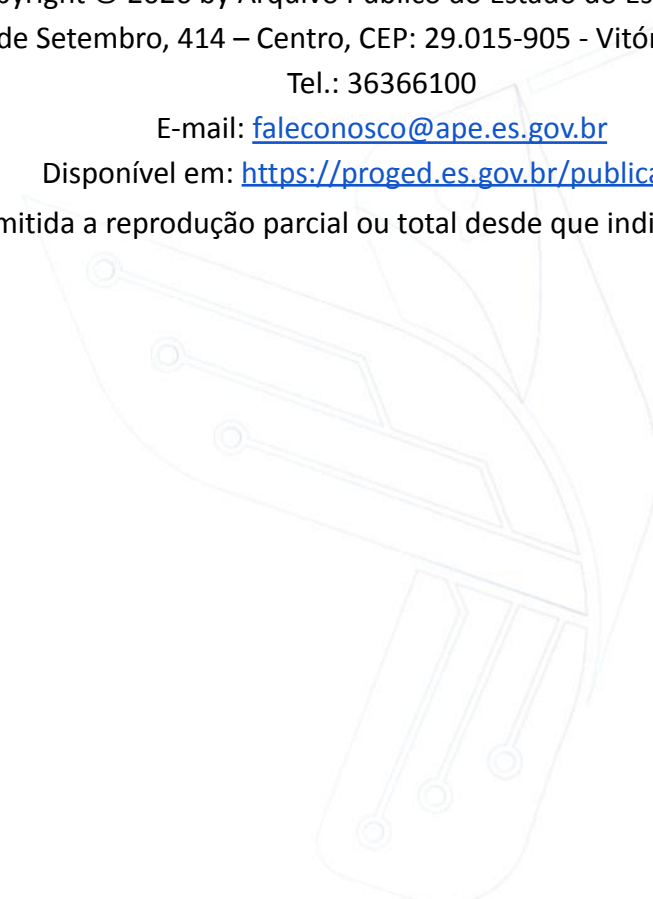
CDD – 025.84

Copyright © 2026 by Arquivo Público do Estado do Espírito Santo
Rua Sete de Setembro, 414 – Centro, CEP: 29.015-905 - Vitória / Espírito Santo
Tel.: 36366100

E-mail: faleconosco@ape.es.gov.br

Disponível em: <https://proged.es.gov.br/publicacoes>

Permitida a reprodução parcial ou total desde que indicada a fonte



SUMÁRIO

1 INTRODUÇÃO E OBJETIVOS.....	6
1.1 OBJETIVO GERAL.....	7
1.2 OBJETIVOS ESPECÍFICOS.....	8
1.3 MISSÃO E METAS.....	9
1.4 COMUNIDADE DESIGNADA.....	9
2 CENÁRIO INSTITUCIONAL E BASE NORMATIVA.....	11
2.1 ESTRUTURA ORGANIZACIONAL E DE GOVERNANÇA.....	11
2.2 ALINHAMENTO DE POLÍTICAS.....	12
3 DESCRIÇÃO E DIAGNÓSTICO DO ACERVO.....	14
3.1 IDENTIFICAÇÃO E ESCOPO.....	14
3.2 ASPECTOS TÉCNICOS.....	15
3.3 ASPECTOS LEGAIS.....	16
4 AVALIAÇÃO E GESTÃO DE RISCOS.....	18
4.1 ANÁLISE DE AMEAÇAS.....	18
4.2 MATRIZ DE RISCO.....	19
5 PLANEJAMENTO DA PRESERVAÇÃO E ESTRATÉGIAS.....	21
5.1 ESTRATÉGIAS AVALIADAS.....	21
5.2 JUSTIFICATIVA DA ESCOLHA.....	22
6 AÇÕES DE PRESERVAÇÃO E FLUXO DE TRABALHO.....	24
6.1 PROCEDIMENTOS OPERACIONAIS.....	24
6.2 MATRIZ DE RESPONSABILIDADES.....	25
6.3 PERIODICIDADE.....	27
7 INFRAESTRUTURA E SUSTENTABILIDADE FINANCEIRA.....	28
7.1 RECURSOS TECNOLÓGICOS.....	28
7.2 PREVISÃO ORÇAMENTÁRIA.....	29
8 REVISÃO E MELHORIA CONTÍNUA.....	30
8.1 GATILHOS DE REVISÃO.....	30
9 OBSERVAÇÕES ADICIONAIS.....	32
REFERÊNCIAS.....	33
APÊNDICE A - CONJUNTO MÍNIMO DE METADADOS.....	38
APÊNDICE B - MATRIZ RACI.....	48

1 INTRODUÇÃO E OBJETIVOS

O presente Plano de Preservação Digital (PPD) estabelece o conjunto de ações, responsabilidades, prazos, procedimentos e requisitos técnicos necessários à preservação de longo prazo dos documentos arquivísticos digitais permanentes sob custódia do Arquivo Público do Estado do Espírito Santo (Apees) e produzidos em sistemas informatizados.

Este documento operacionaliza, no âmbito do Apees, as diretrizes da Política de Preservação Digital institucional adotada pelo Governo do Estado do Espírito Santo, denominada PPDig@ES (Espírito Santo, 2023), transformando a visão estratégica da preservação digital em um roteiro concreto de implementação. Seu foco está orientado à definição de diretrizes, responsabilidades institucionais e cronogramas de implementação das ações voltadas à preservação da autenticidade, integridade, confiabilidade, segurança, inteligibilidade e acesso continuado aos documentos arquivísticos digitais permanentes.

Para orientar sua implementação, o documento estrutura-se em quatro eixos principais, que articulam dimensões institucionais, técnicas, operacionais e estratégicas da preservação digital: Eixo 1) Governança e estratégia; Eixo 2) Arquitetura e fluxo de trabalho; Eixo 3) Estratégias de preservação e metadados; e Eixo 4) Sustentabilidade e gestão de riscos.

Eixo 1 - Governança e Estratégia: estabelece as responsabilidades institucionais, com destaque para a atuação conjunta entre o Apees, responsável pela definição dos requisitos arquivísticos, e o Instituto de Tecnologia da Informação e Comunicação do Estado do Espírito Santo (Prodest), responsável pela infraestrutura tecnológica necessária à preservação digital.

Eixo 2 - Arquitetura e Fluxo de trabalho: define uma arquitetura técnica modular e segura, capaz de articular os sistemas produtores de documentos arquivísticos, a produção de empacotamento dos Pacotes de Informação, contendo os documentos digitais e seus metadados, e o ambiente de preservação. O fluxo de trabalho será baseado na criação, validação e gerenciamento de Pacotes de Informação de Submissão (SIP), Pacotes de Informação de Arquivamento (AIP) e Pacotes de Informação de Disseminação (DIP), conforme diretrizes do modelo *Open Archival Information System* (OAIS).

Eixo 3 - Estratégias de Preservação e Metadados: prevê a adoção de estratégias ativas, tais como migração/conversão e normalização de formatos de arquivo, conforme previsto na PPDig@ES. Essas estratégias serão apoiadas por um conjunto mínimo de metadados descritivos, de gestão e de preservação (Apêndice A), desenvolvido com base em padrões nacionais e internacionais, como o Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (e-ARQ Brasil), *Dublin Core* (DC), *Preservation Metadata: Implementation Strategies* (PREMIS) e demais referenciais aplicáveis.

Eixo 4 - Sustentabilidade e Riscos: reconhece a preservação digital como atividade contínua, dependente de monitoramento tecnológico, gestão de riscos, revisão periódica, equipe capacitada, infraestrutura adequada e planejamento financeiro de longo prazo.

1.1 OBJETIVO GERAL

Estabelecer um modelo operacional de preservação digital para o Apees, capaz de assegurar a preservação de longo prazo e o acesso contínuo aos documentos arquivísticos digitais de guarda permanente ou de longa duração, mantendo sua autenticidade, integridade, confiabilidade e inteligibilidade.

1.2 OBJETIVOS ESPECÍFICOS

São objetivos específicos deste Plano:

1. definir o escopo inicial dos documentos arquivísticos abrangidos;
2. estabelecer responsabilidades entre Apees, Prodest e entidades produtoras e custodiadoras¹;
3. definir o escopo inicial dos documentos arquivísticos abrangidos;
4. estabelecer responsabilidades entre Apees, Prodest e Entidades Custodiadoras/Produtoras;
5. orientar a preparação, submissão, ingestão, armazenamento, monitoramento e acesso aos documentos digitais;
6. estabelecer requisitos mínimos para a estrutura do Pré-SIP pacote² para a geração dos pacotes SIP, AIP e DIP;
7. detalhar como as estratégias de preservação serão aplicadas em cada cenário de preservação, de acordo com as diferentes tipologias documentais e respectivos riscos identificados;
8. estabelecer requisitos mínimos de metadados para preservação, acesso, autenticidade e gestão de direitos;
9. definir procedimentos de avaliação e gestão de riscos;
10. indicar recursos tecnológicos, humanos e financeiros necessários à execução do Plano;
11. estabelecer periodicidade de rotinas e critérios de revisão;
12. permitir a melhoria contínua dos procedimentos de preservação digital.

¹ No âmbito deste Plano de Preservação, consideram-se entidades produtoras e entidades custodiadoras os órgãos e entidades do Poder Executivo Estadual, bem como entidades privadas e pessoas físicas responsáveis pela produção, recebimento, acumulação, guarda, manutenção ou preservação de documentos arquivísticos digitais. Entende-se por entidade produtora aquela responsável pela produção, recebimento ou acumulação dos documentos no exercício de suas atividades; e por entidade custodiadora aquela responsável pela guarda, preservação e manutenção desses documentos ao longo do tempo.

² Produto informacional resultante de um evento de preparação para preservação (Pre-Ingest Event), no qual um ou mais objetos digitais são organizados, validados e contextualizados por meio de um conjunto mínimo de metadados.

1.3 MISSÃO E METAS

A missão deste Plano é garantir que o patrimônio arquivístico digital produzido, recebido ou recolhido no âmbito da Administração Pública Estadual permaneça autêntico, íntegro, preservado e acessível pelo tempo que for necessário, contribuindo para a continuidade administrativa, a transparência pública, a garantia de direitos e a preservação da memória governamental e cultural capixaba.

O escopo deste Plano compreende:

1. documentos arquivísticos digitais oriundos de sistemas informatizados oficiais do Poder Executivo Estadual;
2. documentos arquivísticos digitais oriundos de sistemas legados, quando avaliados como de valor permanente.

1.4 COMUNIDADE DESIGNADA

No âmbito deste Plano, a comunidade designada é constituída pelos grupos de usuários e sistemas que orientam a definição dos requisitos de acesso, descrição, preservação e inteligibilidade dos documentos digitais.

A comunidade designada primária é composta por:

1. **Administração Pública Estadual:** servidores, gestores, unidades administrativas, órgãos de controle e demais agentes públicos que necessitam de documentos preservados para fins administrativos, jurídicos, probatórios e de continuidade institucional;
2. **pesquisadores acadêmicos e estudantes:** historiadores, arquivistas, cientistas sociais, cientistas da informação, juristas, cientistas de dados e demais pesquisadores interessados no patrimônio documental capixaba;

3. **cidadãos:** indivíduos que exercem o direito de acesso à informação, buscam comprovação de direitos, realizam pesquisa genealógica, histórica, cultural ou administrativa.

A comunidade designada secundária compreende os usuários não humanos que interagem com os documentos arquivísticos digitais e seus metadados, como robôs de indexação, sistemas de busca, agentes de *software*, aplicações de interoperabilidade e algoritmos de análise de dados.

Os requisitos gerais de acesso dessa comunidade incluem localização eficiente dos documentos, compreensão do contexto de produção, acesso a metadados confiáveis, geração de cópias de acesso, controle de restrições legais, proteção de dados pessoais e possibilidade de uso dos documentos por pessoas e sistemas autorizados.



2 CENÁRIO INSTITUCIONAL E BASE NORMATIVA

Esta seção contextualiza a unidade responsável pela execução do Plano, seu mandato institucional, sua relação com os demais atores envolvidos e o amparo normativo das ações previstas.

2.1 ESTRUTURA ORGANIZACIONAL E DE GOVERNANÇA

O Apees é a instituição arquivística responsável pela custódia, preservação, tratamento, descrição, acesso e difusão dos documentos arquivísticos sob sua responsabilidade.

No contexto deste Plano, o Apees atua como responsável pela definição dos requisitos arquivísticos aplicáveis à preservação digital. Compete ao Apees orientar critérios de recebimento, avaliação, metadados, autenticidade, descrição, acesso, restrições legais e preservação de longo prazo dos documentos arquivísticos digitais.

No âmbito deste Plano, compete ao Prodest prover, manter e monitorar a infraestrutura tecnológica necessária à execução do Plano, contemplando os serviços de armazenamento, segurança, disponibilidade, suporte técnico, monitoramento, backup e recuperação.

As Entidades Custodiadoras/Produtoras serão responsáveis por preparar os documentos digitais a serem submetidos ao Apees, fornecer metadados de origem, indicar restrições de acesso, informar direitos autorais ou condições de uso, respeitar os requisitos de submissão e colaborar na validação dos conjuntos documentais.

A governança do Plano será organizada em três níveis:

1. **Nível Estratégico:** responsável pela aprovação, priorização, articulação institucional e garantia de recursos;
2. **Nível Tático:** responsável pelo acompanhamento da implementação, análise de riscos, definição de critérios técnicos e revisão dos instrumentos vinculados;
3. **Nível Operacional:** responsável pela execução dos procedimentos de preparação, submissão, ingestão, validação, armazenamento, monitoramento e acesso.

As responsabilidades específicas deverão ser detalhadas na Matriz RACI (Apêndice B), vinculada a este Plano como instrumento técnico de gestão.

2.2 ALINHAMENTO DE POLÍTICAS

Este Plano está alinhado à PPDig@ES e aos demais instrumentos institucionais relacionados à gestão de documentos, ao acesso à informação, à segurança da informação e à proteção de dados pessoais.

O Plano deve ser compreendido como instrumento de execução da política, e não como substituto dela. Assim, suas seções concentram-se nas ações necessárias para a preservação dos documentos digitais, incluindo responsáveis, fluxos, prazos, instrumentos de controle e recursos necessários.

As políticas e normas relacionadas incluem:

1. PPDig@ES (Espírito Santo, 2023b);
2. Programa de Gestão Documental do Governo do Estado do Espírito Santo (Proged) (Espírito Santo, 2018a);
3. normas relacionadas ao E-Docs e aos sistemas produtores de documentos digitais (Espírito Santo, 2018a, 2023a, 2023b, 2023c, 2026):

4. legislação arquivística nacional (Conselho Nacional de Arquivos, 2026);
5. legislação arquivística estadual (Espírito Santo, 2012, 2018a, 2018b, 2023a, 2023b, 2023c, 2024a, 2025, 2026);
6. Lei de Acesso à Informação (Brasil, 2011);
7. Lei Geral de Proteção de Dados Pessoais (Brasil, 2018);
8. normas de segurança da informação aplicáveis ao Governo do Estado (Espírito Santo, 2011a, 2011b, 2019, 2021, 2022, 2023, 2024; Brasil, 2018);
9. e-ARQ Brasil: modelo de requisitos para sistemas informatizados de gestão arquivística de documentos (Conselho Nacional de Arquivos, 2022);
10. diretrizes do CONARQ para Repositórios Arquivísticos Digitais Confiáveis;
11. Modelo OAIS;
12. padrões nacionais e internacionais de metadados, preservação digital e auditoria de repositórios (Conselho Nacional De Arquivos, 2006, 2015, 2022, 2023; Dublin Core Metadata Initiative, 2012; International Council On Archives, 2000, 2023; International Organization For Standardization, 2016, 2017, 2019, 2020, 2021, 2025; Library Of Congress, 2015, 2026).

As políticas de acesso deverão operacionalizar o equilíbrio entre a transparência pública e a proteção de dados pessoais, permitindo a geração de pacotes DIP distintos, com ou sem anonimização, conforme o perfil do solicitante e o fundamento legal aplicável.

3 DESCRIÇÃO E DIAGNÓSTICO DO ACERVO

Esta seção apresenta o retrato técnico, arquivístico e legal do material digital a ser preservado. O diagnóstico do acervo é condição necessária para a definição das estratégias de preservação, da infraestrutura, dos custos, dos riscos e da periodicidade das ações de cada cenário de preservação.

3.1 IDENTIFICAÇÃO E ESCOPO

O escopo deste PPD compreende documentos arquivísticos digitais produzidos no âmbito da Administração Pública Estadual, com ênfase àqueles cuja avaliação arquivística indique como de guarda permanente ou necessidade de preservação por longo prazo.

O escopo inicial deverá contemplar:

1. documentos textuais digitais;
2. processos administrativos digitais;
3. documentos digitalizados com valor permanente;
4. fotografias digitais;
5. áudios;
6. vídeos;
7. documentos cartográficos digitais;
8. bases de dados;
9. mensagens eletrônicas com valor arquivístico;
10. documentos oriundos de sistemas legados.

Para cada conjunto documental, o diagnóstico poderá conter:

1. Entidade custodiadora/Produtora;
2. unidade responsável;

3. sistema de origem;
4. função ou atividade relacionada;
5. série, classe ou agrupamento documental;
6. temporalidade e destinação;
7. volume total em GB ou TB;
8. previsão de crescimento anual;
9. formatos de arquivo existentes;
10. metadados disponíveis;
11. restrições de acesso;
12. existência de dados pessoais ou sensíveis;
13. direitos autorais ou condições de uso;
14. estado de organização;
15. riscos técnicos identificados.

Quando os dados de volume, crescimento anual, formatos predominantes ou sistemas de origem ainda não estiverem consolidados, o diagnóstico deverá registrá-los como informações a levantar, com indicação de responsável e prazo.

3.2 ASPECTOS TÉCNICOS

Os aspectos técnicos do acervo serão avaliados a partir dos formatos de arquivo, dos padrões de metadados, da nomenclatura, dos identificadores e das dependências tecnológicas.

No PPD, recomenda-se indicar:

1. formatos aceitos para submissão;
2. formatos preferenciais de preservação;
3. formatos recomendados para acesso;
4. formatos em risco de obsolescência;

5. formatos que exigem normalização;
6. formatos que exigem migração;
7. ferramentas de identificação e validação.

O conjunto mínimo de metadados deverá contemplar metadados descritivos, técnicos, administrativos, estruturais e de preservação (Apêndice A), onde foram considerados padrões como Dublin Core, PREMIS, e-ARQ Brasil e outros referenciais adotados pelo Apees.

A nomenclatura dos arquivos deverá ser padronizada de modo a evitar ambiguidades, perda de contexto, duplicidades ou descaracterização dos documentos. Sempre que possível, deverá ser preservado o identificador original do sistema produtor, associado a metadados arquivísticos que garantam proveniência, relação orgânica e rastreabilidade.

Os padrões detalhados de formatos, metadados e nomenclatura deverão compor instrumentos técnicos vinculados ao Plano.

3.3 ASPECTOS LEGAIS

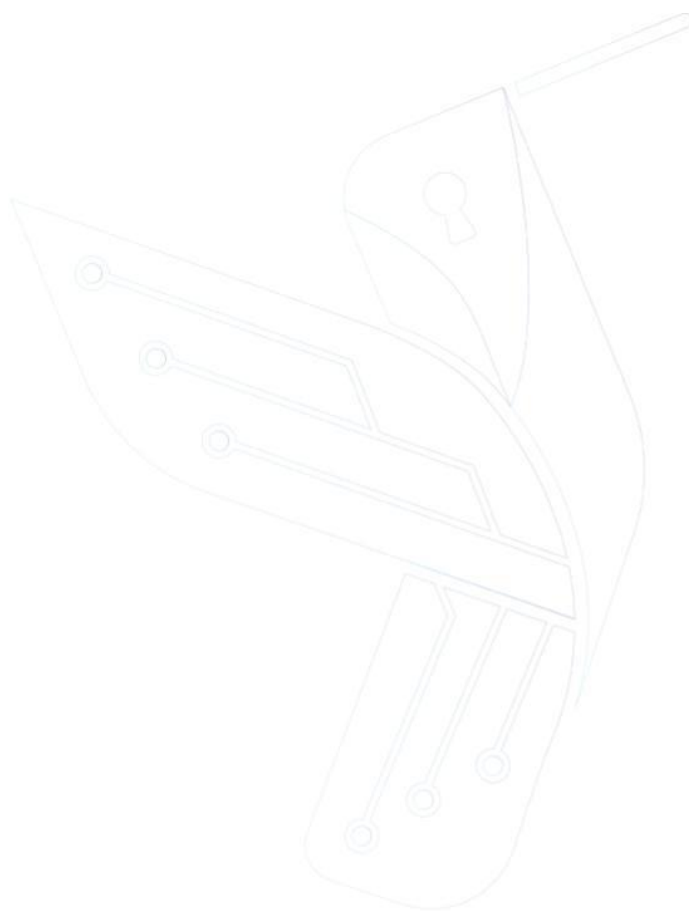
O diagnóstico legal deverá identificar direitos, restrições e condições de uso dos documentos digitais preservados.

No PPD, recomenda-se registrar, quando aplicável:

1. titularidade dos documentos;
2. direitos autorais;
3. termos de doação, cessão, transferência ou recolhimento;
4. existência de dados pessoais;
5. existência de dados pessoais sensíveis;
6. sigilo legal;
7. prazos de restrição;

8. fundamento legal da restrição;
9. possibilidade de acesso parcial;
10. necessidade de anonimização;
11. condições de reprodução e difusão.

A identificação desses elementos é necessária para orientar a geração dos pacotes DIP, a disponibilização pública, o atendimento a solicitações de acesso e a proteção de dados e privacidade.



4 AVALIAÇÃO E GESTÃO DE RISCOS

A gestão de riscos é o componente central deste Plano. Sua finalidade é identificar, avaliar, priorizar, tratar e monitorar ameaças que possam comprometer a autenticidade, a integridade, a disponibilidade, a segurança, a inteligibilidade ou a sustentabilidade do acervo digital.

4.1 ANÁLISE DE AMEAÇAS

A avaliação de riscos deverá considerar ameaças tecnológicas, organizacionais, processuais, legais, ambientais e de segurança.

Os riscos tecnológicos incluem obsolescência de *hardware* e *software*, obsolescência de formatos, corrupção de *bits*, falhas de armazenamento, perda de metadados, indisponibilidade de sistemas, dependência de soluções proprietárias e falhas em processos de migração.

Os riscos organizacionais incluem ausência de equipe dedicada, indefinição de responsabilidades, descontinuidade orçamentária, baixa capacitação, mudanças administrativas, perda de conhecimento institucional e falta de articulação entre Apees, Prodest e Entidades Custodiadoras/Produtoras.

Os riscos processuais incluem pacotes SIP incompletos, metadados insuficientes, ausência de *checksums*³, falhas na validação de formatos, ausência de documentação das intervenções, problemas na cadeia de custódia e inconsistências entre objeto digital, metadados e contexto arquivístico.

³ Código de verificação gerado a partir de um arquivo ou pacote digital para confirmar se ele permaneceu íntegro, isto é, se não foi alterado, corrompido ou perdido parcialmente durante transferência, armazenamento ou preservação.

Os riscos legais incluem divulgação indevida de dados pessoais, ausência de registro de direitos autorais, ausência de termo de cessão ou recolhimento, erro na classificação de acesso, descumprimento de prazos de sigilo e falhas na anonimização.

Os riscos ambientais e de infraestrutura incluem incêndio, inundação, falhas elétricas, indisponibilidade de datacenter, perda de conectividade, falha de climatização, desastres naturais e indisponibilidade prolongada dos serviços de armazenamento.

4.2 MATRIZ DE RISCO

A Matriz de Riscos será o instrumento de registro, classificação e acompanhamento das ameaças identificadas e deverá conter os seguintes elementos:

1. Id do risco;
2. categoria;
3. descrição;
4. causas potenciais;
5. impacto potencial;
6. probabilidade de ocorrência;
7. nível de risco;
8. ação de mitigação ou controle;
9. responsável pela ação;
10. prazo de tratamento;
11. situação de acompanhamento.

As categorias sugeridas são:

1. Tecnológico — TEC;
2. Organizacional — ORG;

3. Processual — PRO;
4. Legal — LEG;
5. Segurança — SEG;
6. Infraestrutura e ambiente — INF.

O impacto será classificado como baixo, médio, alto ou crítico. A probabilidade será classificada como baixa, média ou alta. O nível de risco será definido pela combinação entre impacto e probabilidade, permitindo priorizar as ações de mitigação.

Riscos críticos deverão ter tratamento imediato. Riscos altos deverão ter plano de ação de curto prazo. Riscos médios deverão ser acompanhados e tratados conforme prioridade institucional. Riscos baixos deverão permanecer em monitoramento.

A Matriz de Riscos deverá ser revisada periodicamente e sempre que houver alteração relevante no acervo, nos sistemas, na infraestrutura, nas políticas institucionais ou na legislação aplicável.

5 PLANEJAMENTO DA PRESERVAÇÃO E ESTRATÉGIAS

Esta seção define as estratégias avaliadas e as ações selecionadas para garantir a longevidade, a autenticidade, a integridade e o acesso continuado aos documentos digitais.

5.1 ESTRATÉGIAS AVALIADAS

As estratégias avaliadas por este Plano são:

1. normalização;
2. migração/conversão;
3. refrescamento;
4. emulação;
5. encapsulamento.

A **normalização** tem como objetivo simplificar o processo de preservação digital por meio da redução da diversidade de formatos aceitos na plataforma de preservação. Os formatos aceitos em cada cenário de preservação devem ser apresentados de forma explícita em cada Plano de preservação digital e devem estar de acordo com a política institucional de preservação.

A **conversão** de formatos será aplicada quando o objeto digital apresentar risco de obsolescência, dependência tecnológica, não conformidade com formatos institucionais ou limitações de acesso e interoperabilidade, resultando na produção de uma nova representação digital. A **conversão de formatos** corresponde a um evento técnico no qual um objeto digital é transformado de um formato de codificação para outro, mantendo, na medida do possível, seu conteúdo intelectual, sua estrutura lógica e suas características essenciais de representação. Seu objetivo principal é promover **padronização, interoperabilidade, acesso ou adequação a requisitos**

técnicos específicos, sem necessariamente estar associada a um risco de obsolescência tecnológica.

A **migração** corresponde a uma estratégia de preservação digital na qual um objeto digital, ou conjunto de objetos, é transferido de um ambiente tecnológico para outro com o objetivo de mitigar riscos de obsolescência e garantir sua continuidade de acesso, interpretação e uso ao longo do tempo.

Refrescamento é a estratégia de preservação digital que consiste na transferência periódica dos objetos digitais para novos suportes ou ambientes de armazenamento, sem alteração de seu formato ou conteúdo, com o objetivo de reduzir riscos associados à degradação física, falhas tecnológicas ou obsolescência dos meios de armazenamento.

A **emulação** é uma estratégia baseada na utilização de um software, denominado **emulador**, capaz de reproduzir o comportamento de outro software que se tornou obsoleto. Essa estratégia será considerada apenas quando a compreensão do documento depender, no futuro, da reprodução do ambiente tecnológico específico no qual ele foi criado.

Encapsulamento será adotado na constituição dos AIPs, reunindo objeto digital, metadados, registros de eventos, informações de contexto, direitos, restrições e demais elementos necessários à preservação.

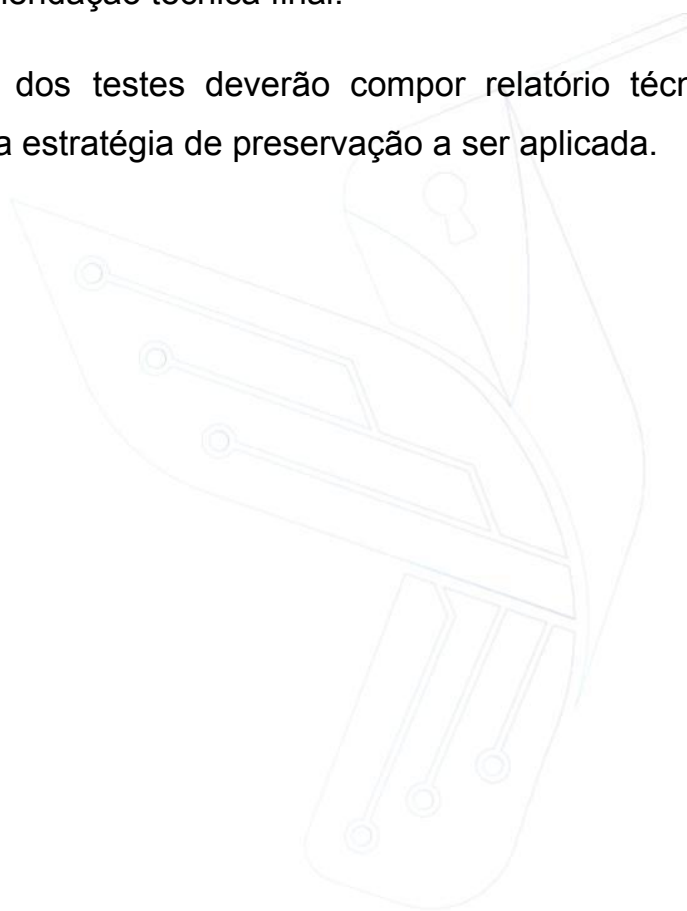
5.2 JUSTIFICATIVA DA ESCOLHA

As estratégias de preservação devem ser adotadas de forma combinada, considerando a diversidade dos acervos digitais, que podem apresentar diferentes características documentais, formatos, sistemas de origem, requisitos legais, necessidades de acesso e riscos tecnológicos.

Antes da adoção definitiva de uma estratégia para determinado acervo arquivístico, deverão ser realizados testes com amostras representativas do acervo. Esses testes deverão avaliar:

1. formatos encontrados;
2. ferramentas utilizadas;
3. sucesso na identificação dos formatos;
4. metadados extraídos;
5. qualidade da normalização ou migração;
6. alterações em propriedades significativas;
7. tempo de processamento;
8. necessidade de intervenção manual;
9. capacidade de geração de DIP;
10. recomendação técnica final.

Os resultados dos testes deverão compor relatório técnico e subsidiar a decisão sobre a estratégia de preservação a ser aplicada.



6 AÇÕES DE PRESERVAÇÃO E FLUXO DE TRABALHO

Esta seção detalha os procedimentos operacionais, as responsabilidades e a periodicidade das ações de preservação.

6.1 PROCEDIMENTOS OPERACIONAIS

O fluxo de trabalho adotará o modelo OAIS, com uso de pacotes SIP, AIP e DIP.

O Pré-SIP será o pacote preparado pelo sistema produtor ou custodiante para submissão ao ambiente de preservação. O SIP será o pacote intermediário de submissão, formado a partir do Pré-SIP após as etapas de recepção, conferência, validação, complementação de metadados e organização dos objetos digitais, constituindo a base para geração do AIP. O AIP será o pacote arquivístico preservado pelo ambiente de preservação (Repositórios Arquivísticos Digitais Confiáveis - RDC-Arq). O DIP será o pacote gerado para acesso, consulta, difusão ou atendimento a solicitações (se aplicável).

O fluxo operacional será composto pelas seguintes etapas:

- 1. Preparação do conjunto documental** - O sistema produtor, com orientação do Apees, identificará os documentos a serem submetidos, verificará sua destinação, reunirá os objetos digitais, organizará os metadados disponíveis e indicará restrições de acesso, direitos e condições de uso.
- 2. Comunicação oficial ao Apees** - A Entidade Custodiadora/Produtora comunicará formalmente ao Apees a intenção de recolher documentos digitais. Essa comunicação iniciará a definição das condições de recebimento, preservação e acesso.

3. **Formação do Pré-SIP** - O Pré-SIP deverá conter os objetos digitais e conjunto mínimo de metadados específico de cada cenário de preservação.
4. **Validação do Pré-SIP** - Dependendo do cenário de preservação, caberá ao Apees avaliar aspectos relacionados à qualidade, integridade, segurança, conformidade técnica, metadados e restrições de acesso dos objetos digitais.
5. **Ingestão** - Após a validação, o Pré-SIP será processado no ambiente de preservação. A ingestão inclui identificação de formatos, gestão de metadados, geração e/ou conferência de *checksums*, normalização quando aplicável e registro dos eventos de preservação.
6. **Geração do AIP** - O AIP reunirá o objeto digital original, versões normalizadas quando geradas, metadados descritivos, de gestão e de preservação, informações de direitos e restrições de acesso.
7. **Armazenamento e gerenciamento do AIP** - O AIP será armazenado em ambiente seguro, controle de acesso, logs, verificação periódica de integridade e mecanismos de recuperação.
8. **Geração do DIP** - O DIP será produzido para acesso, consulta, difusão ou interoperabilidade. Poderá conter cópia de acesso, metadados públicos, versões anonimizadas ou outros elementos necessários ao perfil do solicitante.

6.2 MATRIZ DE RESPONSABILIDADES

A Matriz RACI detalha as responsabilidades específicas dos atores envolvidos. No escopo deste Plano, ficam definidos os seguintes papéis gerais:

Apees

1. definir requisitos arquivísticos;
2. orientar a preparação de pré-SIP;
3. validar metadados arquivísticos;
4. avaliar autenticidade na entrada (quando aplicável);
5. definir restrições de acesso;
6. aprovar estratégias de preservação;
7. acompanhar geração de pacotes AIP e DIP;
8. manter documentação arquivística do processo.

Prodest

1. prover e manter infraestrutura tecnológica;
2. garantir armazenamento;
3. executar rotinas técnicas de segurança;
4. apoiar verificação de integridade;
5. manter disponibilidade dos sistemas;
6. apoiar *backup* e recuperação;
7. registrar incidentes técnicos.

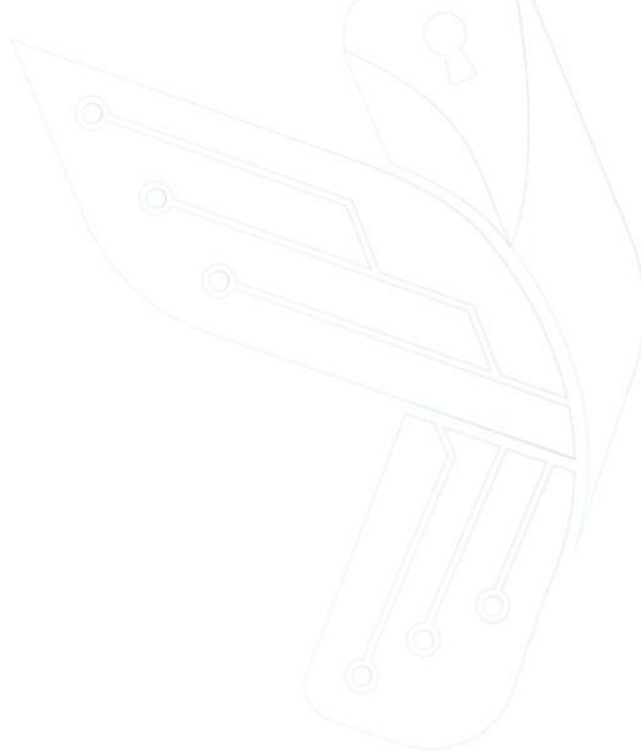
Entidades Custodiadoras/Produtoras

1. selecionar os documentos que comporão os acervos arquivísticos a serem submetidos;
2. garantir organização mínima dos acervos;
3. fornecer metadados de origem (se aplicável);
4. informar restrições de acesso;
5. indicar direitos, sigilos e dados sensíveis;
6. cumprir formatos e requisitos de submissão.

6.3 PERIODICIDADE

A periodicidade das rotinas de integração poderá variar de acordo com o caso, o cenário de preservação digital, as características dos acervos digitais e as condições técnicas e institucionais envolvidas.

São exemplos de rotinas de preservação: verificar metadados, registrar ações realizadas, controlar acessos, acompanhar logs, monitorar sistemas e armazenamento, realizar backups quando necessário, verificar alertas de segurança, conferir a integridade dos arquivos, acompanhar falhas e pendências, elaborar relatórios, avaliar riscos, testar restaurações, revisar formatos em risco, atualizar o diagnóstico do acervo, revisar a infraestrutura, avaliar custos e atualizar o plano de ações.



7 INFRAESTRUTURA E SUSTENTABILIDADE FINANCEIRA

Esta seção aborda aspectos relacionados aos recursos tecnológicos, humanos e financeiros necessários à execução do Plano.

7.1 RECURSOS TECNOLÓGICOS

A infraestrutura tecnológica deverá ser suficiente para receber, validar, preservar, monitorar e disponibilizar documentos digitais de forma segura e sustentável.

A infraestrutura mínima deverá contemplar:

1. ambiente controlado para recebimento de pacotes Pré-SIP;
2. área de quarentena para verificação de vírus e validação inicial;
3. ferramenta de identificação de formatos;
4. ferramenta de geração e verificação de *checksums*;
5. plataforma de preservação digital compatível com o modelo OAIS;
6. armazenamento seguro para pacotes AIP;
7. *backup* e recuperação;
8. controle de acesso;
9. logs de auditoria;
10. ferramenta ou ambiente de acesso, difusão ou plataforma de transparência ativa.

O RDC-Arq poderá utilizar sistemas especializados, como Archivematica ou solução equivalente, desde que compatíveis com o modelo OAIS.

A arquitetura técnica deverá seguir os padrões da arquitetura computacional, articulando sistemas produtores, aplicação de empacotamento, ambiente de

preservação, armazenamento seguro e ambiente de acesso, permitindo rastreabilidade, validação, segurança, interoperabilidade e auditoria.

7.2 PREVISÃO ORÇAMENTÁRIA

A sustentabilidade financeira deverá contemplar custos de implantação, operação, manutenção, capacitação e atualização tecnológica.

A previsão orçamentária deverá considerar:

1. equipe técnica e arquivística;
2. capacitação continuada;
3. infraestrutura de armazenamento;
4. servidores ou serviços equivalentes;
5. manutenção de sistemas;
6. atualização tecnológica;
7. ferramentas de segurança;
8. *backup* e recuperação;
9. migração de formatos;
10. documentação técnica;
11. auditorias ou autoavaliações;
12. expansão de capacidade conforme crescimento do acervo.

A estimativa orçamentária poderá considerar aspectos relacionados ao acervo, à infraestrutura tecnológica, aos processos de preservação digital, aos recursos humanos, à capacitação das equipes e à manutenção das condições técnicas necessárias à execução do Plano.

Enquanto esses dados não estiverem consolidados, a previsão orçamentária deverá ser tratada como estimativa preliminar, a ser atualizada após a conclusão do diagnóstico do acervo.

8 REVISÃO E MELHORIA CONTÍNUA

O PPD deverá ser revisto periodicamente, pois as condições técnicas, institucionais, normativas e documentais da preservação digital se alteram ao longo do tempo.

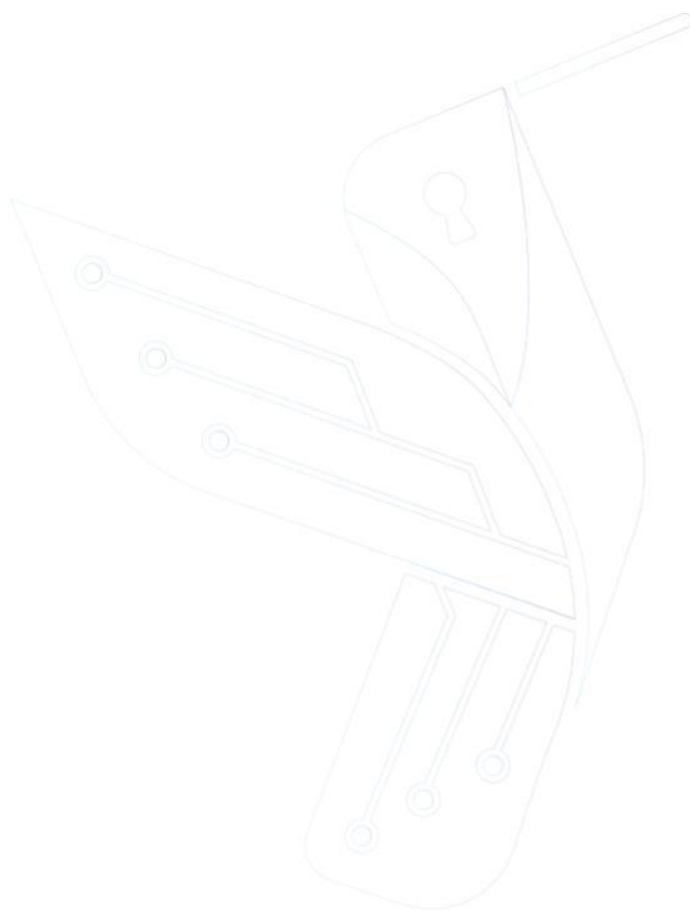
Sugere-se uma revisão ordinária a cada dois anos. Revisões extraordinárias poderão ocorrer sempre que houver alteração significativa no escopo, nos procedimentos, nos sistemas, na infraestrutura, nas responsabilidades, nos riscos ou na legislação aplicável.

8.1 GATILHOS DE REVISÃO

São gatilhos de revisão:

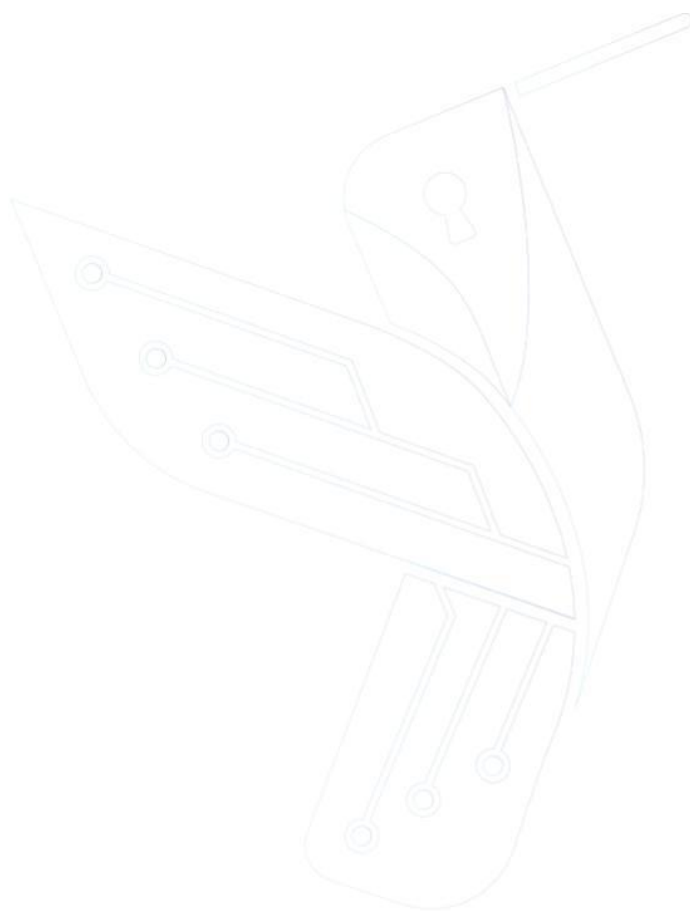
1. alteração da Política de Preservação Digital institucional;
2. alteração de normas estaduais de gestão documental, acesso à informação, segurança ou proteção de dados;
3. atualização do e-ARQ Brasil, das diretrizes de RDC-Arq ou de normas técnicas aplicáveis;
4. implantação, substituição ou alteração relevante de sistema produtor;
5. inclusão de novas tipologias documentais;
6. identificação de novos formatos de arquivo;
7. crescimento do acervo acima do previsto;
8. falha relevante em ingestão, armazenamento, verificação de integridade ou geração de DIP;
9. incidente de segurança;
10. necessidade de migração tecnológica;
11. mudança na infraestrutura do Prodest ou do ambiente de preservação;
12. alteração nas demandas da comunidade designada.

Toda revisão deverá gerar registro formal contendo data, responsáveis, itens alterados, justificativa, impacto sobre procedimentos, responsabilidades, custos e prazos, bem como indicação da nova versão do Plano ou de seus instrumentos técnicos vinculados.



9 OBSERVAÇÕES ADICIONAIS

Esta seção poderá conter observações específicas do Plano de Preservação Digital, especialmente aquelas que não foram contempladas nas seções anteriores. Também poderão ser incluídos instrumentos técnicos complementares necessários à sua operacionalização, acompanhamento e atualização periódica.



REFERÊNCIAS

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais — LGPD. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 18 maio 2026.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). **NOBRADE: Norma Brasileira de Descrição Arquivística.** Rio de Janeiro: Arquivo Nacional, 2006.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). **Diretrizes para a implementação de repositórios arquivísticos digitais confiáveis — RDC-Arq.** Rio de Janeiro: Arquivo Nacional, 2015.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). **Coletânea da legislação arquivística e correlata.** Brasília, DF: CONARQ, 2020. Disponível em: <https://www.gov.br/conarq/pt-br/legislacao-arquivistica/coletanea-da-legislacao-arquivistica-e-correlata>. Acesso em: 18 maio 2026.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). **e-ARQ Brasil: modelo de requisitos para sistemas informatizados de gestão arquivística de documentos.** 2. versão. Rio de Janeiro: Arquivo Nacional, 2022. Disponível em: <https://www.gov.br/conarq/pt-br/centrais-de-conteudo/publicacoes/EARQV203MAI2022.pdf>. Acesso em: 18 maio 2026.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). **Diretrizes para certificação de repositórios arquivísticos digitais confiáveis — RDC-Arq.** Rio de Janeiro: Arquivo Nacional, 2023.

DUBLIN CORE METADATA INITIATIVE. **Dublin Core Metadata Element Set, Version 1.1.** [S. l.]: DCMI, 2012.

ESPÍRITO SANTO (Estado). **Decreto n. 2.884-R, de 21 de outubro de 2011.** Institui a Política Estadual de Segurança da Informação no âmbito do Poder Executivo do Estado — PESI; cria o Comitê Estadual de Segurança da Informação do Estado do Espírito Santo. Vitória: Governo do Estado do Espírito Santo, 2011a. Disponível em: https://www.informanet.com.br/Prodinfor/boletim/2011/es/decreto_2884_44_2011.html. Acesso em: 18 maio 2026.

ESPÍRITO SANTO (Estado). **Portaria n. 2.068-R, de 2011.** Regulamenta a Política Estadual de Segurança da Informação — PESI. Vitória: Governo do Estado do Espírito Santo, 2011b. Disponível em: <https://prodest.es.gov.br/privacidade-legislacao>. Acesso em: 18 maio 2026.

ESPÍRITO SANTO (Estado). **Decreto n. 3.130-R, de 19 de outubro de 2012.** Institui a Política Estadual de Tecnologia da Informação e Comunicação — PETI, no âmbito do Poder Executivo do Estado do Espírito Santo. Vitória: Governo do Estado do Espírito Santo, 2012. Disponível em:

<https://leisestaduais.com.br/es/decreto-n-3130-2012-espirito-santo-institui-a-politica-estadual-de-tecnologia-da-informacao-e-comunicacao-peti-no-ambito-do-poder-executivo-do-estado-do-espirito-santo>. Acesso em: 18 maio 2026.

ESPÍRITO SANTO (Estado). **Decreto n. 4.343-R, de 20 de dezembro de 2018.** Atualiza as normas do Programa de Gestão Documental — PROGED, instituído pelo Decreto n. 1.552-R, de 10 de outubro de 2005. Vitória: Governo do Estado do Espírito Santo, 2018. Disponível em:

<https://ape.es.gov.br/GrupodeArquivos/decreto-no-4343-r-de-2018>. Acesso em: 18 maio 2026.

ESPÍRITO SANTO (Estado). **Decreto n. 4.505-R, de 20 de setembro de 2019.** Institui a nova Política Estadual de Tecnologia da Informação e Comunicação — PETI, no âmbito do Poder Executivo do Estado do Espírito Santo. Vitória: Governo do Estado do Espírito Santo, 2019. Disponível em:

https://prodest.es.gov.br/media/Legislacao/Peti_2019.pdf. Acesso em: 18 maio 2026.

ESPÍRITO SANTO (Estado). **Decreto n. 4.922-R, de 9 de julho de 2021.** Institui a Política Estadual de Proteção de Dados Pessoais e da Privacidade do Poder Executivo Estadual em consonância com a Lei Federal n. 13.709, de 14 de agosto de 2018. Vitória: Governo do Estado do Espírito Santo, 2021. Disponível em:

<https://seq.es.gov.br/pepdp>. Acesso em: 18 maio 2026.

ESPÍRITO SANTO (Estado). **Decreto n. 5.198-R, de 2022.** Altera o Decreto n. 4.922-R, de 9 de julho de 2021, que instituiu a Política Estadual de Proteção de Dados Pessoais e da Privacidade do Poder Executivo Estadual. Vitória: Governo do Estado do Espírito Santo, 2022a. Disponível em:

<https://prodest.es.gov.br/privacidade-legislacao>. Acesso em: 18 maio 2026.

ESPÍRITO SANTO (Estado). Comitê Encarregado Central. **Resolução CEC n. 02/2022.** Disciplina os procedimentos para casos de incidente de segurança da informação envolvendo dados pessoais no âmbito da Administração Pública Direta e Indireta do Estado do Espírito Santo. Vitória: Comitê Encarregado Central, 2022b. Disponível em:

<https://sedu.es.gov.br/Media/sedu/pdf%20e%20Arquivos/Resolu%C3%A7%C3%A3o%20CEC%20N%C2%BA%202022-02%20-%20Disciplina%20os%20procedimentos%20para%20casos%20de%20incidente%20de%20seguran%C3%A7a.pdf>. Acesso em: 18 maio 2026.

ESPÍRITO SANTO (Estado). **Decreto n. 5.491-R, de 1º de setembro de 2023.** Regulamenta a técnica e os requisitos a serem utilizados pelos órgãos e entidades da administração pública direta e indireta do Estado do Espírito Santo para a digitalização de documentos públicos ou privados. Vitória: Governo do Estado do Espírito Santo, 2023a. Disponível em: <https://leisestaduais.com.br/es/decreto-n-6024-2025-espirito-santo-altera-o-decreto-n-5491-r-de-1-de-setembro-de-2023-que-regulamenta-a-tecnica-e-os-requisitos-a-ser-em-utilizados-pelos-orgaos-e-entidades-da-administracao-publica-direta-e-indireta-d-o-estado-do-espirito-santo-para-a-digitalizacao-de-documentos-publicos-ou-privados>. Acesso em: 18 maio 2026.

ESPÍRITO SANTO (Estado). **Lei Complementar n. 1.064, de 19 de dezembro de 2023.** Reorganiza a estrutura organizacional básica do Instituto de Tecnologia da Informação e Comunicação do Estado do Espírito Santo — PRODEST. Vitória: Governo do Estado do Espírito Santo, 2023b. Disponível em: <https://www3.al.es.gov.br/Arquivo/Documents/legislacao/html/LEC10642023.html>. Acesso em: 18 maio 2026.

ESPÍRITO SANTO (Estado). **Política de Preservação Digital — PPDig@ES.** Vitória: Governo do Estado do Espírito Santo, 2023c. Disponível em: <https://proged.es.gov.br/Media/Proged/Publicacoes%20Tecnicas/Pol%C3%ADtica-Pr eserva%C3%A7%C3%A3o%20Digital.pdf>. Acesso em: 18 maio 2026.

ESPÍRITO SANTO (Estado). Instituto de Tecnologia da Informação e Comunicação do Estado do Espírito Santo. **Política de Segurança da Informação.** Vitória: PRODEST, 2023d. Disponível em: <https://prodest.es.gov.br/Media/seguranca-da-informacao/PSI/Pol%C3%ADtica%20de%20Seguran%C3%A7a%20da%20Informa%C3%A7%C3%A3o%20da%20Prodest.pdf>. Acesso em: 18 maio 2026.

ESPÍRITO SANTO (Estado). **Decreto n. 5.778-R, de 25 de julho de 2024.** Regulamenta o Governo Digital Estadual, no âmbito da administração pública estadual direta, autarquias, fundações, empresas públicas e empresas de sociedade de economia mista do Estado do Espírito Santo. Vitória: Governo do Estado do Espírito Santo, 2024a. Disponível em: <https://sedu.es.gov.br/Media/sedu/pdf%20e%20Arquivos/5778-r-Regulamenta%20G overno%20Digital%20Estadual%20-%20DOES%20de%2025.07.2024.pdf>. Acesso em: 18 maio 2026.

ESPÍRITO SANTO (Estado). **Lei Complementar n. 1.076, de 2 de abril de 2024.** Dispõe sobre a transformação do Arquivo Público do Estado do Espírito Santo — APEES em autarquia e dá outras providências. Vitória: Governo do Estado do Espírito Santo, 2024b. Disponível em: <https://ape.es.gov.br/GrupodeArquivos/lei-complementar-no-1-076>. Acesso em: 18 maio 2026.

ESPÍRITO SANTO (Estado). Arquivo Público do Estado do Espírito Santo. **Norma de Procedimento n. 002: procedimentos para consulta ao acervo.** Vitória: APEES, 2025. Disponível em: <https://ape.es.gov.br/ueci-normas>. Acesso em: 18 maio 2026.

ESPÍRITO SANTO (Estado). Instituto de Tecnologia da Informação e Comunicação do Estado do Espírito Santo. **Política de Privacidade do PRODEST**. Vitória: PRODEST, 2026. Disponível em: <https://prodest.es.gov.br/seguranca-e-privacidade/>. Acesso em: 18 maio 2026.

INTERNATIONAL COUNCIL ON ARCHIVES. **ISAD(G): General International Standard Archival Description**. 2nd ed. Ottawa: ICA, 2000.

INTERNATIONAL COUNCIL ON ARCHIVES. **Records in Contexts: Conceptual Model — RiC-CM**. Version 1.0. Paris: ICA, 2023.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 16919:2014: Space data and information transfer systems: Requirements for bodies providing audit and certification of candidate trustworthy digital repositories**. Geneva: ISO, 2014.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 15489-1:2016: Information and documentation: Records management: Part 1: Concepts and principles**. Geneva: ISO, 2016.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 15836-1:2017: Information and documentation: The Dublin Core metadata element set: Part 1: Core elements**. Geneva: ISO, 2017a.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 23081-1:2017: Information and documentation: Records management processes: Metadata for records: Part 1: Principles**. Geneva: ISO, 2017b.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 15836-2:2019: Information and documentation: The Dublin Core metadata element set: Part 2: DCMI properties and classes**. Geneva: ISO, 2019.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 16175-1:2020: Information and documentation: Processes and functional requirements for software for managing records: Part 1: Functional requirements and associated guidance for any applications that manage digital records**. Geneva: ISO, 2020.

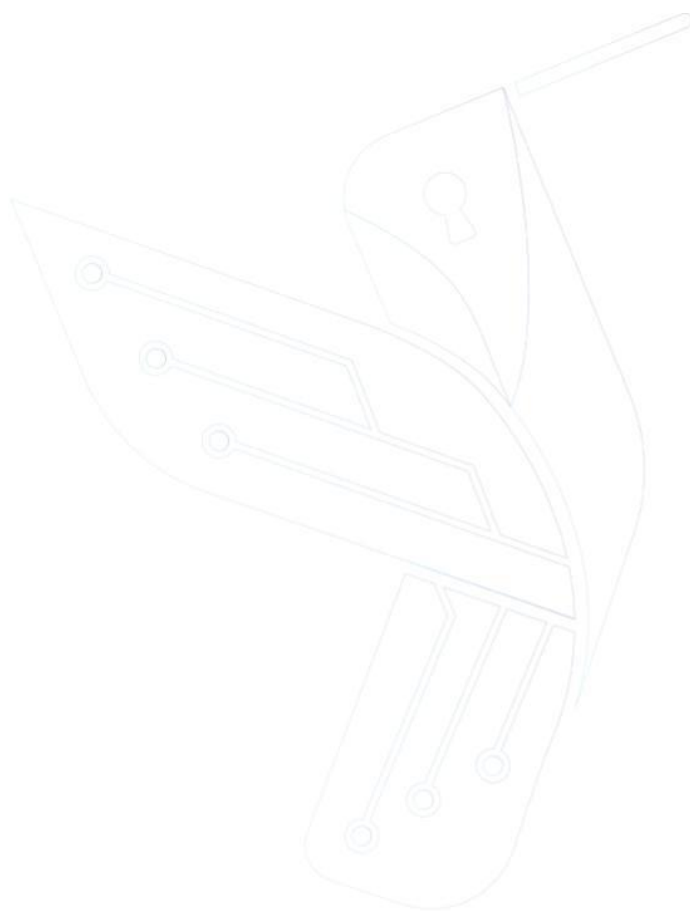
INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 23081-2:2021: Information and documentation: Records management processes: Metadata for records: Part 2: Conceptual and implementation issues**. Geneva: ISO, 2021.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 14721:2025: Space data and information transfer systems: Open archival information system — OAIS: Reference model**. Geneva: ISO, 2025a.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 16363:2025: Space data and information transfer systems: Audit and certification of trustworthy digital repositories**. Geneva: ISO, 2025b.

LIBRARY OF CONGRESS. **PREMIS Data Dictionary for Preservation Metadata**. Version 3.0. Washington, DC: Library of Congress, 2015.

LIBRARY OF CONGRESS. **METS: Metadata Encoding and Transmission Standard**. Washington, DC: Library of Congress, 2026. Disponível em: <https://www.loc.gov/standards/mets/>. Acesso em: 18 maio 2026.



APÊNDICE A - CONJUNTO MÍNIMO DE METADADOS

nº	CATEGORIA	ELEMENTO DO CONJUNTO MÍNIMO	RÓTULO ADOTADO	EXEMPLOS DE EQUIVALÊNCIAS	TIPO FUNCIONAL
1	Documento	Tipo Recurso	pds.tipoRecurso	QRKMS Record category type	Gestão
2	Documento	Identificador do Recurso	dc.identifier	PREMIS Object Identifier; QRKMS Record Identifier; e-PMG identificador.idDoSistema	Gestão
3	Documento	Número Recurso	pds.numeroRecurso	Elemento próprio do conjunto mínimo	Gestão
4	Documento	Tipo de meio	earq.documento.meio	PREMIS ObjectCategory; QRKMS Record format.Medium; NOBRADE Dimensão e suporte / Características físicas e requisitos técnicos	Gestão/ Preservação
5	Documento	Status	earq.documento.status	e-ARQ Brasil	Gestão
6	Documento	Identificador de versão	earq.documento.versão / dcterms.isVersionOf	PREMIS hasVersion; QRKMS Record Relation; e-PMG identificador.versao	Gestão/ Preservação
7	Documento	Título	dc.title	QRKMS Record Title; e-PMG Título; ISAD(G) Title; NOBRADE Título	Descritivo

8	Documento	Descrição	dc.description	QRKMS Record Description; e-PMG Descrição.resumo; ISAD(G) Scope and content	Descritivo
9	Documento	Assunto	dc.subject	QRKMS Record Subject; e-PMG Assunto.palavra-chave; ISAD(G) Subject	Descritivo
10	Documento	Autor	dc.creator	QRKMS Record creator; e-PMG Criador; ISAD(G) Name of creator(s)	Descritivo/ Gestão
11	Documento	Destinatário	earq.documento.destinatario	e-PMG Destinatário; IPAM Addressee	Descritivo/ Gestão
12	Documento	Originador	earq.documento.originador	IPAM Originator	Descritivo/ Gestão
13	Documento	Redator	earq.documento.redator	IPAM Writer	Descritivo/ Gestão
14	Documento	Interessado Nome	earq.documento.interessadoNome	Elemento próprio do conjunto mínimo	Gestão
15	Documento	Interessado Tipo	earq.documento.interessadoTipo	Elemento próprio do conjunto mínimo	Gestão
16	Documento	Identificador do componente digital	earq.componente.id / pds.linkingDigitalComponentId	PREMIS relationshipType; PREMIS relatedObjectIdentifier; e-PMG relação.temParteDe	Preservação
17	Documento	Gênero	earq.documento.genero / dc:type	QRKMS Record type; e-PMG Tipo de Recurso;	Descritivo

				NOBRADE Dimensão e suporte	
18	Documento	Espécie	earq.documento.especie / dc:type	QRKMS Record type; e-PMG Tipo de Recurso; NOBRADE Dimensão e suporte	Descritivo
19	Documento	Tipo	dc.type	QRKMS Record type; e-PMG Tipo de Recurso; NOBRADE Dimensão e suporte	Descritivo
20	Documento	Idioma	dc.language	QRKMS Language; e-PMG Idioma; ISAD(G) Language of material; NOBRADE Idioma	Descritivo
21	Documento	Quantidade de folhas	earq.documento.folhaNum / dcterms:extent	QRKMS Record format.Extent; e-PMG formato.dimensão; ISAD(G) Extent and medium	Gestão
22	Documento	Numeração sequencial dos documentos	earq.documento.sequencia	PREMIS relatedObjectSequence	Gestão / Preservação
23	Documento	Indicação de anexos	earq.documento.anexo	Elemento próprio do conjunto mínimo	Gestão
24	Documento	Indicação de anotação	earq.documento.anotacao	Elemento próprio do conjunto mínimo	Gestão/ Preservação

25	Documento	Setor responsável pela execução da ação	earq.documento.setorExecucao	Elemento próprio do conjunto mínimo	Gestão
26	Documento	Relação com outros documentos	dc.relation	QRKMS Record relation; PREMIS Relationship; e-PMG Relação; ISAD(G) Relationships	Descritivo / Preservação
27	Documento	Níveis de acesso	dc.rights / dcterms:accessRights	QRKMS Record access; e-PMG Direitos.classificaçãoDoGrauDeSigilo; ISAD(G) Conditions of access; NOBRADE Condições de acesso	Gestão
28	Documento	Previsão de desclassificação	earq.documento.previsaoDesclassificacao	dcterms:date; e-PMG Direitos.dataDeExpiraçãoDoGrauDeSigilo	Gestão
29	Documento	Data de produção	dc.date.created	PREMIS eventDateTime; QRKMS Record date.Creation date; e-PMG data.criação; ISAD(G) Dates; NOBRADE Data(s)	Descritivo/ Gestão

30	Documento	Classe	earq.documento.classe	QRKMS Record classification; e-PMG identificador.códigoDeClassificação; ISAD(G) Reference code	Gestão
31	Documento	Destinação prevista	earq.documento.destinacao	e-PMG Destinação; NOBRADE Avaliação, eliminação e temporalidade	Gestão
32	Documento	Prazo de guarda	earq.documento.prazoGuarda	e-PMG Destinação.prazoDeGuarda; NOBRADE Avaliação, eliminação e temporalidade	Gestão
33	Documento	Nível de descrição	isad.nivelDescricao	ISAD(G); NOBRADE	Descritivo
34	Documento	Coverage	dc.coverage	QRKMS Record coverage; e-PMG Abrangência.especial	Descritivo
35	Documento	Source	dc.source	e-PMG Fonte	Descritivo / Preservação
36	Documento	Localização	earq.documento.localizacao	QRKMS Record location; e-PMG Localização	Gestão
37	Evento	Identificador do evento	premis-eventIdentifier	QRKMS Event ID	Preservação
38	Evento	Tipo de evento	premis.eventType	QRKMS Event Type	Preservação
39	Evento	Identificador recurso	premis.linkableObjectIdentifier	PREMIS linkingObjectIdentifier	Preservação

40	Evento	Data e hora do evento	<code>premis.eventDateTime</code>	QRKMS Event Date/Time; dcterms:date	Preservação
41	Evento	Agente responsável pelo evento	<code>premis.linkingAgentIdentifier</code>	QRKMS Record agent; QRKMS Action Officer	Preservação
42	Evento	Cargo do agente responsável pelo evento	<code>premis.linkingAgentRole</code>	PREMIS linkingAgentRole	Preservação
43	Evento	Resultado do evento	<code>premis:eventOutcome</code>	PREMIS eventOutcome	Preservação
44	Evento	Detalhes do evento	<code>premis:eventDetailInformation</code>	QRKMS Event Description	Preservação
45	Classe	Identificador da classe	<code>earq.classe.id</code>	e-PMG identificador.códigoDeClassificação	Gestão
46	Classe	Nome da classe	<code>earq.classe.nome</code>	Elemento próprio do conjunto mínimo	Gestão
47	Classe	Código da classe	<code>earq.classe.codigo</code>	Elemento próprio do conjunto mínimo	Gestão
48	Classe	Subordinação da classe	<code>earq.classe.subordinacao</code>	Elemento próprio do conjunto mínimo	Gestão
49	Classe	Indicação de permissão de uso	<code>earq.classe.indicadorUso</code>	Elemento próprio do conjunto mínimo	Gestão

50	Classe	Indicação de classe ativa/inativa	earq.classe.indicadorAtiva	Elemento próprio do conjunto mínimo	Gestão
51	Classe	Prazo na idade corrente	earq.classe.prazoCorrente	e-PMG Destinação.prazoDeGuarda	Gestão
52	Classe	Evento de contagem na idade corrente	earq.classe.eventoCorrente	e-PMG destinação.ação	Gestão
53	Classe	Prazo na idade intermediária	earq.classe.prazoIntermediaria	e-PMG Destinação.prazoDeGuarda	Gestão
54	Classe	Evento de contagem na idade intermediária	earq.classe.eventoIntermediaria	e-PMG destinação.ação	Gestão
55	Classe	Destinação final	earq.classe.destinacao	e-PMG destinação.localDeDestinação	Gestão
56	Classe	Sigilo associado à classe	earq.classe.sigilo	e-PMG Direitos.classificaçãoDoGrauDeSigilo	Gestão
57	Classe	Observação	earq.classe.observacao	e-PMG Observação	Gestão
58	Componente digital	Identificador do componente digital	earq.componente.id	PREMIS ObjectIdentifierValue	Preservação
59	Componente digital	Nome original	earq.componente.nomeOriginal	PREMIS originalName	Preservação

60	Componente digital	Tamanho	earq.componente.tamanho	PREMIS size	Preservação
61	Componente digital	Software de criação	earq.componente.software Criacao	PREMIS creatingApplicationName; creatingApplicationVersion; dateCreatedByApplication; QRKMS Original creating environment	Preservação
62	Componente digital	Nível de composição	earq.componente.nivelCom posicao	PREMIS compositionLevel	Preservação
63	Componente digital	Inibidor	earq.componente.inibidor	PREMIS inhibitorType; inhibitorTarget; inhibitorKey	Preservação
64	Componente digital	Formato	dc:format	PREMIS formatName; PREMIS formatVersion; QRKMS Record Format	Preservação
65	Componente digital	Localização	earq.componente.localiza cao	PREMIS contentLocationType; contentLocationValue	Preservação
66	Componente digital	Suporte	earq.componente.suporte	PREMIS storageMedium	Preservação
67	Componente digital	Dependência de software	earq.componente.sw	PREMIS CreatingApplication; PREMIS software environment	Preservação
68	Componente digital	Dependência de hardware	earq.componente.hw	PREMIS Environment; hardware dependency	Preservação

69	Componente digital	Outras Dependências	earq.componente.outrasDependencias	PREMIS relationshipType=dependency; relationshipSubType=requires / is required by	Preservação
70	Componente digital	Relação	earq.componente.relacao	PREMIS relationshipType; relationshipSubType; relatedObjectIdentifier	Preservação
71	Componente digital	Fixidade	earq.componente.fixidade	PREMIS Fixity; messageDigestAlgorithm; messageDigest; messageDigestOriginator	Preservação
72	Componente digital	Assinatura digital	earq.componente.assinatura	PREMIS Signature	Preservação
73	Componente digital	Assinatura digital-Codificação	earq.componente.assinaturaCodificacao	PREMIS signatureEncoding	Preservação
74	Componente digital	Assinatura digital-Signatário	earq.signatario	PREMIS signer	Preservação
75	Componente digital	Assinatura digital-Método	earq.componente.assinaturaMetodo	PREMIS signatureMethod	Preservação
76	Componente digital	Assinatura digital-Valor	earq.componente.assinaturaValor	PREMIS signatureValue	Preservação
77	Componente digital	Assinatura digital-Regras de Validação	earq.componente.assinaturaRegrasValidacao	PREMIS signatureValidationRules	Preservação

78	Componente digital	Assinatura digital-Propriedades	<code>premis:signatureProperties</code>	PREMIS signatureProperties	Preservação
79	Componente digital	Assinatura digital-Chave	<code>earq.componente.assinaturaChave</code>	PREMIS keyInformation	Preservação
80	Componente digital	Assinatura digital-Extensão	<code>premis:signatureInformationExtension</code>	PREMIS signatureInformationExtension	Preservação
81	Agente	Identificador do agente	<code>earq.agente.id</code>	Elemento próprio do conjunto mínimo	Gestão / Preservação
82	Agente	Nome do agente	<code>earq.agente.nome</code>	Elemento próprio do conjunto mínimo	Gestão / Preservação
83	Agente	Status do agente	<code>earq.agente.status</code>	Elemento próprio do conjunto mínimo	Gestão / Preservação
84	Agente	Tipo Agente	<code>premis.agentType</code>	QRKMS Agent category type	Gestão / Preservação

APÊNDICE B - MATRIZ RACI

ATIVIDADE / RESPONSABILIDADE	APEES	PRODEST	ENTIDADES PRODUTORES
Definir requisitos arquivísticos	A/R	C	I
Orientar a preparação de pré-SIP	A/R	C	R
Selecionar os documentos que comporão os acervos arquivísticos a serem submetidos	C	I	A/R
Garantir organização mínima dos acervos	C	I	A/R
Fornecer metadados de origem, quando aplicável	C	I	A/R
Validar metadados arquivísticos	A/R	C	C
Avaliar autenticidade na entrada, quando aplicável	A/R	C	C
Informar restrições de acesso	C	I	A/R
Definir restrições de acesso	A/R	C	C
Indicar direitos, sigilos e dados sensíveis	C	I	A/R
Cumprir formatos e requisitos de submissão	C	C	A/R
Prover e manter infraestrutura tecnológica	I	A/R	I
Garantir armazenamento	I	A/R	I
Executar rotinas técnicas de segurança	I	A/R	I

Apoiar verificação de integridade	C	R	I
Manter disponibilidade dos sistemas	I	A/R	I
Apoiar backup e recuperação	I	A/R	I
Registrar incidentes técnicos relacionados à infraestrutura tecnológica	I	A/R	I
Aprovar estratégias de preservação	A/R	C	I
Acompanhar geração de pacotes AIP e DIP	A/R	R	I
Manter documentação arquivística do processo	A/R	C	I

Legenda:

R = Responsável pela execução

A = Autoridade/ Aprovador final

C = Consultado

I = Informado