CERTIFICAÇÃO DE REPOSITÓRIOS DIGITAIS

SUDESTE/RIAA

Rede Sudeste de Repositórios Institucionais

Agenda

01 **Preservação Digital**

- Aspectos gerais
- Estratégias

02 **Repositórios**

- Aspectos conceituais
- Modelo OAIS

03 **Normas e Certificação**

- Aspectos gerais
- ISO 16.363

Preservação Digital

Preservação Digital

Obsolescência Tecnológica

-Hardware
-Software

Adulterações e corrupções

Tornam as informações não confiáveis ou inacessíveis

Garantir a preservação e acesso pelo tempo que for necessário

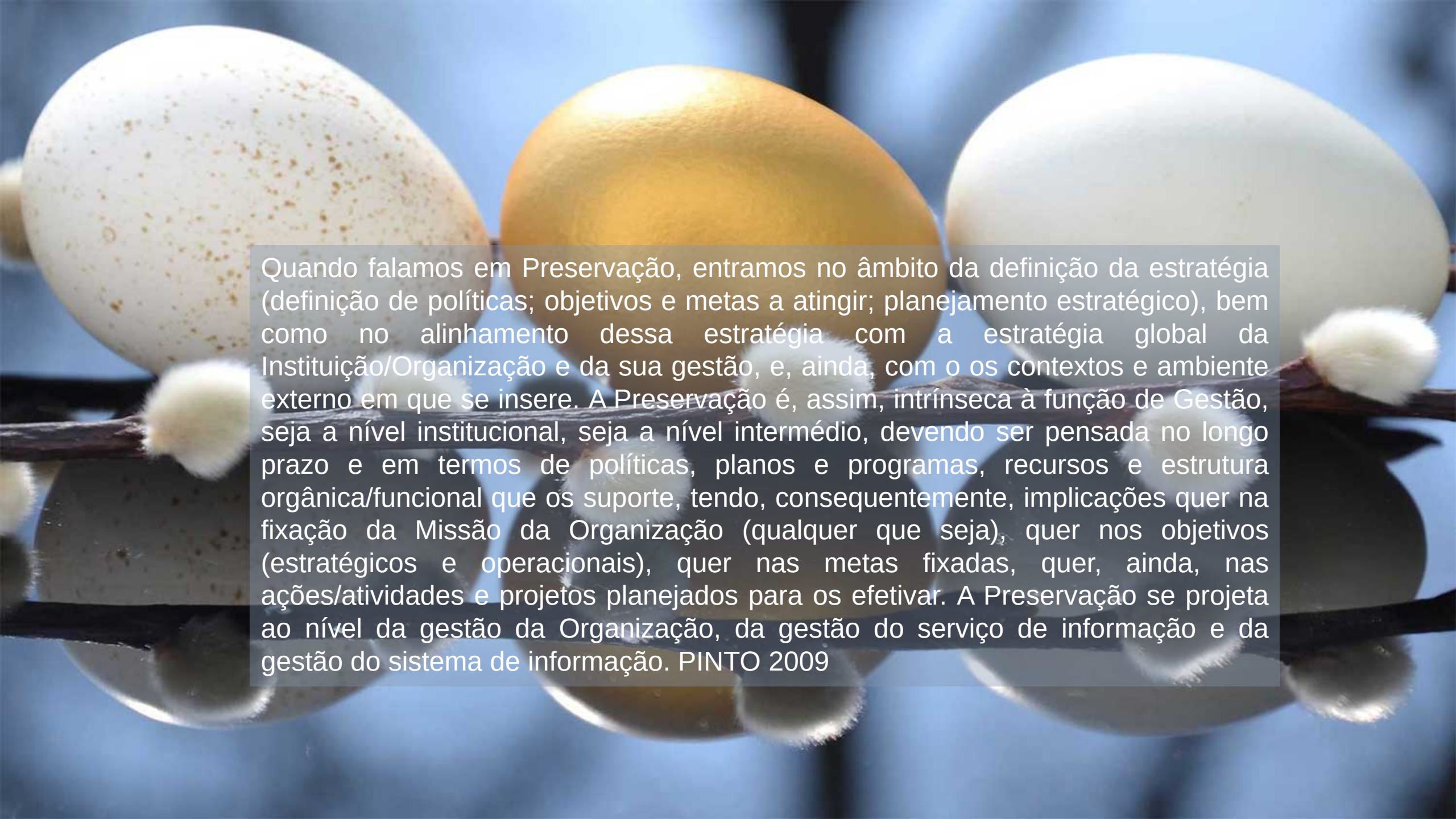
Manutenção da autenticidade

Garantia de integridade e identidade

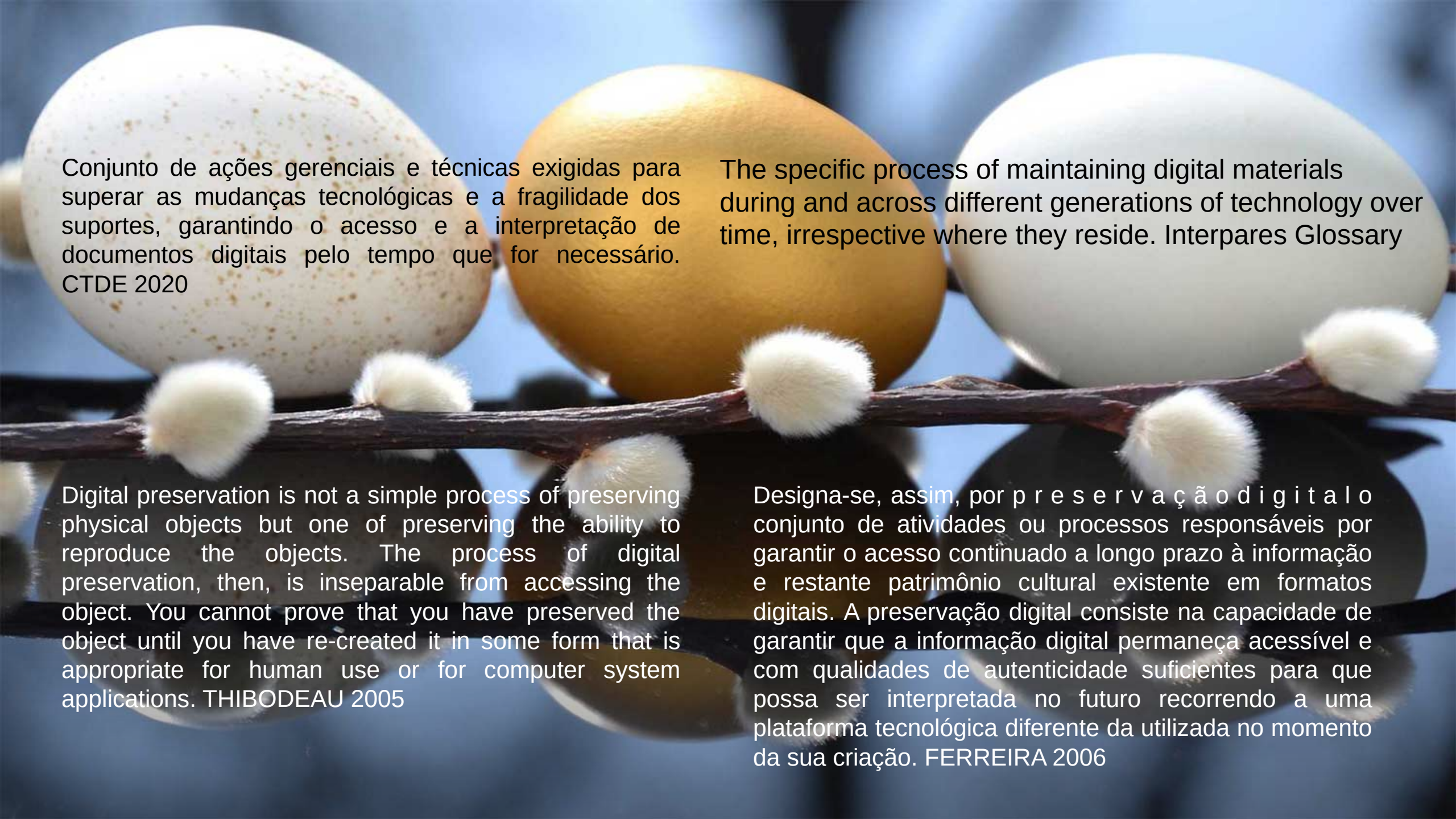
Metadados

Fundamentais para preservação, recuperação e autenticidade

Garantir documentos dotados de credibilidade durante sua vida útil



Quando falamos em Preservação, entramos no âmbito da definição da estratégia (definição de políticas; objetivos e metas a atingir; planejamento estratégico), bem como no alinhamento dessa estratégia com a estratégia global da Instituição/Organização e da sua gestão, e, ainda, com o os contextos e ambiente externo em que se insere. A Preservação é, assim, intrínseca à função de Gestão, seja a nível institucional, seja a nível intermédio, devendo ser pensada no longo prazo e em termos de políticas, planos e programas, recursos e estrutura orgânica/funcional que os suporte, tendo, consequentemente, implicações quer na fixação da Missão da Organização (qualquer que seja), quer nos objetivos (estratégicos e operacionais), quer nas metas fixadas, quer, ainda, nas ações/atividades e projetos planejados para os efetivar. A Preservação se projeta ao nível da gestão da Organização, da gestão do serviço de informação e da gestão do sistema de informação. PINTO 2009



Conjunto de ações gerenciais e técnicas exigidas para superar as mudanças tecnológicas e a fragilidade dos suportes, garantindo o acesso e a interpretação de documentos digitais pelo tempo que for necessário. CTDE 2020

The specific process of maintaining digital materials during and across different generations of technology over time, irrespective where they reside. Interpares Glossary

Digital preservation is not a simple process of preserving physical objects but one of preserving the ability to reproduce the objects. The process of digital preservation, then, is inseparable from accessing the object. You cannot prove that you have preserved the object until you have re-created it in some form that is appropriate for human use or for computer system applications. THIBODEAU 2005

Designa-se, assim, por p r e s e r v a ç ã o d i g i t a l o conjunto de atividades ou processos responsáveis por garantir o acesso continuado a longo prazo à informação e restante patrimônio cultural existente em formatos digitais. A preservação digital consiste na capacidade de garantir que a informação digital permaneça acessível e com qualidades de autenticidade suficientes para que possa ser interpretada no futuro recorrendo a uma plataforma tecnológica diferente da utilizada no momento da sua criação. FERREIRA 2006

Objeto Digital

Objeto conceitual

O objeto conceitual é o objeto com o qual lidamos no mundo real: é uma entidade que reconheceríamos como uma unidade significativa de informação, como um livro, um contrato, um mapa ou, por exemplo, uma fotografia.

Objeto físico

um objeto digital é simplesmente uma inscrição de signos em um meio

Objeto Lógico

Um objeto lógico é uma unidade reconhecida por algum software aplicativo

As estratégias de preservação agem sobre uma ou mais dimensões destes objetos

Estratégias

Encapsulamento

A preservação do objeto digital, juntamente com toda a informação considerada necessária e suficiente para garantir o desenvolvimento futuro de software aplicacional para conversão, visualização ou emulação, por exemplo, a descrição formal e detalhada do formato de ficheiro do objeto a preservar.

Normalização

Tem como objetivo simplificar o processo de preservação através da redução do número de formatos.

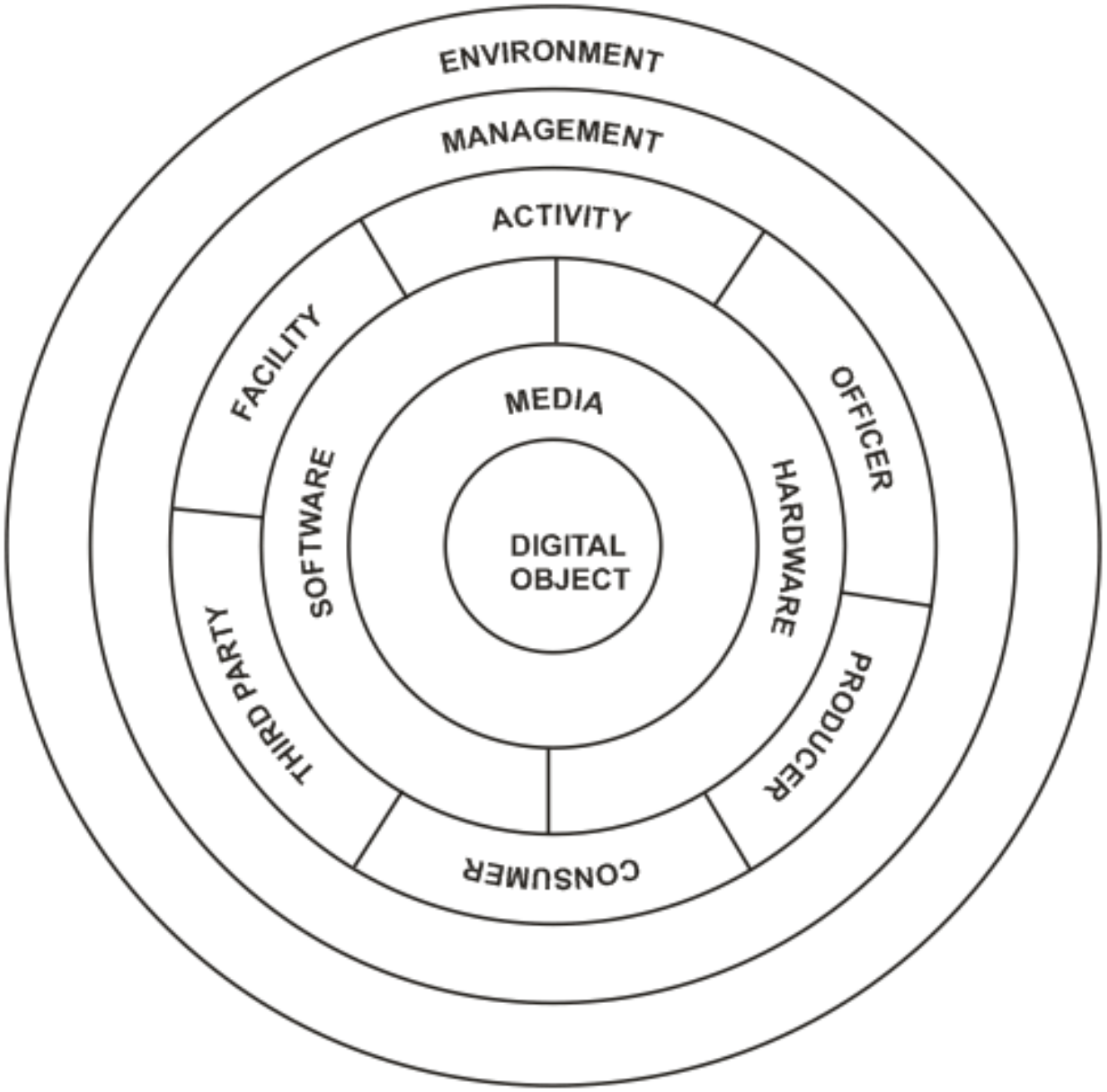
Migração / Conversão

É a transferência periódica de materiais digitais de uma configuração de hardware / software para outra ou de uma geração de tecnologia de computador para uma geração subsequente.

Diretório de formatos

Diretório centralizado de informação técnica sobre formatos digitais. Esta informação inclui, por exemplo, a identificação dos produtores de um dado formato, a sua data de criação, informação sobre as aplicações que o suportam, especificações técnicas, grau de obsolescência, entre outros.

Four criteria apply in all cases: any method chosen for preservation must be feasible, sustainable, practicable, and appropriate.
THIBODEAU 2005



Digital Object Context Model

> As relações entre as variáveis da organização mostram como o centro depende da periferia. Na verdade, o objecto de arquivo digital depende do suporte de armazenamento, onde é registado, do software de apresentação que o interpreta, no hardware de processamento que o lê e processa, da interacção entre a actividade de Manutenção, Actividade de Negócios, funcionário, Produtor, Consumidor, terceiros e as Instalações que o gerem, da gestão para estabelecer políticas de preservação e, finalmente, do ambiente no qual ele é mantido

CORUJO 2014

Repositórios e o modelo OAIS

Como executar as estratégias de forma sistemática e controlada

?

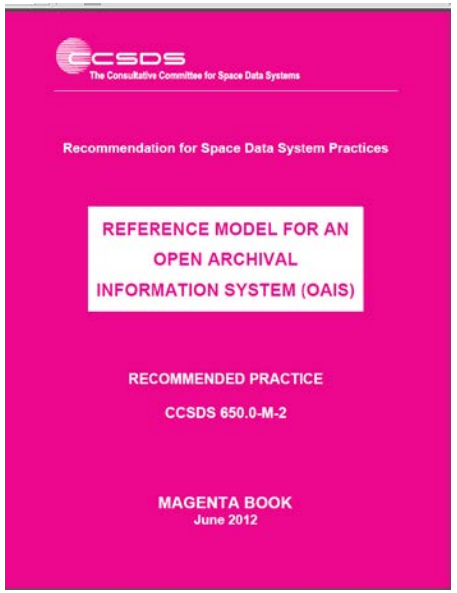
"envisions the development of a national system of digital archives, which it defines as repositories of digital information that are collectively responsible for the long-term accessibility of the nation's social, economic, cultural and intellectual heritage instantiated in digital form"

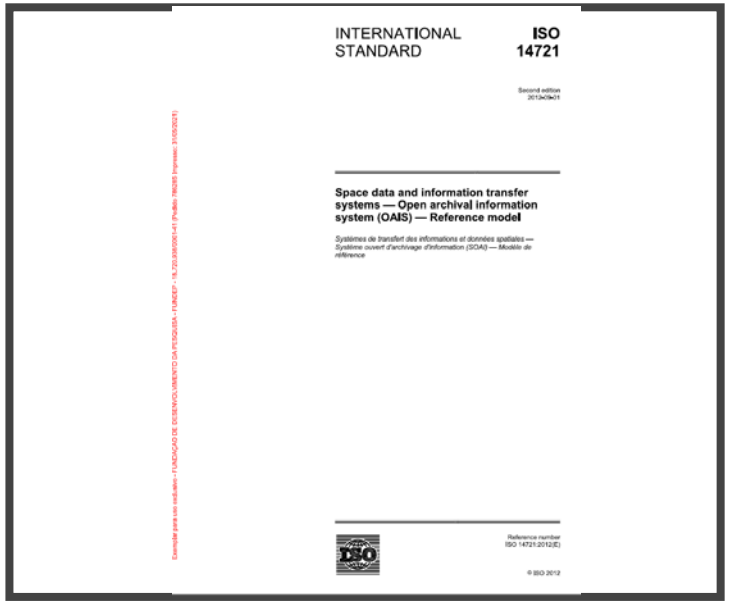
Walters; Garrett

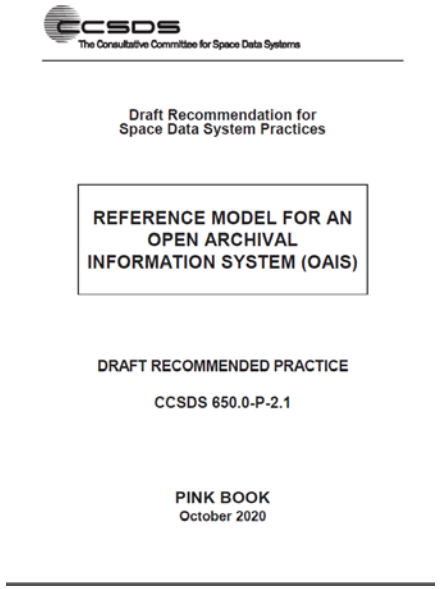
OAIS

Open Archival Information System

Open Archival Information System (OAIS) - um Arquivo, que consiste em uma organização de pessoas e sistemas, que aceitam a responsabilidade de preservar informações e disponibilizá-las para uma comunidade designada.



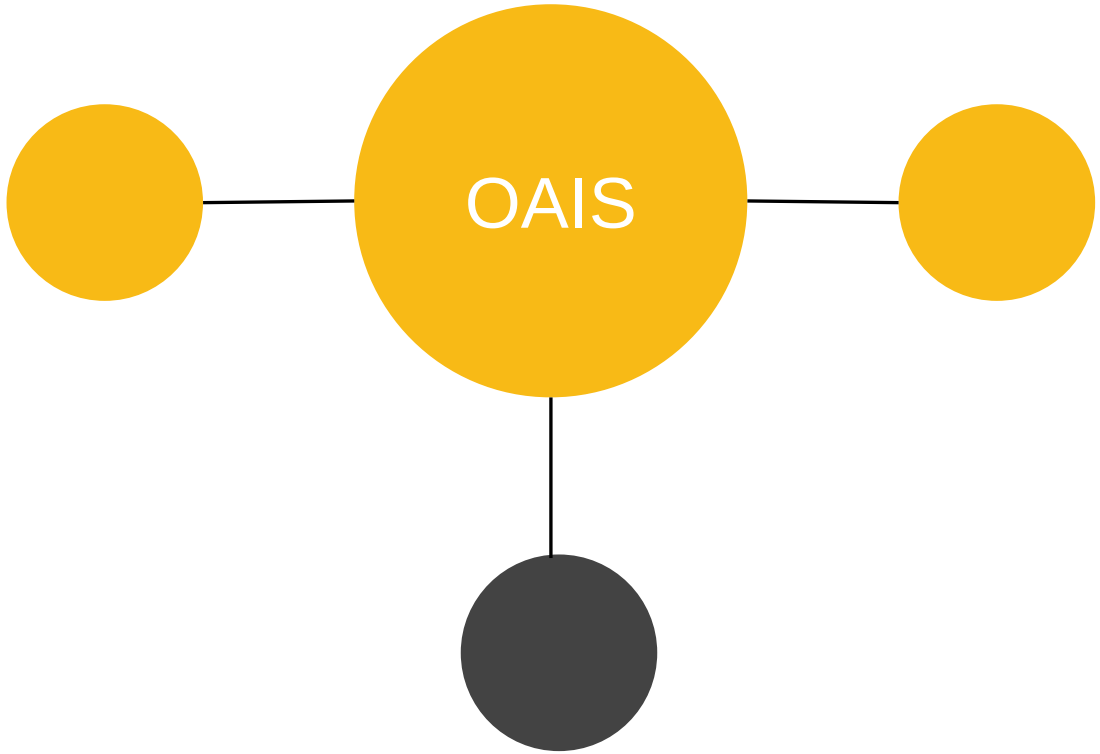




Responsabilidades

1. Negociar e aceitar as informações apropriadas dos produtores de informações.
2. Obter controle suficiente das informações fornecidas ao nível necessário para garantir a preservação de longo prazo.
3. Determinar, isoladamente ou em conjunto com outras partes, quais entidades devem se tornar a Comunidade Designada, ou seja, as comunidades que devem ser capazes de compreender as informações prestadas.
4. Certificar que a comunidade designada é capaz de compreender as informações preservadas sem a necessidade de recursos especiais ou da ajuda dos produtores.
5. Seguir as políticas e procedimentos documentados que garantem que a informação seja preservada contra todas as contingências razoáveis, incluindo a extinção do arquivo, garantindo que nunca seja excluído, a menos que seja permitido como parte de uma estratégia aprovada.
6. Disponibilizar as informações preservadas para a comunidade designada e permitir que as informações sejam disseminadas como cópias ou rastreáveis ao original enviando informações de conteúdo com evidências que apóiam sua autenticidade.

Ambiente Externo



Produtor

Que fornece a informação a ser preservada

Consumidor

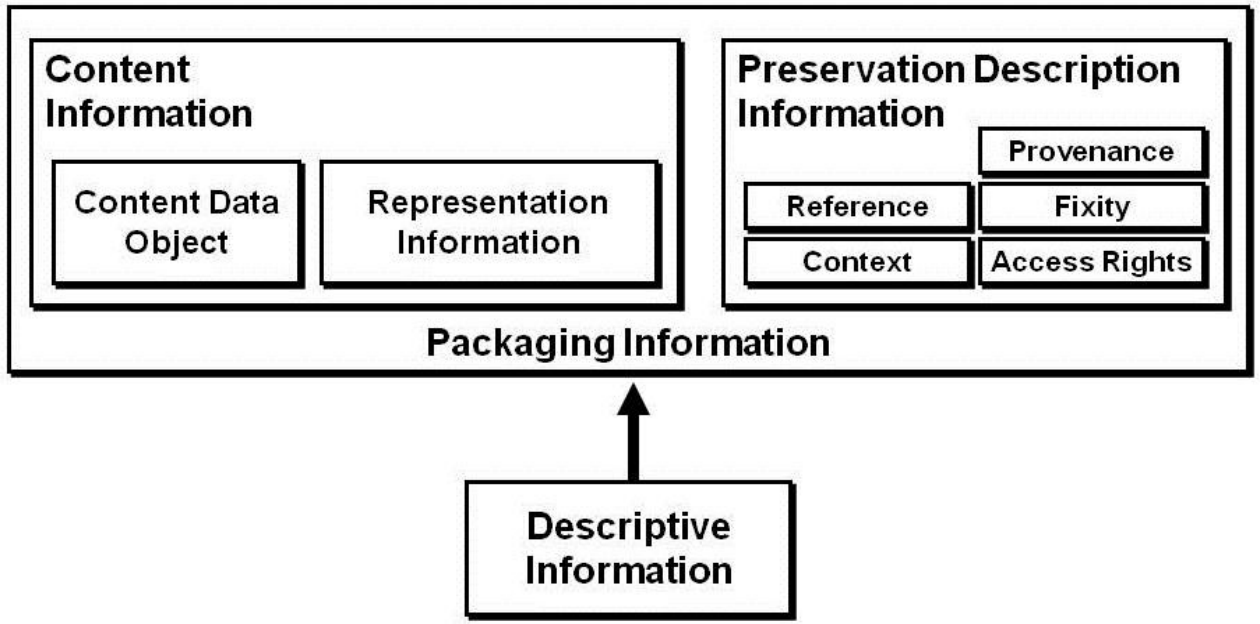
Que procura e adquire informação que se encontra preservada no arquivo OAIS

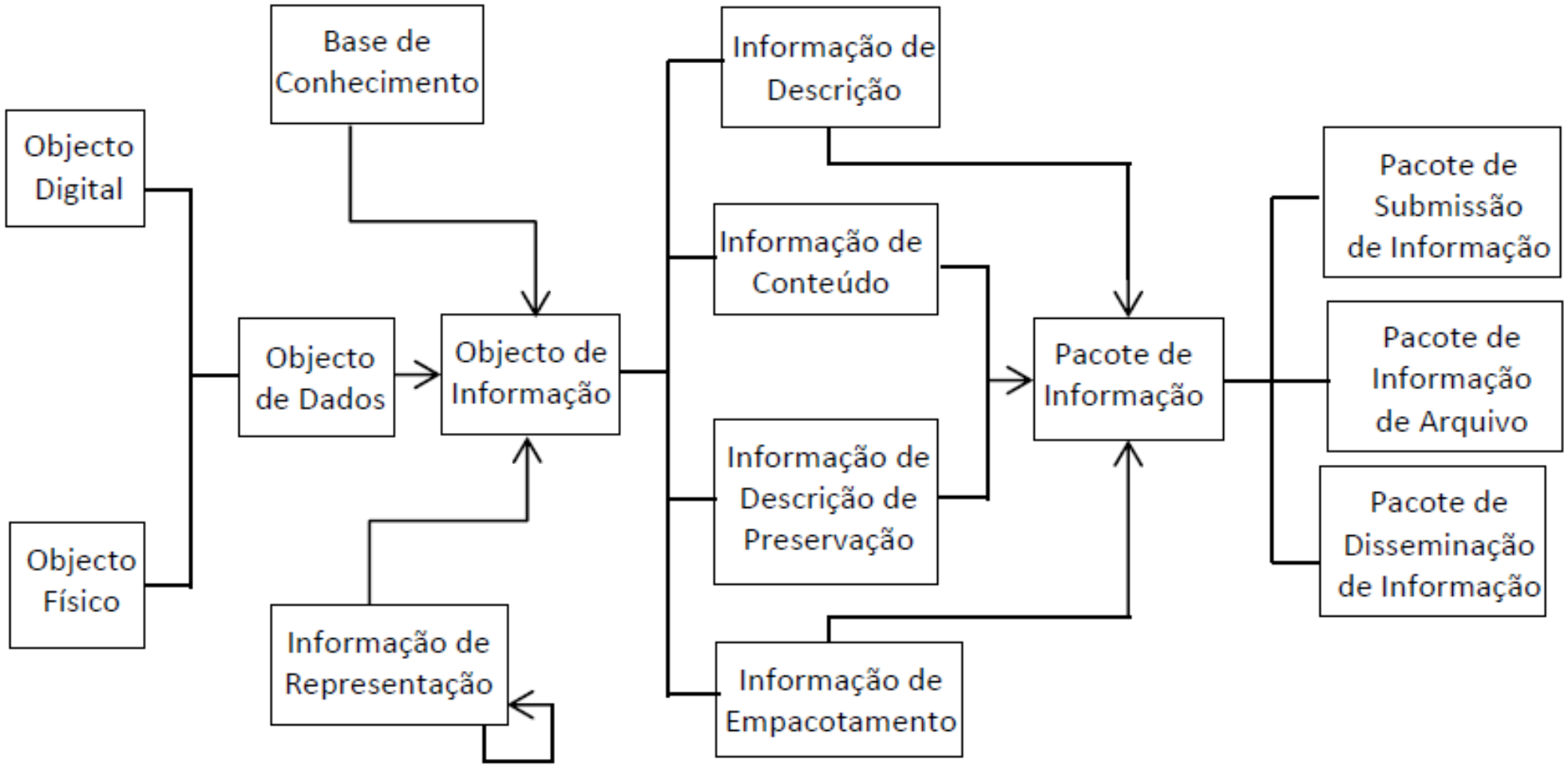
Administrador

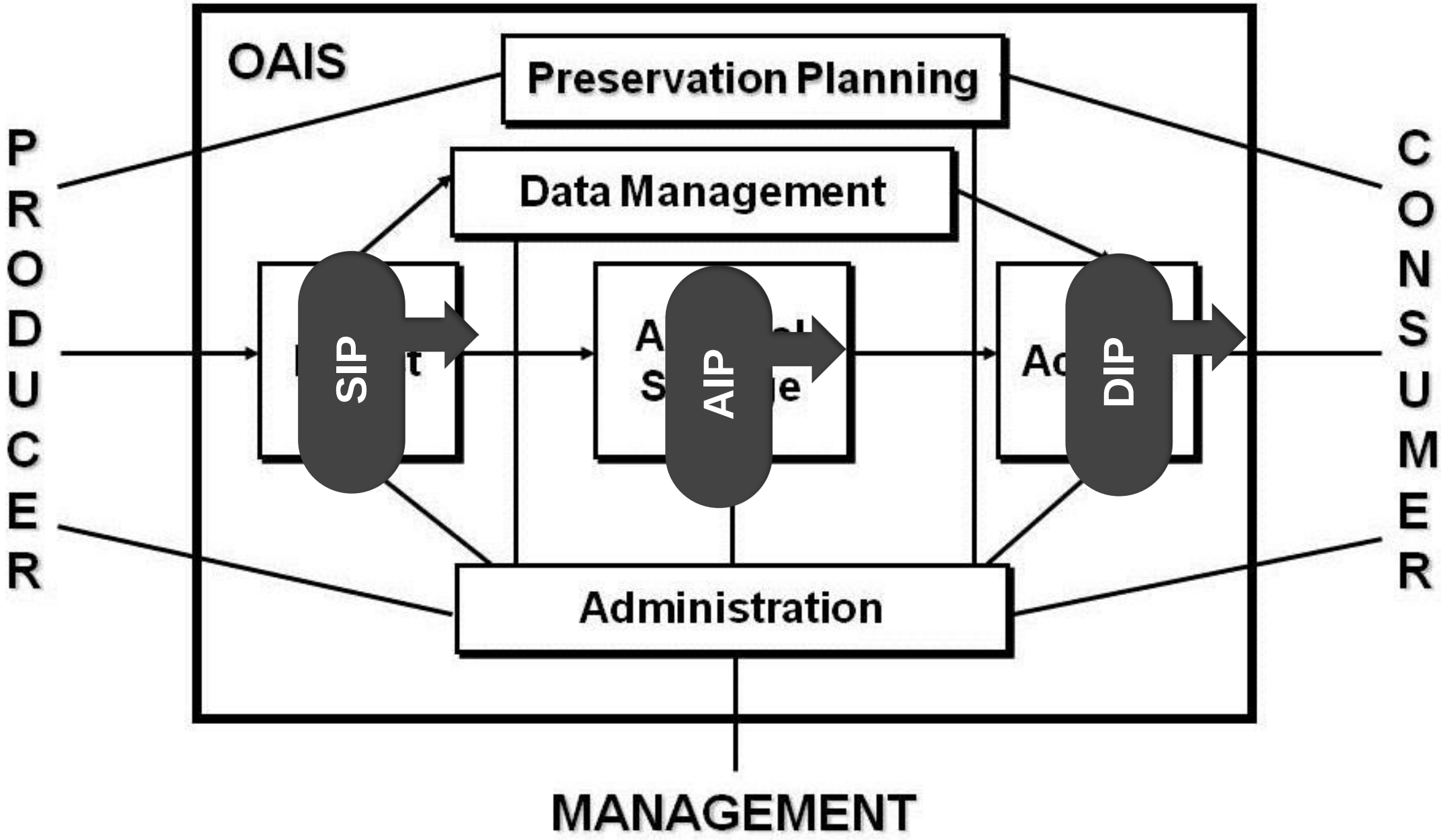
Que fornece a política geral do arquivo OAIS e efetua o controle de gestão

As informações OAIS modelo é construído em torno do conceito de um pacote de informações: uma conceituação da estrutura de informações à medida que se movem para dentro, através e fora do sistema de arquivamento. Um pacote de informações consiste no objeto que é o foco de preservação, juntamente com os metadados necessários para apoiar sua preservação a longo prazo, acesso e compreensibilidade vinculados a um único pacote lógico

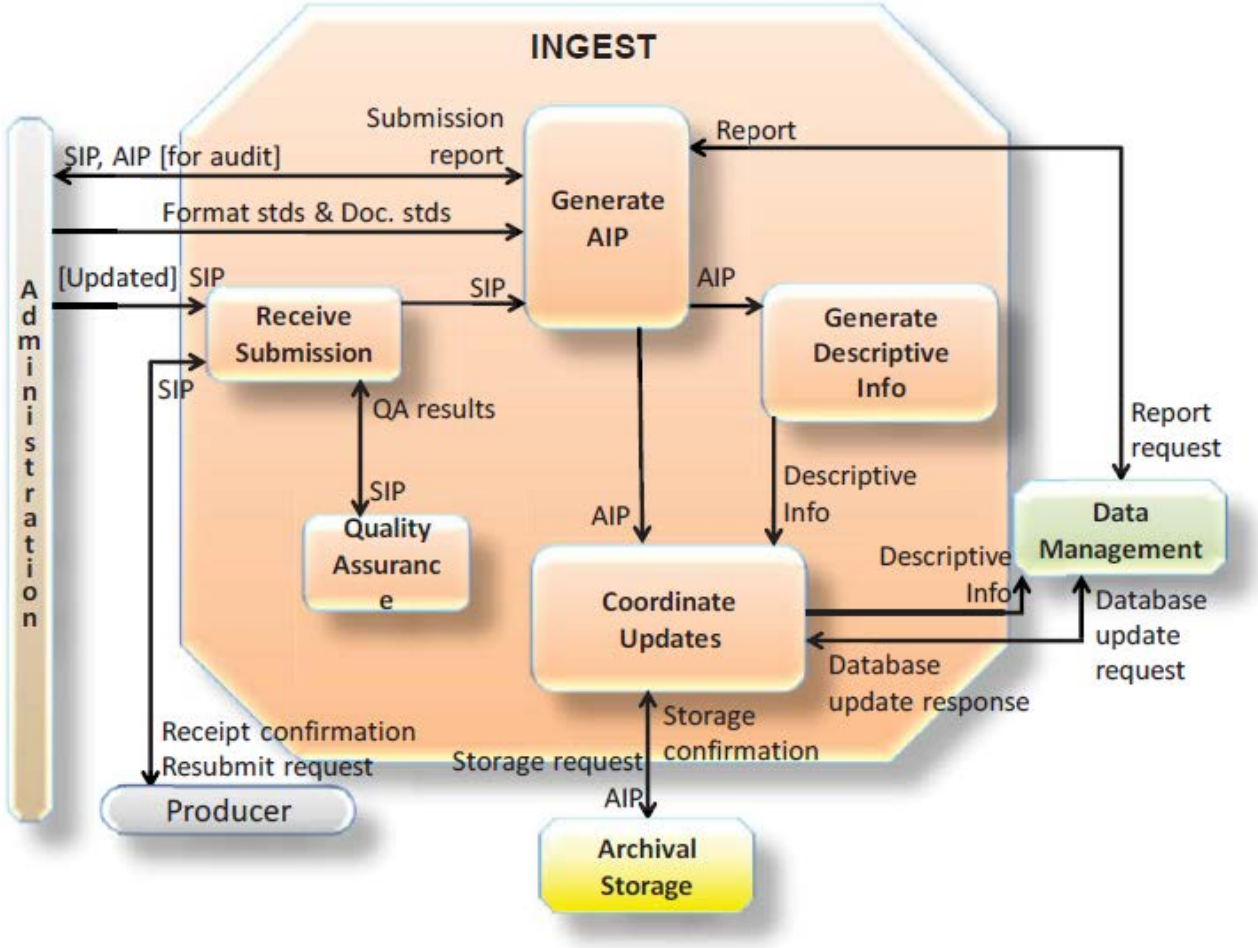
Pacote de Informação




Base de Conhecimento
Objecto Digital
Objecto de Dados
Objecto Físico
Objecto de Informação
Informação de Representação
Informação de Descrição
Informação de Conteúdo
Informação de Descrição de Preservação
Informação de Empacotamento
Pacote de Informação
Pacote de Submissão de Informação
Pacote de Informação de Arquivo
Pacote de Disseminação de Informação

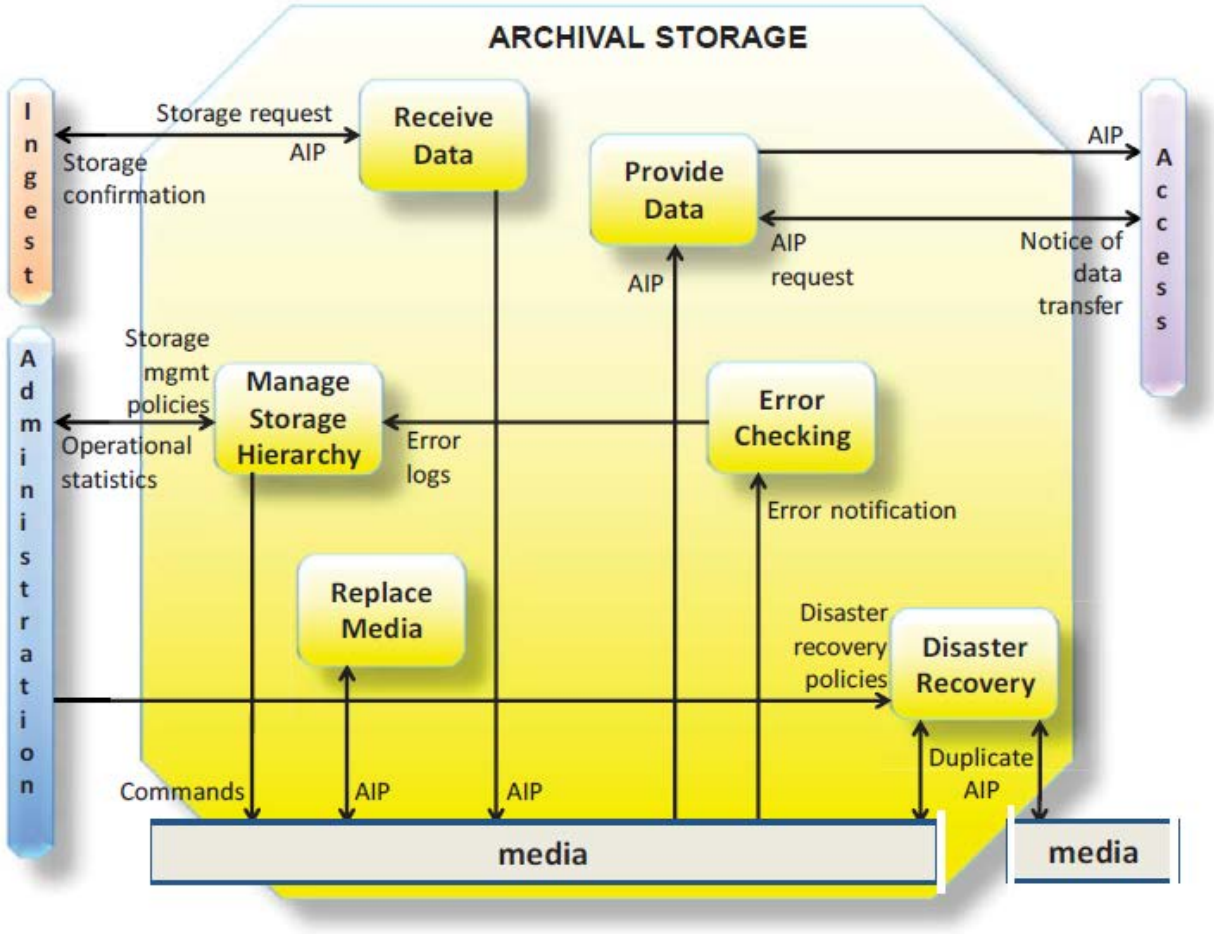

OAIS
Preservation Planning
Data Management
SIP
AIP
DIP
Administration
PRODUCER
CONSUMER
MANAGEMENT

INGEST



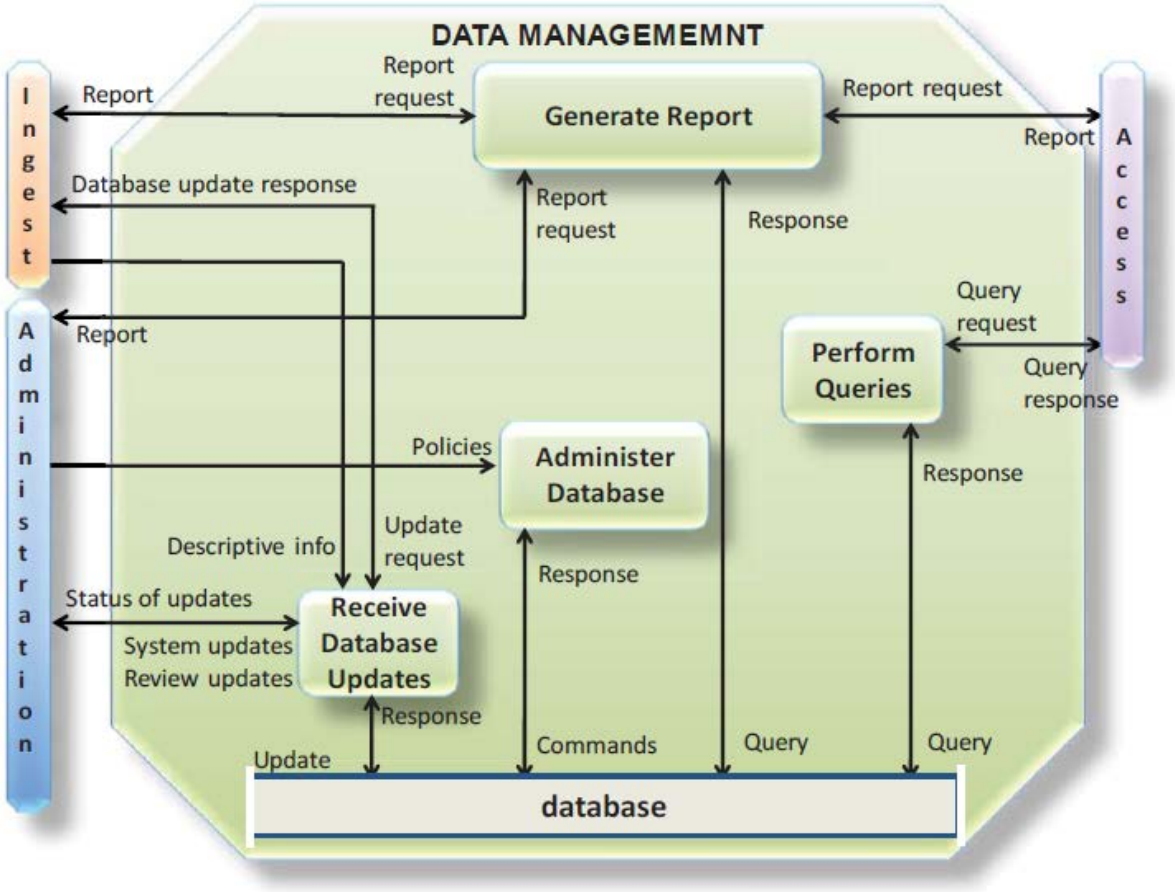
Função Ingest serve como interface externa da OAIS com os produtores, gerenciando todo o processo de aceitação da custódia das informações enviadas e preparando-as para a retenção do arquivo.

ARCHIVAL STORAGE



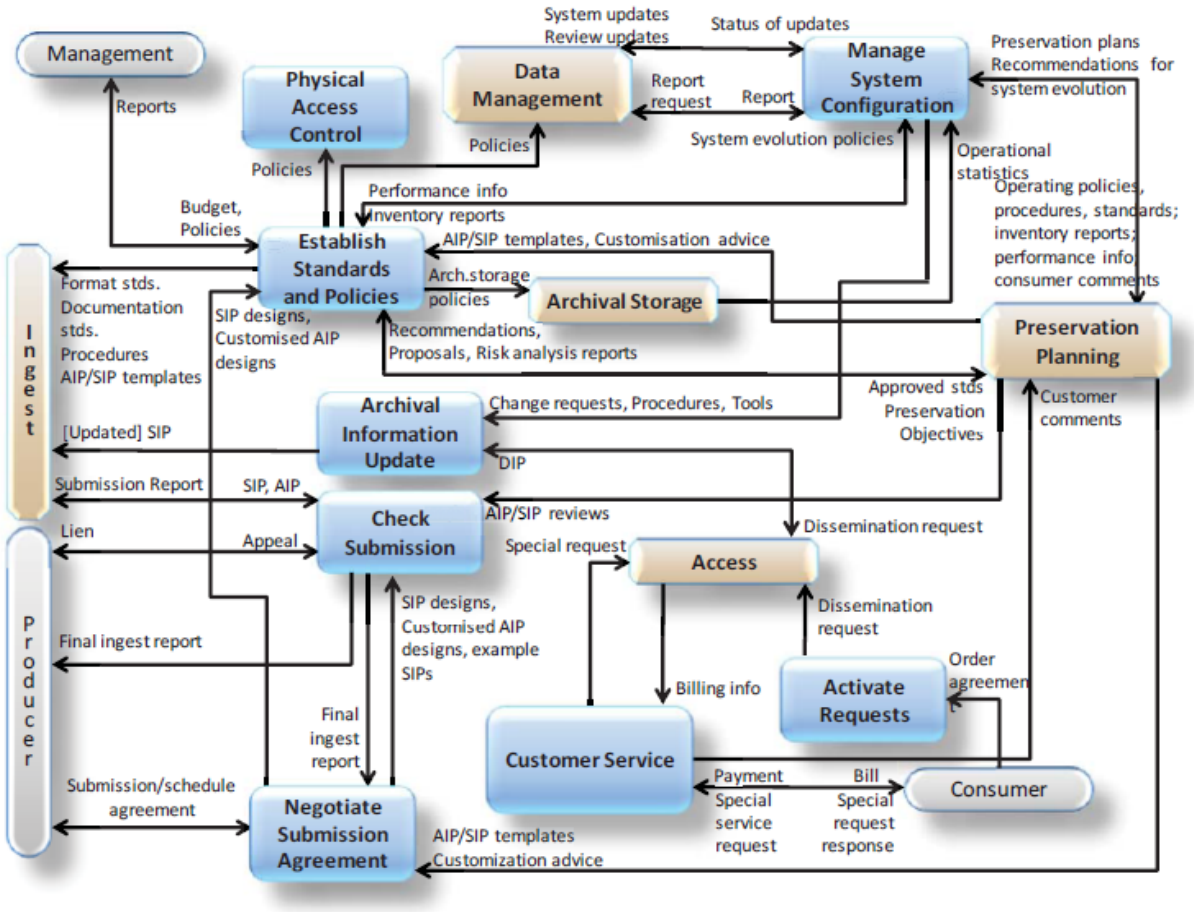
As funções de armazenamento de arquivo incluem a recepção do AIP da entidade funcional de ingestão e adicionamento do mesmo no armazenamento permanente, gestão da hierarquia de armazenamento para responder às exigências de qualidade de serviço das entidades utilizadoras, refrescamento dos suportes nos quais estão armazenados as informações custodiadas pelo Arquivo OAIS, realização de verificações de rotina e de erro, fornecimento de recursos para recuperação de desastres e envio do AIP para a entidade funcional de Acesso para resolução de encomendas.

DATA MANAGEMENT



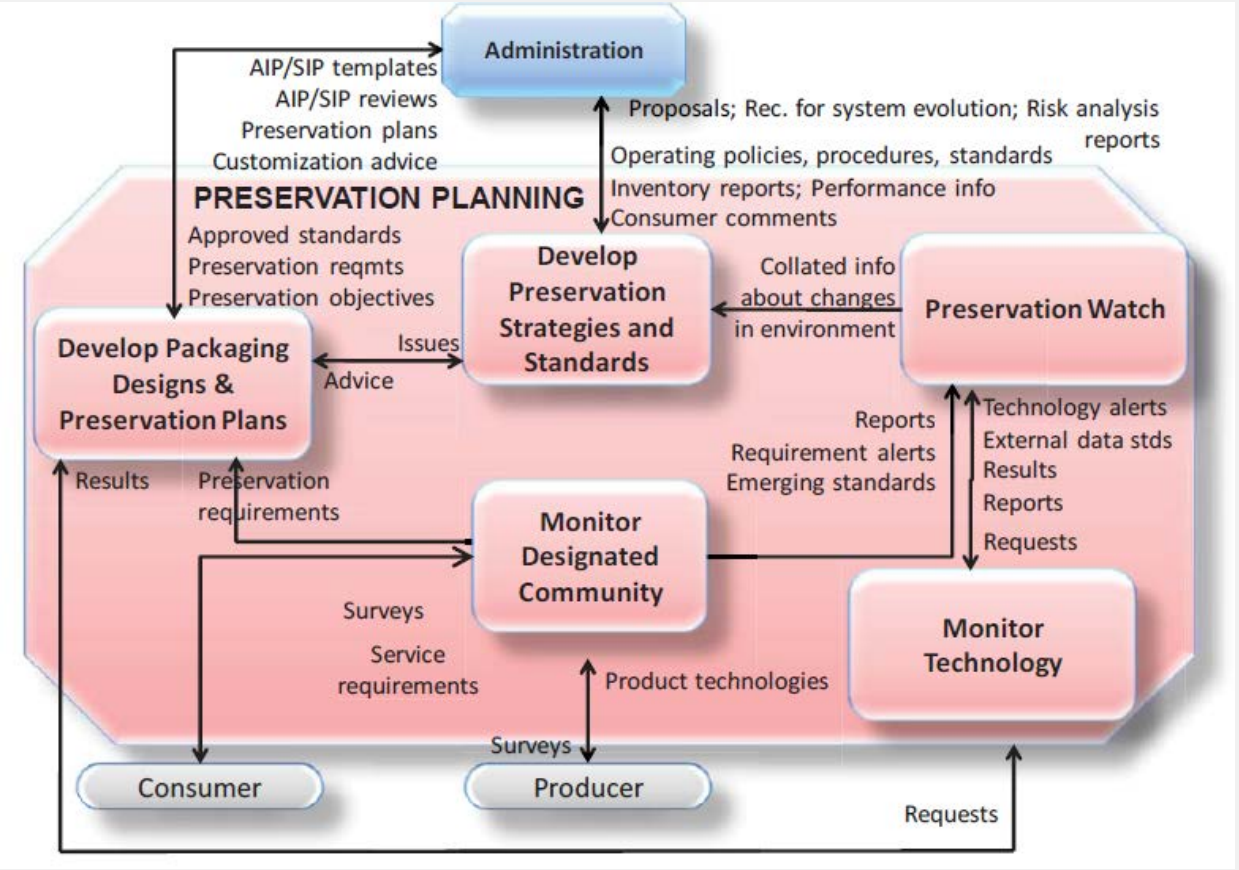
Fornece os serviços e funções de preenchimento, manutenção e acesso à Informação Descritiva que identifica e documenta a informação custodiada pelo Arquivo e dados administrativos utilizados para gerir o Arquivo OAIS. As funções de gestão de dados incluem a administração da base de dados do arquivo OAIS (mantendo as definições de esquema e de visualização e integridade referencial), realização das atualizações à base de dados (carregamento de nova Informação Descritiva ou dados administrativos do Arquivo), realização de consultas sobre os dados de gestão de dados para gerar respostas a consultas e elaboração de relatórios a partir das respostas à consultas.

ADMINISTRATION



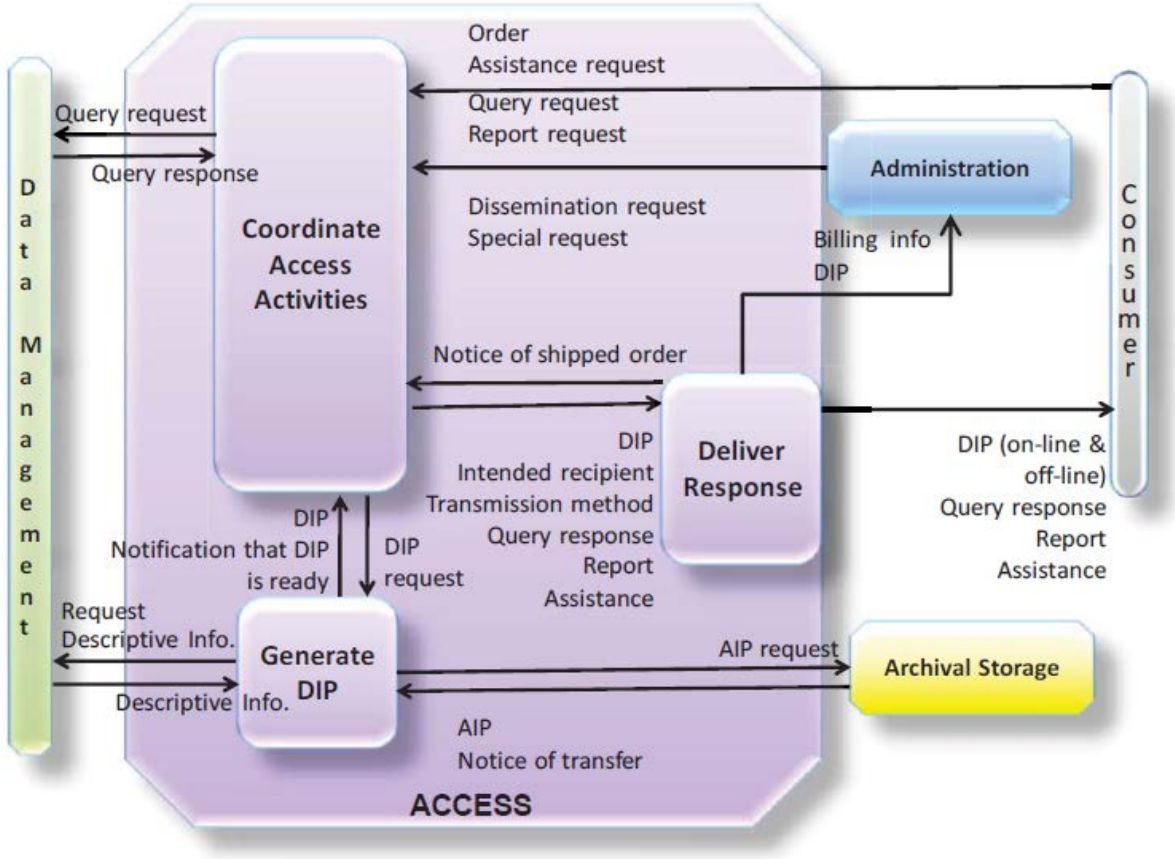
As funções de administração incluem a solicitação e negociação de acordos de submissão com os produtores, auditoria de submissões para assegurar que cumprem as normas do Arquivo, controle e fornecimento de mecanismos para restringir ou permitir o acesso físico (portas, fechaduras, guardas) a elementos do arquivo, conforme determinado pelas políticas de arquivo. As funções de engenharia de sistemas incluem a manutenção da gestão de configuração do *hardware* e *software* do sistema, monitorizar e aperfeiçoar as operações do arquivo, inventariar, reportar e migrar/atualizar os conteúdos do arquivo. Outras funções incluem o estabelecimento e manutenção de normas e políticas de arquivo, fornecimento de suporte ao cliente, ativar pedidos/solicitações armazenadas.

PRESERVATION PLANNING



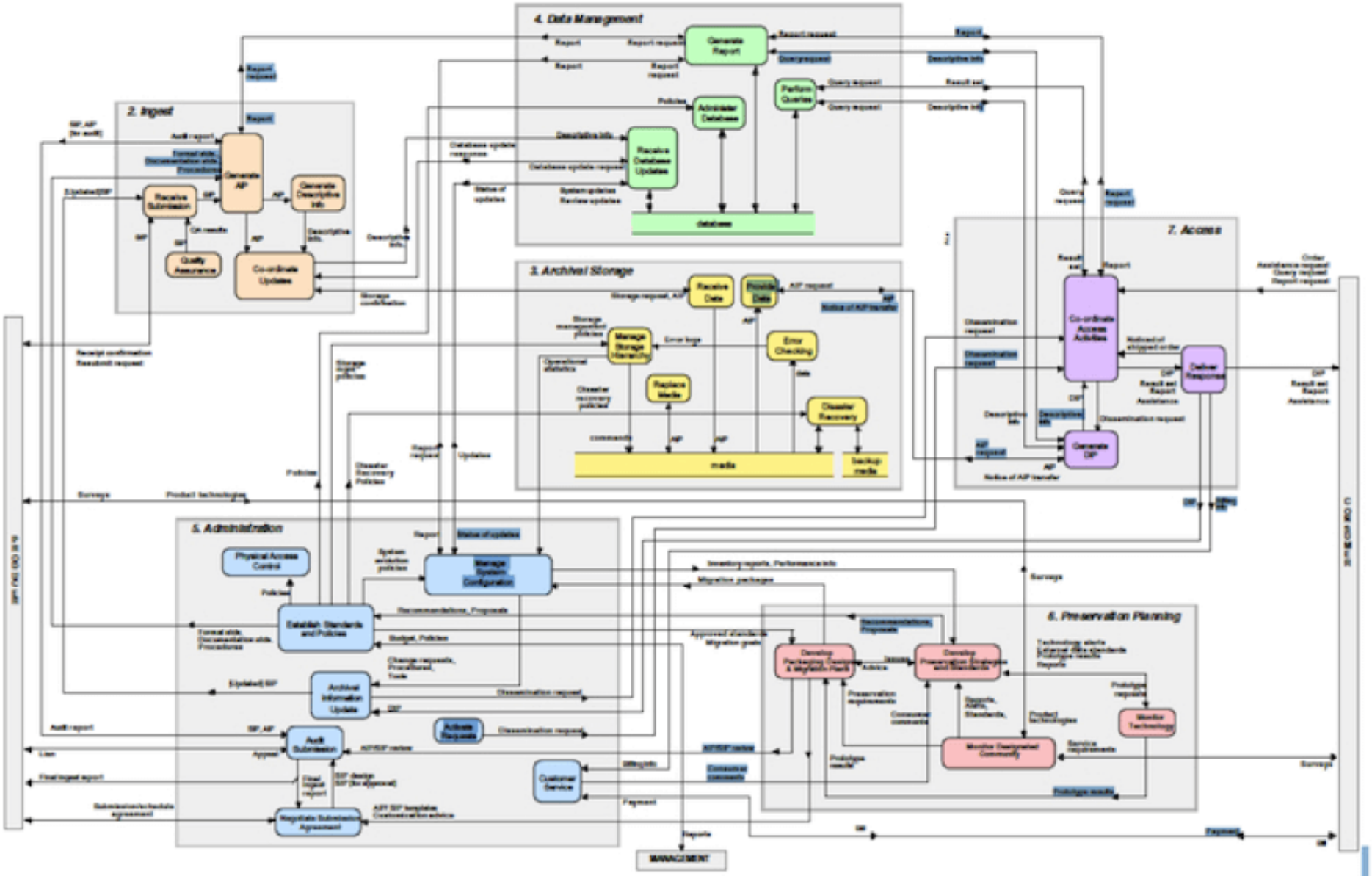
Fornece os serviços e funções de monitorização do ambiente envolvente do OAIS e fornecimento de recomendações e planos de preservação para assegurar que a informação armazenada no OAIS permaneça acessível e compreensível pela Comunidade Designada a longo prazo, mesmo que o ambiente informático inicial se tiver tornado obsoleto.

ACCESS



Fornece os serviços e funções de apoio aos consumidores na verificação da existência, descrição, localização e disponibilidade das informações armazenadas no OAIS e permite aos consumidores a solicitação e recepção de produtos de informação.

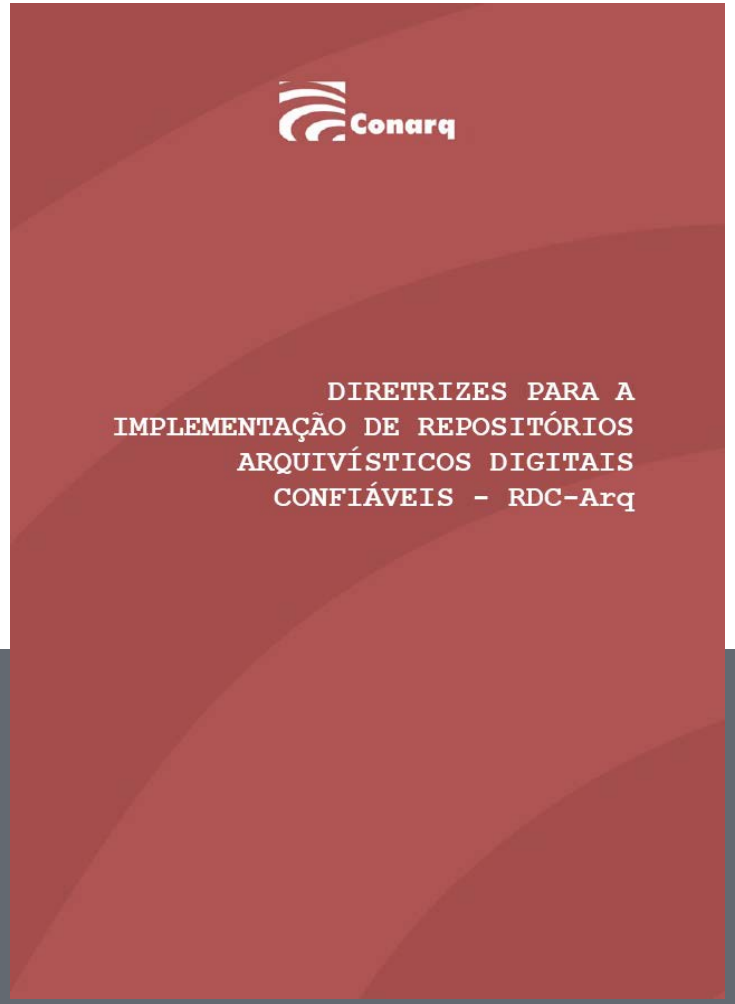
ENTIDADES FUNCIONAIS

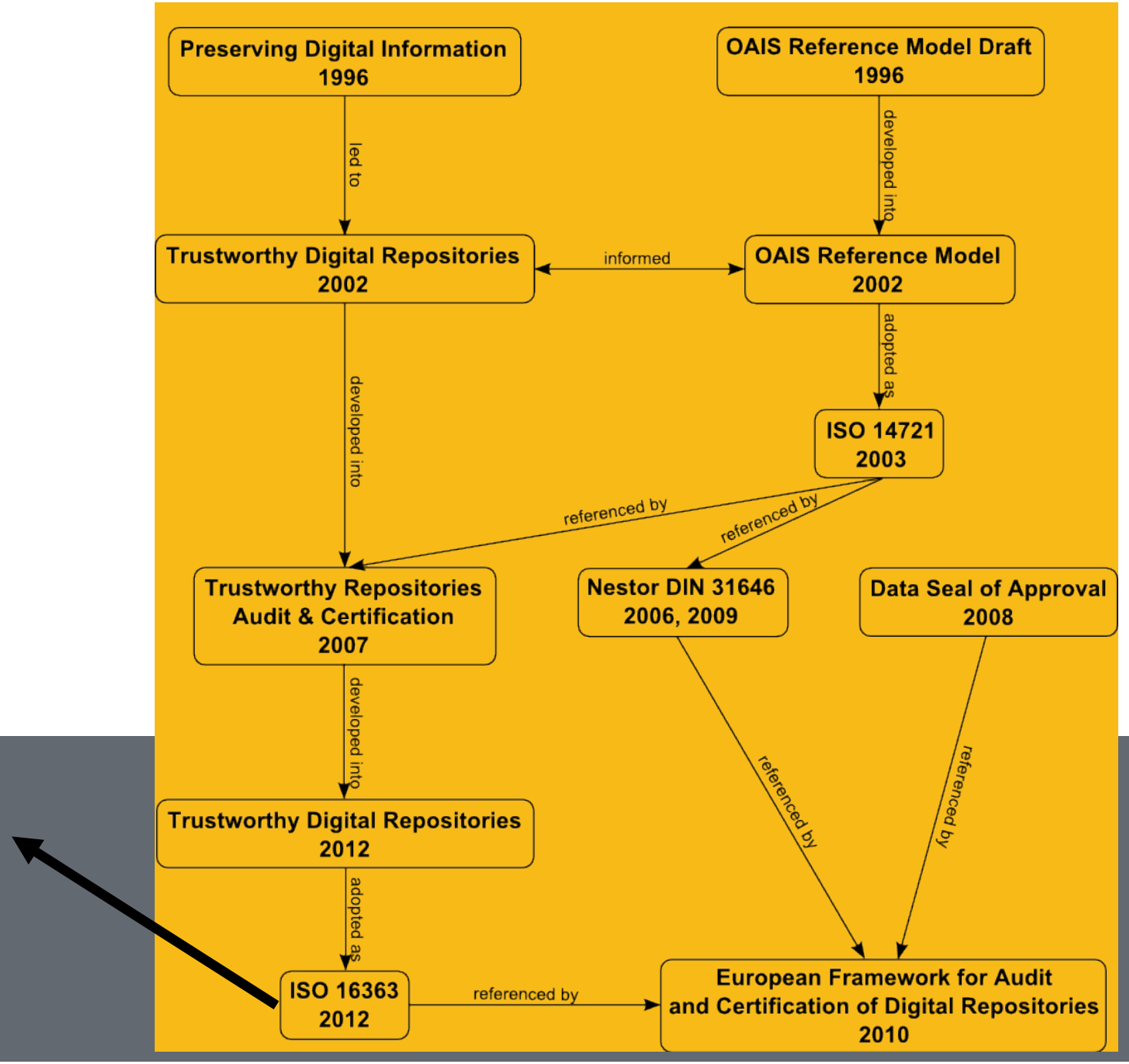


NORMAS

CERTIFICAÇÃO E CONFIABILIDADE

Normas


Conarq
DIRETRIZES PARA A IMPLEMENTAÇÃO DE REPOSITÓRIOS ARQUIVÍSTICOS DIGITAIS CONFIÁVEIS - RDC-Arq


Preserving Digital Information 1996
OAIS Reference Model Draft 1996
led to
developed into
Trustworthy Digital Repositories 2002
informed
OAIS Reference Model 2002
developed into
adopted as
ISO 14721 2003
referenced by
referenced by
Trustworthy Repositories Audit & Certification 2007
Nestor DIN 31646 2006, 2009
Data Seal of Approval 2008
developed into
referenced by
referenced by
Trustworthy Digital Repositories 2012
adopted as
ISO 16363 2012
referenced by
European Framework for Audit and Certification of Digital Repositories 2010

RLG/CPA Task Force on Archiving of Digital Information (1996)

"Para garantir a longevidade da informação, talvez o papel mais importante na operação de um arquivo digital seja gerenciar a identidade, integridade e qualidade dos próprios arquivos como uma fonte confiável de registro cultural. Os usuários de informações arquivadas em formato eletrônico e de serviços de arquivamento relacionados a essas informações precisam ter a garantia de que um arquivo digital é o que diz ser e de que as informações nele armazenadas são seguras por um longo prazo."

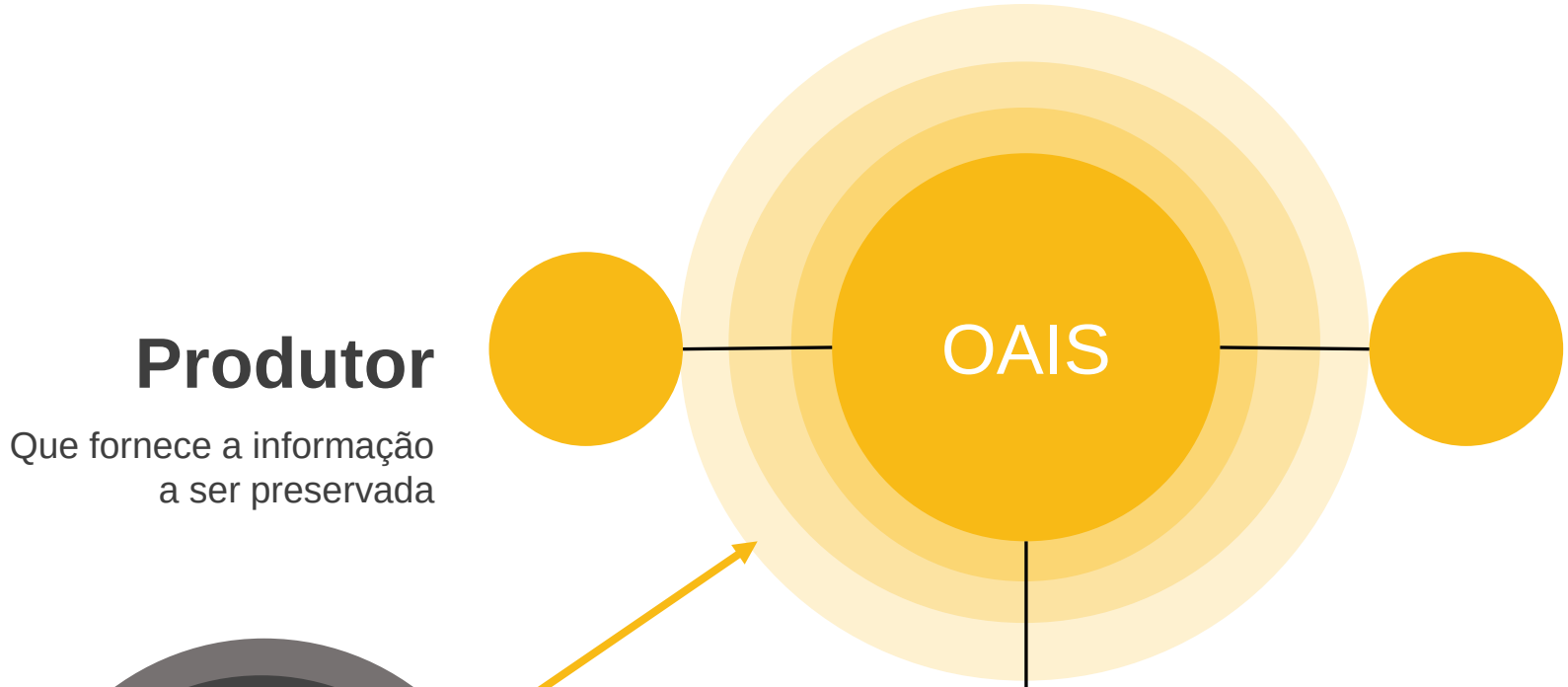
Trusted Digital Repositories: Attributes and Responsibilities

No âmbito dos repositórios digitais confiáveis, se aplicam três níveis de confiança:

1. Como as instituições culturais conquistam a confiança das suas comunidades designadas;
2. Como as instituições culturais confiam nos fornecedores externos;
3. Como os utilizadores confiam nos documentos que lhes são fornecidos por um repositório.

"A trusted digital repository is one whose mission is to provide reliable, long-term access to managed digital resources to its designated community, now and in the future."

Ambiente Externo



Produtor

Que fornece a informação a ser preservada

Consumidor

que procura e adquire informação que se encontra preservada no arquivo OAIS

ISO 16919

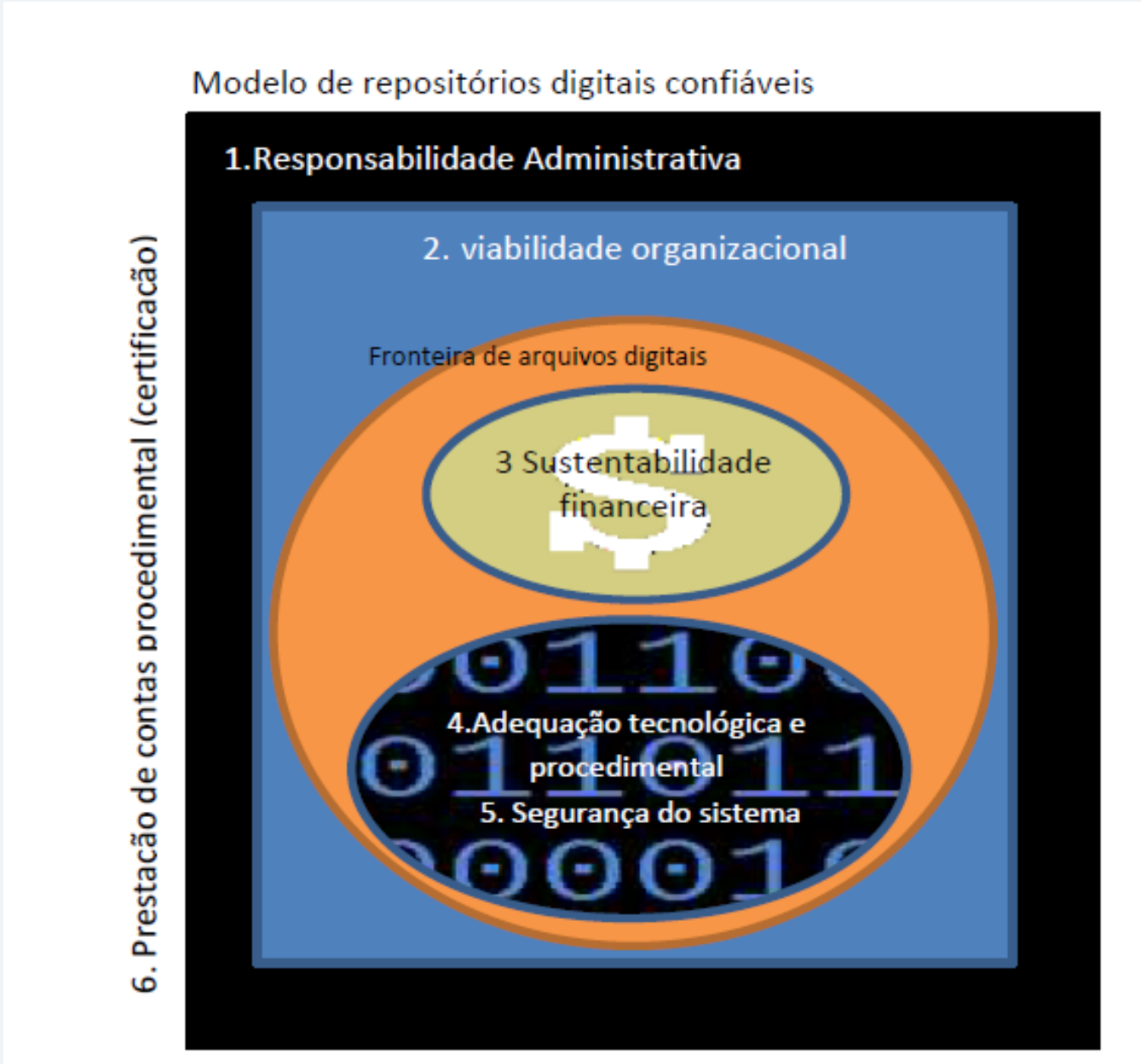
Certificador

ISO 17021

Administrador

Administrador fornece a política geral do arquivo OAIS e efetua o controle de gestão

Acreditador

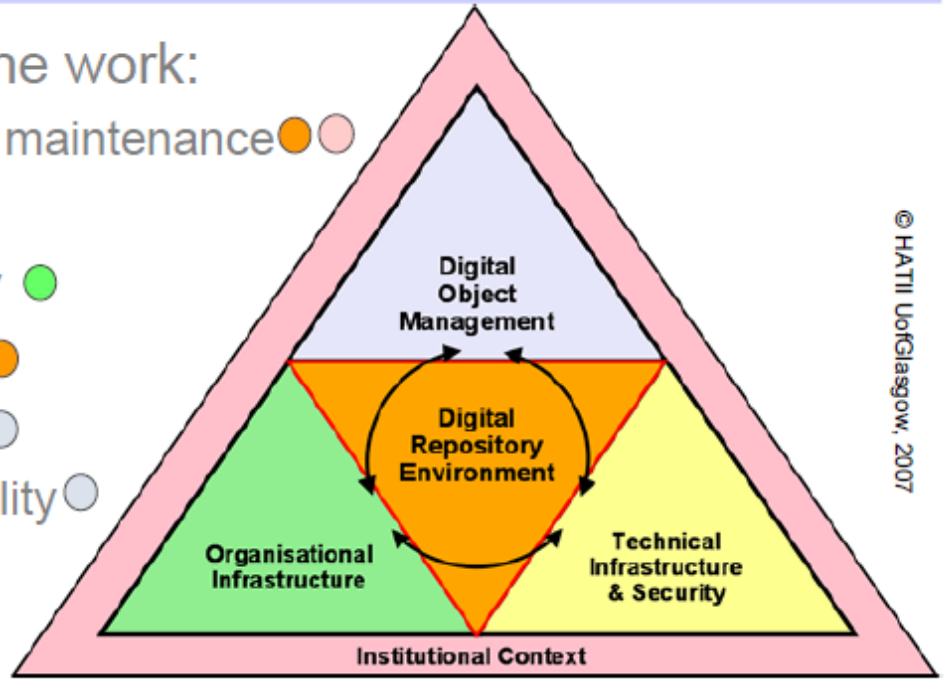


Modelo de Cornell

O *Trusted Digital Repositories: Attributes and Responsibilities*

10 Characteristics of Digital Repositories

- An intellectual context for the work:
  - Commitment to digital object maintenance
  - Organisational fitness
  - Legal & regulatory legitimacy
  - Effective & efficient policies
  - Acquisition & ingest criteria
  - Integrity, authenticity & usability
  - Audit trail and metadata
  - Dissemination
  - Preservation planning & action
  - Adequate technical infrastructure



(CRL/OCLC/NESTOR/DPE/DCC meeting, January 2007)

ISO 16.363

Infraestrutura Organizacional

3

Questões relativas a políticas institucionais direcionadas a preservação, que delineiam o planejamento e funcionamento legal da instituição.

Aspectos organizacionais e técnicos relacionados a ingestão, aquisição dos conteúdos digitais, geração dos pacotes, estratégias de preservação, entidades funcionais, metadados e etc.

4

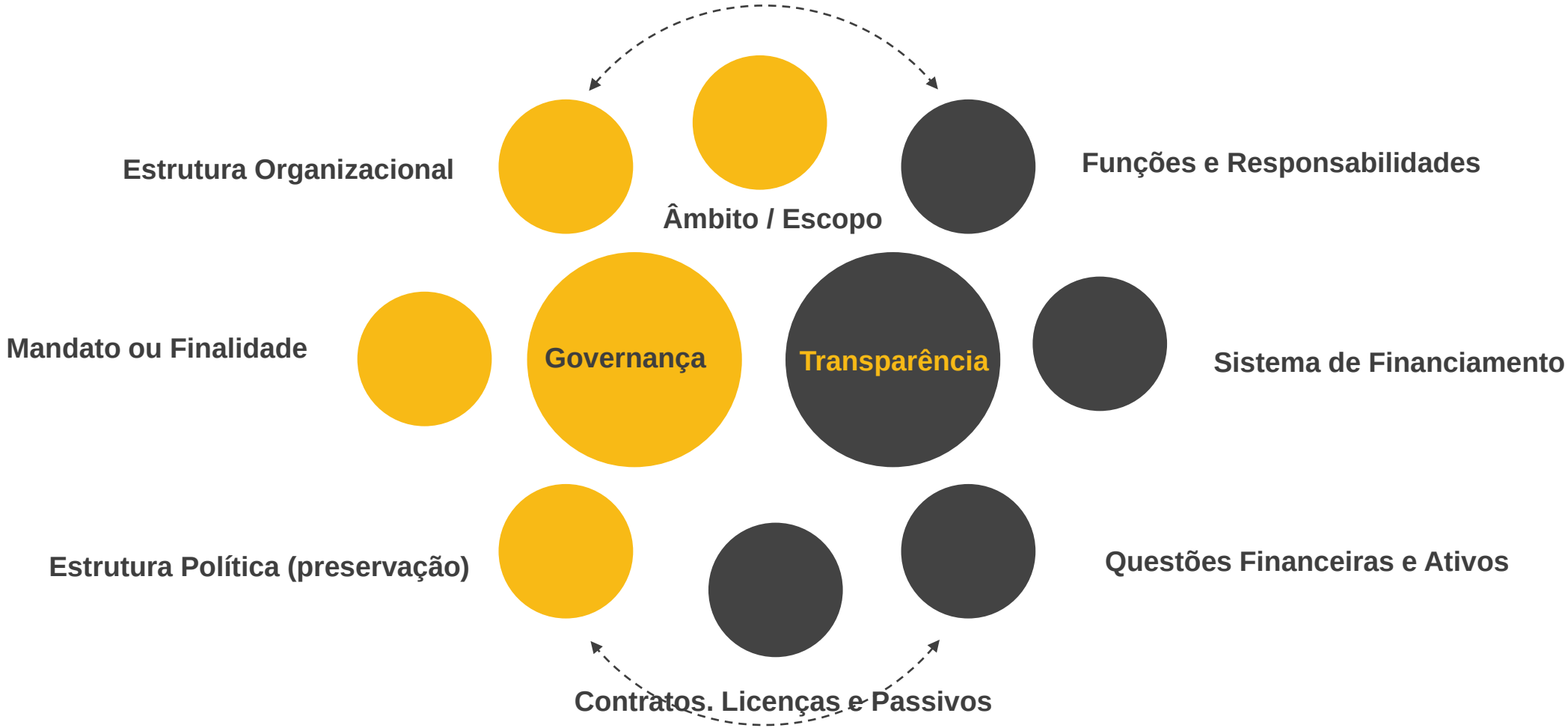
Gestão do Objeto Digital

Gestão de Riscos da Infraestrutura e de Segurança

5

Infraestrutura e as tecnologias no âmbito da gestão de risco da infraestrutura técnica e aborda a Segurança também na perspectiva da Gestão de Risco.

Infraestrutura Organizacional



3.1 Governança e viabilidade organizacional

3.1.1 O repositório deve ter uma declaração de missão que reflita um compromisso com a preservação, retenção de longo prazo, gerenciamento e acesso às informações digitais.

Declaração de missão ou estatuto do repositório ou de sua organização controladora que aborde especificamente ou implique implicitamente a preservação de informações e/ou outros recursos sob sua supervisão; um mandato regulamentar legal, estatutário ou governamental aplicável ao repositório que aborda especificamente ou requer implicitamente a preservação, retenção, gestão e acesso a informações e/ou outros recursos sob sua alçada.

3.1.2 O repositório deve ter um Plano Estratégico de Preservação que define a abordagem que o repositório terá no suporte de longo prazo de sua missão.

Plano Estratégico de Preservação; atas de reuniões; documentação das decisões administrativas tomadas.

3.1 Governança e viabilidade organizacional

3.1.2.1 O repositório deve ter um plano de sucessão, planos de contingência e/ou acordos de custódia adequados no caso de o repositório deixar de operar ou a instituição governante ou de financiamento alterar substancialmente o seu âmbito.

Sucessão escrita e confiável e plano(s) de contingência; declaração explícita e específica documentando a intenção de garantir a continuidade do repositório e as medidas a serem tomadas para garantir a continuidade; custódia de código crítico, software e metadados suficientes para permitir a reconstituição do repositório e seu conteúdo em caso de falha do repositório.

3.1.2.2 O repositório deve monitorar seu ambiente organizacional para determinar quando executar seu plano de sucessão, planos de contingência e/ou acordos de custódia.

Políticas administrativas, procedimentos, protocolos, requisitos; orçamentos e documentos de análise financeira; calendários fiscais; Planos de negócios; qualquer evidência de monitoramento ativo.

3.1 Governança e viabilidade organizacional

3.1.3 O repositório deve ter uma Política de Coleta ou outro documento que especifique o tipo de informação que irá preservar, reter, gerenciar e fornecer acesso.

Política de aquisição e documentos de suporte; Política de preservação, missão, objetivos e visão do repositório.

3.2 Estrutura Organizacional e Pessoal

3.2.1 O repositório deve ter uma Política de Coleta ou outro documento que especifique o tipo de informação que irá preservar, reter, gerenciar e fornecer acesso.

O repositório deve ter identificado e estabelecido as funções que precisa desempenhar e deve ter nomeado pessoal com habilidades e experiência adequadas para cumprir essas funções.

3.2.1.1 O repositório deve ter identificado e estabelecido as funções que precisa cumprir.

Um plano de pessoal; definições de competência; descrições de emprego; planos de desenvolvimento profissional da equipe; certificados de treinamento e credenciamento; além da evidência de que o repositório analisa e mantém esses documentos conforme os requisitos evoluem.

3.2.1.2 O repositório deve ter o número adequado de funcionários para apoiar todas as funções e serviços.

Organogramas; definições de papéis e responsabilidades; comparação dos níveis de pessoal com benchmarks e padrões do mercado.

3.2 Estrutura Organizacional e Pessoal

3.2.1.3 O repositório deve ter implementado um programa de desenvolvimento profissional ativo que forneça à equipe oportunidades de desenvolvimento de habilidades e conhecimentos.

Planos e relatórios de desenvolvimento profissional; requisitos de treinamento e orçamentos de treinamento, documentação de despesas de treinamento (valor por equipe); metas de desempenho e documentação das atribuições e realizações da equipe, cópias dos certificados concedidos.

3.3 Políticas de Responsabilidade (*Accountability*) e Preservação

3.3.1 O repositório deve ter definido a sua comunidade designada e a(s) base(s) de conhecimento associada(s) e deve ter essas definições devidamente acessíveis.

Como?

Uma definição escrita da Comunidade Designada.

3.3.2 O repositório deve ter Políticas de Preservação em vigor para garantir que seu Plano Estratégico de Preservação seja atendido.

Políticas de preservação; Declaração da missão do repositório.

3.3.2.1 O repositório deve ter mecanismos para revisão, atualização e desenvolvimento contínuo de suas Políticas de Preservação à medida que o repositório cresce e a tecnologia e a prática da comunidade evoluem.

Documentação escrita atual e anterior na forma de Políticas de Preservação, Planos Estratégicos de Preservação e Planos de Implementação de Preservação, procedimentos, protocolos e fluxos de trabalho; especificações de ciclos de revisão para documentação; documentação detalhando revisões, pesquisas e feedback. Se a documentação estiver embutida na lógica do sistema, a funcionalidade deve demonstrar a implementação de políticas e procedimentos.

3.3 Políticas de Responsabilidade (*Accountability)* e Preservação

3.3.3 O repositório deve ter um histórico documentado das mudanças em suas operações, procedimentos, software e hardware.

Inventário de bens de capital; documentação de aquisição, implementação, atualização e retirada de software e hardware de repositório crítico; retenção de arquivos e cronogramas e políticas de descarte, cópias de versões anteriores de políticas e procedimentos; minutas de encontros.

3.3.4 O repositório deve se comprometer com a transparência e responsabilidade em todas as ações de apoio à operação e gestão do repositório que afetem a preservação do conteúdo digital ao longo do tempo.

Relatórios de auditorias e certificações financeiras e técnicas; divulgação de documentos de governança, revisões de programas independentes e contratos e acordos com fornecedores de financiamento e serviços essenciais.

3.3 Políticas de Responsabilidade (*Accountability*) e Preservação

3.3.5 O repositório deve definir, coletar, rastrear e fornecer adequadamente suas medições de integridade de informações.

Definição ou especificação escrita das medidas de integridade do repositório (por exemplo, soma de verificação calculada ou valor de hash); documentação dos procedimentos e mecanismos para monitorar as medições de integridade e para responder aos resultados das medições de integridade que indicam que o conteúdo digital está em risco; um processo de auditoria para coletar, rastrear e apresentar medições de integridade; Política de preservação e documentação do fluxo de trabalho.

3.3.6 O repositório deve se comprometer com um cronograma regular de autoavaliação e certificação externa.

Listas de verificação preenchidas e datadas de autoavaliações e/ou auditorias de terceiros; certificados concedidos para conformidade com os padrões ISO relevantes; cronogramas e evidências de alocações orçamentárias adequadas para certificação futura.

3.4 Sustentabilidade Financeira

3.4.1 O repositório deve ter processos de planejamento de negócios de curto e longo prazo em vigor para sustentar o repositório ao longo do tempo.

Planos estratégicos, operacionais e/ou de negócios atualizados e plurianuais; demonstrações financeiras anuais auditadas; previsões financeiras com múltiplos cenários de orçamento; planos de contingência; análise de mercado.

3.4.2 O repositório deve ter práticas e procedimentos financeiros transparentes, em conformidade com as normas e práticas de contabilidade relevantes e auditados por terceiros de acordo com os requisitos legais territoriais.

Requisitos de disseminação demonstrados para planejamento e práticas de negócios; citações e/ou exemplos de requisitos, normas e práticas de contabilidade e auditoria; demonstrações financeiras anuais auditadas.

3.4 Sustentabilidade Financeira

3.4.3 O repositório deve ter um compromisso contínuo de analisar e relatar riscos, benefícios, investimentos e despesas financeiras (incluindo ativos, licenças e passivos).

Documentos de gerenciamento de risco que identificam ameaças percebidas e potenciais e respostas planejadas ou implementadas (um registro de risco); documentos de planejamento de investimento em infraestrutura de tecnologia; análises de custo/benefício; documentos e carteiras de investimentos financeiros; requisitos e exemplos de licenças, contratos e gerenciamento de ativos; evidência de revisão com base no risco.

3.5 Contratos, Licenças e Passivos

3.5.1 O repositório deve ter e manter contratos apropriados ou acordos de depósito para materiais digitais que gerencia, preserva e/ou aos quais fornece acesso.

Contratos e licenças de depósito devidamente assinados e executados de acordo com as leis e regulamentos locais, nacionais e internacionais; políticas sobre acordos de depósito de terceiros;
definições de níveis de serviço e usos permitidos; políticas de repositório sobre o tratamento de "obras órfãs" e resolução de disputas de direitos autorais; relatórios de avaliações de risco independentes dessas políticas; procedimentos para revisar e manter regularmente acordos, contratos e licenças.

3.5.1.1 O repositório deve ter contratos ou acordos de depósito que especifiquem e transfiram todos os direitos de preservação necessários, e esses direitos transferidos devem ser documentados.

Contratos, acordos de depósito; especificação(ões) de direitos transferidos para diferentes tipos de conteúdo digital (se aplicável); declarações de política sobre os direitos de preservação necessários.

3.5 Contratos, Licenças e Passivos

3.5.1.2 O repositório deve ter especificado todos os aspectos apropriados de aquisição, manutenção, acesso e retirada em acordos escritos com depositantes e outras partes relevantes.

Contratos de submissão, contratos de depósito e atos de doação executados adequadamente; procedimentos operacionais padrão escritos.

3.5.1.3 O repositório deve ter políticas escritas que indiquem quando ele aceita a responsabilidade pela preservação do conteúdo de cada conjunto de objetos de dados enviados.

Contratos de submissão, contratos de depósito e atos de doação executados adequadamente; recibo de confirmação enviado de volta ao produtor/depositante.

3.5.1.4 O repositório deve ter políticas em vigor para lidar com responsabilidades e desafios de propriedade/direitos.

Uma definição de direitos, licenças e permissões a serem obtidos de produtores e contribuidores de conteúdo digital; citações de leis e regulamentos relevantes; política de resposta aos desafios; histórico documentado para responder aos desafios de maneiras que não inibam a preservação; registros de aconselhamento jurídico relevante procurado e recebido.

3.5 Contratos, Licenças e Passivos

3.5.1.4 O repositório deve ter políticas em vigor para lidar com responsabilidades e desafios de propriedade/direitos.

Uma definição de direitos, licenças e permissões a serem obtidos de produtores e contribuidores de conteúdo digital; citações de leis e regulamentos relevantes; política de resposta aos desafios; histórico documentado para responder aos desafios de maneiras que não inibam a preservação; registros de aconselhamento jurídico relevante procurado e recebido.

3.5.2 O repositório deve rastrear e gerenciar os direitos de propriedade intelectual e as restrições ao uso do conteúdo do repositório, conforme exigido pelo acordo de depósito, contrato ou licença.

Uma declaração de Política de Preservação que define e especifica os requisitos do repositório e o processo de gerenciamento de direitos de propriedade intelectual; acordos de depositantes; amostras de acordos e outros documentos que especificam e tratam dos direitos de propriedade intelectual; documentação de monitoramento por repositório ao longo do tempo de mudanças no status e propriedade intelectual em conteúdo digital mantido pelo repositório; resultados do monitoramento, metadados que capturam informações de direitos.

4 GESTÃO DE OBJETOS DIGITAIS

4.1 INGEST: AQUISIÇÃO DE CONTEÚDO

4.1.1 O repositório deve identificar as Informações do Conteúdo e as Propriedades da Informação que o repositório irá preservar.

Declaração de missão; acordos de submissão / acordos de depósito / títulos de doação; documentos de fluxo de trabalho e Política de Preservação, incluindo definição por escrito de propriedades conforme acordado no contrato de depósito / escritura de doação; procedimentos de processamento escritos; documentação das propriedades a serem preservadas.

4.1.1.1 O repositório deve ter procedimento (s) para identificar as Propriedades da Informação que irá preservar.

Definições das Propriedades da Informação que devem ser preservadas; acordos de submissão / acordos de depósito, políticas de preservação, procedimentos de processamento por escrito, documentação de fluxo de trabalho.

4.1.1.2 O repositório deve ter um registro das Informações do Conteúdo e das Propriedades da Informação que irá preservar.

Políticas de preservação, manuais de processamento, inventários ou pesquisas de coleção, registros de tipos de informações de conteúdo, estratégias de preservação adquiridas e planos de ação.

4.1 INGEST: AQUISIÇÃO DE CONTEÚDO

4.1.2 O repositório deve especificar claramente as informações que precisam ser associadas às Informações de Conteúdo específico no momento de seu depósito.

Requisitos de transferência; acordos produtor-arquivo; planos de fluxo de trabalho para produzir o AIP.

4.1.3 O repositório deve ter especificações adequadas que permitam o reconhecimento e a análise dos SIPs.

Informações de pacote para os SIPs; Informações de representação para os dados de conteúdo SIP, incluindo especificações de formato de arquivo documentado; padrões de dados publicados; documentação da construção de objetos válidos.

4.1.4 O repositório deve ter mecanismos para verificar adequadamente a identidade do Produtor de todos os materiais.

Acordos de submissão / acordos de depósito / títulos de doação juridicamente vinculativos, evidência de medidas tecnológicas apropriadas; logs de procedimentos e autenticações.

4.1.5 O repositório deve ter um processo de ingestão que verifica cada SIP quanto à integridade e exatidão.

Política de preservação apropriada e documentos do plano de implementação de preservação e arquivos de log do sistema do(s) sistema(s) que executam o(s) procedimento(s) de ingestão; logs ou registros de arquivos recebidos durante o processo de transferência e ingestão; documentação de procedimentos operacionais padrão, procedimentos detalhados e/ou fluxos de trabalho; registros de formato; definições de integridade e exatidão

4.1 INGEST: AQUISIÇÃO DE CONTEÚDO

4.1.6 O repositório deve obter controle suficiente sobre os Objetos Digitais para preservá-los.

Documentos que mostram o nível de controle que o repositório realmente possui. Um banco de dados / catálogo de metadados separado listando todos os objetos digitais no repositório e metadados suficientes para validar a integridade desses objetos (tamanho do arquivo, checksum, hash, localização, número de cópias, etc.)

4.1.7 O repositório deve fornecer ao produtor/depositante as respostas adequadas nos pontos acordados durante os processos de ingestão.

Acordos de envio / acordos de depósito / títulos de doação; documentação de fluxo de trabalho; procedimentos operacionais padrão; evidência de ‘reportar’, como relatórios, correspondência, memorandos ou e-mails.

4.1.8 O repositório deve ter registros atualizados de ações e processos de administração que sejam relevantes para a aquisição de conteúdo.

Documentação escrita das decisões e/ou ações tomadas; metadados de preservação registrados, armazenados e vinculados a objetos digitais pertinentes, recibos de confirmação enviados de volta aos fornecedores.

4.2 INGEST: CRIAÇÃO DO AIP

4.2.1 O repositório deve ter para cada AIP ou classe de AIPs preservado pelo repositório uma definição associada que seja adequada para analisar o AIP e adequada para necessidades de preservação de longo prazo.

Informações documentadas sobre as definições associadas ao AIP, incluindo informações de empacotamento que possam sempre ser encontradas, processadas e gerenciadas dentro do arquivo.

4.2.1.1 O repositório deve ser capaz de identificar qual definição se aplica a qual AIP.

Documentação que liga claramente cada AIP, ou classe de AIPs, à sua definição.

4.2.1.2 O repositório deve ter uma definição de cada AIP que seja adequada para preservação de longo prazo, permitindo a identificação e análise de todos os componentes necessários dentro daquele AIP.

Demonstração do uso das definições para extrair informações de conteúdo e PDI (procedência, direitos de acesso, contexto, referência e informações de fixidez) de AIPs. Deve-se notar que a proveniência de um objeto digital, por exemplo, pode ser estendida ao longo do tempo para refletir ações adicionais de preservação.

4.2 INGEST: CRIAÇÃO DO AIP

4.2.2 O repositório deve ter uma descrição de como os AIPs são construídos a partir dos SIPs.

Documentos de descrição do processo; documentação da relação SIP-AIP; documentação clara de como os AIPs são derivados dos SIPs.

4.2.3 O repositório deve documentar a disposição final de todos os SIPs.

Documentos que registram os procedimentos relativos ao tratamento dos SIPs para indicar sua localização como AIPs ou mesmo sua eliminação.

4.2.3.1 O repositório deve seguir procedimentos documentados se um SIP não for incorporado a um AIP ou descartado e deve indicar porque o SIP não foi incorporado ou descartado.

Arquivos de processamento do sistema; registros de descarte; acordos/escrituras de doadores ou depositantes; sistema de rastreamento de proveniência; arquivos de log do sistema; documentos de descrição do processo; documentação da relação SIP com AIP; documentação clara de como os AIPs são derivados dos SIPs; documentação do padrão/processo contra o qual ocorre a normalização; documentação do resultado da normalização e como o AIP resultante é diferente do(s) SIP(s).

4.2.4 O repositório deve ter e usar uma convenção que gere identificadores únicos e persistentes para todos os AIPs.

4.2 INGEST: CRIAÇÃO DO AIP

4.2.4.1 O repositório deve identificar exclusivamente cada AIP dentro do repositório.

4.2.4.1.1 O repositório deve ter identificadores únicos.

4.2.4.1.2 O repositório deve atribuir e manter identificadores persistentes do AIP e seus componentes de forma a serem únicos no contexto do repositório.

4.2.4.1.3 A documentação deve descrever quaisquer processos usados para mudanças em tais identificadores.

4.2.4.1.4 O repositório deve ser capaz de fornecer uma lista completa de todos esses identificadores e fazer verificações pontuais para duplicações.

4.2.4.1.5 O sistema de identificadores deve ser adequado para atender aos requisitos atuais e futuros previsíveis do repositório, como o número de objetos.

Documentação que descreve a convenção de nomenclatura e a evidência física de sua aplicação (por exemplo, registros).

4.2 INGEST: CRIAÇÃO DO AIP

4.2.4.2 O repositório deve ter um sistema de serviços de ligação/resolução confiáveis, a fim de encontrar o objeto identificado exclusivamente, independentemente de sua localização física.

Documentação que descreve a convenção de nomenclatura e a evidência física de sua aplicação (por exemplo, registros).

4.2 INGEST: CRIAÇÃO DO AIP

4.2.5 O repositório deve ter acesso às ferramentas e recursos necessários para fornecer informações de representação oficial para todos os objetos digitais que ele contém.

4.2.5.1 O repositório deve ter ferramentas ou métodos para identificar o tipo de arquivo de todos os Objetos de Dados enviados.

4.2.5.2 O repositório deve ter ferramentas ou métodos para determinar quais Informações de Representação são necessárias para tornar cada Objeto de Dados compreensível para a Comunidade Designada.

4.2.5.3 O repositório deve ter acesso às Informações de Representação necessárias.

4.2.5.4 O repositório deve ter ferramentas ou métodos para garantir que as Informações de Representação necessárias sejam persistentemente associadas aos Objetos de Dados relevantes.

Assinatura ou acesso a registros de Informações de Representação (incluindo registros de formato); registros visíveis em registros locais (com links persistentes para objetos digitais); registros de banco de dados que incluem informações de representação e um link persistente para objetos digitais relevantes.

4.2 INGEST: CRIAÇÃO DO AIP

4.2.6 O repositório deve ter processos documentados para adquirir Informações de Descrição de Preservação (PDI) para suas Informações de Conteúdo associadas e adquirir PDI de acordo com os processos documentados.

4.2.6.1 O repositório deve ter processos documentados para aquisição de PDI.

4.2.6.2 O repositório deve executar seus processos documentados para aquisição de PDI.

4.2.6.3 O repositório deve garantir que o PDI seja persistentemente associado às Informações de Conteúdo relevantes.

Procedimentos operacionais padrão; manuais que descrevem os procedimentos de ingestão; documentação visível sobre como o repositório adquire e gerencia Preservation Description Information (PDI); criação de checksum ou hash, consultando a comunidade designada sobre o contexto.

4.2 INGEST: CRIAÇÃO DO AIP

4.2.7 O repositório deve garantir que as informações de conteúdo dos AIPs sejam compreensíveis para a sua comunidade designada no momento da criação do AIP.

4.2.7.1 O repositório deve ter um processo documentado para testar a compreensibilidade para suas Comunidades Designadas das Informações de Conteúdo dos AIPs em sua criação.

4.2.7.2 O repositório deve executar o processo de teste para cada classe de Informações de Conteúdo dos AIPs.

4.2.7.3 O repositório deve trazer as Informações de Conteúdo do AIP até o nível exigido de compreensibilidade se falhar no teste de compreensibilidade.

Procedimentos de teste a serem executados em relação aos acervos digitais para garantir sua compreensibilidade para a comunidade designada definida; registros de tais testes sendo realizados e avaliados; evidências de coleta ou identificação de Informações de Representação para preencher quaisquer lacunas de inteligibilidade que tenham sido encontradas; retenção de indivíduos com experiência em disciplina.

4.2 INGEST: CRIAÇÃO DO AIP

4.2.8 O repositório deve verificar cada AIP quanto à integridade e exatidão no ponto em que é criado.

Descrição do procedimento que verifica se os AIPs estão completos e corretos; registros do procedimento.

4.2.9 O repositório deve fornecer um mecanismo independente para verificar a integridade da coleção/conteúdo do repositório.

Documentação fornecida para 4.2.1 a 4.2.4; acordos documentados negociados entre o produtor e o repositório (ver 4.1.1-4.1.8); registros de material recebido e datas de ação associada (recebimento, ação, etc.); logs de verificações periódicas.

4.2.10 O repositório deve ter registros contemporâneos de ações e processos de administração que sejam relevantes para a criação de AIP.

Documentação escrita das decisões e/ou ações realizadas com carimbo de data/hora; metadados de preservação registrados, armazenados e vinculados a objetos digitais pertinentes.

4.3 Planejamento de Preservação

4.3.1 O repositório deve ter estratégias de preservação documentadas relevantes para seus acervos.

Documentação que identifica cada risco de preservação identificado e a estratégia para lidar com esse risco.

4.3.2 O repositório deve ter mecanismos para monitorar seu ambiente de preservação.

Pesquisas da comunidade designada do repositório.

4.3.2.1 O repositório deve ter mecanismos para monitorar e notificar quando as informações de representação forem inadequadas para que a comunidade designada compreenda os acervos de dados.

Assinatura de serviço de registro de Informações de Representação; assinatura de um serviço de observação de tecnologia, pesquisas entre seus membros da Comunidade Designada, processos de trabalho relevantes para lidar com essas informações.

4.3.3 O repositório deve possuir mecanismos para alterar seus planos de preservação em decorrência de suas atividades de monitoramento.

Planos de preservação vinculados a vigilância(s) de tecnologia formal ou informal; planejamento ou processos de preservação programados para intervalos mais curtos (por exemplo, não mais de cinco anos); prova de atualizações frequentes de Políticas de Preservação e Planos de Preservação; seções das Políticas de Preservação que tratam de como os planos podem ser atualizados e da frequência com que os planos devem ser revisados e reafirmados ou atualizados.

4.3 Planejamento de Preservação

4.3.3.1 O repositório deve possuir mecanismos para a criação, identificação ou coleta de quaisquer Informações de Representação extras necessárias.

Assinatura de um serviço de registro de formato; assinatura de um serviço de observação de tecnologia; planos de preservação.

4.3.4 O repositório deve fornecer evidências da eficácia de suas atividades de preservação.

Coleta de metadados de preservação apropriados; prova de usabilidade de objetos digitais selecionados aleatoriamente mantidos dentro do sistema; histórico demonstrável para reter objetos digitais utilizáveis ao longo do tempo; pesquisas da comunidade designada.

4.4 PRESERVAÇÃO DO AIP

4.4.1 O repositório deve ter especificações de como os AIPs são armazenados até o nível de bits.

Documentação do formato dos AIPs; EAST e descrições de Linguagem de Especificação de Dicionário de Entidades de Dados (DEDSL) dos componentes de dados (consulte as referências [B6] e [B7]).

4.4.1.1 O repositório deve preservar as Informações de Conteúdo dos AIPs.

Documentação do procedimento de fluxo de trabalho de preservação; documentação do procedimento de fluxo de trabalho; Documentos da Política de Preservação que especificam o tratamento dos AIPs e sob quais circunstâncias eles podem ser excluídos; capacidade de demonstrar a sequência de conversões de um AIP para qualquer objeto digital específico ou grupo de objetos ingeridos; documentação que liga os objetos ingeridos e os AIPs atuais.

4.4.1.2 O repositório deve monitorar ativamente a integridade dos AIPs.

Informações de fixidez (por exemplo, CHECKSUM) para cada objeto digital / AIP ingerido; registros de verificações de fixidez; documentação de como as informações de AIPs e fixidez são mantidas separadas; documentação de como os AIPs e os registros de adesão são mantidos separados.

4.4.2 O repositório deve ter registros atualizados de ações e processos de administração que sejam relevantes para o armazenamento e preservação dos AIPs.

Documentação escrita das decisões e/ou ações tomadas; metadados de preservação registrados, armazenados e vinculados a objetos digitais pertinentes.

4.4 PRESERVAÇÃO DO AIP

4.4.2.1 O repositório deve ter procedimentos para todas as ações realizadas em AIPs.

Documentação escrita que descreve todas as ações que podem ser executadas em um AIP.

4.4.2.2 O repositório deve ser capaz de demonstrar que quaisquer ações tomadas em AIPs estavam em conformidade com a especificação dessas ações.

Metadados de preservação registrados, armazenados e vinculados a objetos digitais pertinentes e documentação dessa ação; auditorias procedimentais do repositório mostrando que todas as ações estão em conformidade com os processos documentados.

4.5 GESTÃO DE INFORMAÇÕES

4.5.1 O repositório deve especificar os requisitos mínimos de informação para permitir que a Comunidade Designada descubra e identifique o material de interesse.

Informações de recuperação e descritivas, metadados descritivos, como Dublin Core e outras documentações que descrevem o objeto.

4.5.2 O repositório deve capturar ou criar informações descritivas mínimas e garantir que esteja associado ao AIP.

Metadados descritivos; identificador ou localizador único persistente interno ou externo associado ao AIP (ver também 4.2.4 sobre identificador único e persistente); documentação do sistema e arquitetura técnica; acordos de depositantes; documentação da política de metadados, incorporando detalhes dos requisitos de metadados e uma declaração descrevendo onde recai a responsabilidade por sua aquisição; documentação do fluxo de trabalho do processo.

4.5.3 O repositório deve manter a ligação bidirecional entre cada AIP e suas informações descritivas.

Metadados descritivos; identificador ou localizador único e persistente associado ao AIP; relação documentada entre o AIP e seus metadados; documentação do sistema e arquitetura técnica; documentação do fluxo de trabalho do processo.

4.5.3.1 O repositório deve manter as associações entre seus AIPs e suas informações descritivas ao longo do tempo.

Registro detalhando a manutenção contínua ou verificação da integridade dos dados e suas relações com as informações descritivas associadas, especialmente após o reparo ou modificação do AIP; informações descritivas legadas; persistência do identificador ou localizador; relação documentada entre AIP e suas informações descritivas; documentação do sistema e arquitetura técnica; documentação do fluxo de trabalho do processo.

4.6 GESTÃO DE ACESSOS

4.6.1 O repositório deve cumprir as Políticas de Acesso.

Declarações de políticas que estão disponíveis para as comunidades de usuários; informações sobre as capacidades do usuário (matrizes de autenticação); logs e trilhas de auditoria de solicitações de acesso; testes explícitos de alguns tipos de acesso.

4.6.1.1 O repositório deve registrar e revisar todas as falhas e anomalias de gerenciamento de acesso.

Logs de acesso, capacidade do sistema de usar ferramentas automatizadas de análise/monitoramento e gerar mensagens de problemas/erros; notas de revisões realizadas ou ações tomadas como resultado das revisões.

4.6.2 O repositório deve seguir políticas e procedimentos que possibilitem a disseminação de objetos digitais rastreáveis aos originais, com evidências que comprovem sua autenticidade.

Documentos de *design* do sistema; instruções de trabalho (se os DIPs envolverem processamento manual); passo a passo do processo; produção de cópia de amostra com comprovação de autenticidade; documentação dos requisitos da comunidade para evidências de autenticidade.

4.6.2.1 O repositório deve registrar e agir sobre relatórios de problemas sobre erros em dados ou respostas de usuários.

Documentos de *design* do sistema; instruções de trabalho (se os DIPs envolverem processamento manual); passo a passo do processo; registros de pedidos e produção DIP; documentação de relatórios de erros e as ações tomadas.

5 GESTÃO DE RISCO DE INFRAESTRUTURA E SEGURANÇA

5.1 GESTÃO DE RISCO DE INFRAESTRUTURA TÉCNICA

5.1.1 O repositório deve identificar e gerenciar os riscos às suas operações de preservação e objetivos associados à infraestrutura do sistema.

Inventário de infraestrutura de componentes do sistema; avaliações periódicas de tecnologia; estimativas da vida útil dos componentes do sistema; exportação de registros autênticos para um sistema independente; uso de software fortemente suportado pela comunidade, por exemplo, Apache, iRODS, Fedora); recriação de arquivos a partir de backups.

5.1.1.1 O repositório deve empregar relógios de tecnologia ou outros sistemas de notificação de monitoramento de tecnologia.

Gerenciamento de relatórios periódicos de avaliação de tecnologia. Comparação da tecnologia existente para cada nova avaliação.

5.1.1.1.1 O repositório deve ter tecnologias de hardware adequadas aos serviços que fornece às comunidades designadas.

Manutenção de tecnologia, expectativas e perfis de uso atualizados da Comunidade Designada; fornecimento de largura de banda adequada para suportar demandas de ingestão e uso; elicitação sistemática de feedback sobre a adequação de hardware e serviço; manutenção de um inventário atual de hardware.

5.1.1.1.2 O repositório deve ter procedimentos em vigor para monitorar e receber notificações quando mudanças na tecnologia de hardware são necessárias.

Auditorias de capacidade *versus* uso real; auditorias de taxas de erro observadas; auditorias de gargalos de desempenho que limitam a capacidade de atender aos requisitos de acesso da comunidade de usuários; documentação de avaliações de observação de tecnologia; documentação de atualizações de tecnologia de fornecedores.

5.1 GESTÃO DE RISCO DE INFRAESTRUTURA TÉCNICA

5.1.1.1.3 O repositório deve ter procedimentos em vigor para avaliar quando mudanças são necessárias no hardware atual.

Procedimentos de avaliação implementados; experiência documentada da equipe em cada subsistema de tecnologia.

5.1.1.1.4 O repositório deve ter procedimentos, compromisso e financiamento para substituir o hardware quando a avaliação indicar a necessidade de fazê-lo.

Declaração de compromisso de fornecer os níveis de serviço previstos e contratados; evidências de ativos financeiros em andamento reservados para aquisição de hardware; demonstração de redução de custos por meio do custo amortizado do novo sistema.

5.1.1.1.5 O repositório deve ter tecnologias de software adequadas aos serviços que fornece às comunidades designadas.

Manutenção de tecnologia, expectativas e perfis de uso atualizados da Comunidade Designada; fornecimento de sistemas de software adequados para suportar as demandas de ingestão e uso; obtenção sistemática de feedback sobre a adequação do software e do serviço; manutenção de um inventário de software atual.

5.1.1.1.6 O repositório deve ter procedimentos em vigor para monitorar e receber notificações quando mudanças de software são necessárias.

Auditorias de capacidade *versus* uso real; auditorias de taxas de erro observadas; auditorias de gargalos de desempenho que limitam a capacidade de atender aos requisitos de acesso da comunidade de usuários; documentação de avaliações de observação de tecnologia; documentação de atualizações de tecnologia de fornecedores.

5.1 GESTÃO DE RISCO DE INFRAESTRUTURA TÉCNICA

5.1.1.1.7 O repositório deve ter procedimentos em vigor para avaliar quando mudanças são necessárias no software atual.

Procedimentos de avaliação implementados; experiência documentada da equipe em cada subsistema de tecnologia de software.

5.1.1.1.8 O repositório deve ter procedimentos, compromisso e financiamento para substituir o software quando a avaliação indicar a necessidade de fazê-lo.

Declaração de compromisso de fornecer os níveis de serviço previstos e contratados; evidências de ativos financeiros em andamento reservados para aquisição de hardware; demonstração de redução de custos por meio do custo amortizado do novo sistema.

5.1.1.2 O repositório deve ter suporte de hardware e software adequado para funcionalidade de backup suficiente para preservar o conteúdo do repositório e rastrear as funções do repositório.

Documentação do que está sendo feito o backup e com que frequência; log de auditoria/inventário de backups; validação de backups concluídos; plano, política e documentação de recuperação de desastres; exercícios contra incêndio; teste de backups; contratos de suporte de hardware e software para mecanismos de backup; preservação demonstrada de metadados do sistema, como controles de acesso, localização de réplicas, trilhas de auditoria, valores de checksum.

5.1 GESTÃO DE RISCO DE INFRAESTRUTURA TÉCNICA

5.1.1.3 O repositório deve ter mecanismos eficazes para detectar corrupção ou perda de bits.

Documentos que especificam os mecanismos de detecção e correção de erros de bits usados; análise de risco; relatórios de erros; análise de ameaças; análise periódica da integridade dos acervos do repositório. Discussão.

5.1.1.3.1 O repositório deve registrar e relatar à sua administração todos os incidentes de corrupção ou perda de dados, e medidas devem ser tomadas para reparar/substituir dados corrompidos ou perdidos.

Procedimentos relacionados ao relato de incidentes aos administradores; registros de metadados de preservação (por exemplo, PDI); comparação de logs de erros com relatórios para administração; procedimentos de escalonamento relacionados à perda de dados; rastreamento de fontes de incidentes; ações de remediação tomadas para remover fontes de incidentes.

5.1.1.4 O repositório deve ter um processo para registrar e reagir à disponibilidade de novas atualizações de segurança com base em uma avaliação de risco-benefício.

Registro de risco (lista de todos os patches disponíveis e análise de documentação de risco); evidências de processos de atualização (por exemplo, daemon do gerenciador de atualização do servidor); documentação relacionada com as instalações de atualização.

5.1 GESTÃO DE RISCO DE INFRAESTRUTURA TÉCNICA

5.1.1.5 O repositório deve ter processos definidos para mídia de armazenamento e/ou mudança de hardware (por exemplo, atualização, migração).

Documentação de processos de migração; políticas relacionadas a suporte, manutenção e substituição de hardware; documentação dos ciclos de vida de suporte esperados do fabricante do hardware; políticas relacionadas à migração de registros para sistemas de hardware alternativos.

5.1.1.6 O repositório deve ter processos críticos identificados e documentados que afetam sua capacidade de cumprir com suas responsabilidades obrigatórias.

Matriz de rastreabilidade entre processos e requisitos obrigatórios.

5.1.1.6.1 O repositório deve ter um processo de gerenciamento de mudanças documentado que identifique as mudanças nos processos críticos que potencialmente afetam a capacidade do repositório de cumprir com suas responsabilidades obrigatórias.

Documentação do processo de gerenciamento de mudanças; avaliação de risco associado a uma mudança de processo; análise do impacto esperado de uma mudança de processo; comparação de registros de mudanças reais em processos *versus* análises associadas de seu impacto e criticidade.

5.1.1.6.2 O repositório deve ter um processo para testar e avaliar o efeito das mudanças nos processos críticos do repositório.

Procedimentos de teste documentados; documentação dos resultados dos testes anteriores e comprovação das alterações feitas em decorrência dos testes; análise do impacto de uma mudança de processo.

5.1 GESTÃO DE RISCO DE INFRAESTRUTURA TÉCNICA

5.1.2 O repositório deve gerenciar o número e localização de cópias de todos os objetos digitais.

Testes de recuperação aleatória; validação da existência do objeto para cada local registrado; validação de um local registrado para cada objeto em sistemas de armazenamento; informações de verificação de proveniência e fixidez; registro / registro de localização de objetos digitais em comparação com o número esperado e localização de cópias de objetos específicos.

5.1.2.1 O repositório deve ter mecanismos para garantir que quaisquer / múltiplas cópias de objetos digitais sejam sincronizadas.

Fluxos de trabalho de sincronização; análise do sistema de quanto tempo leva para as cópias serem sincronizadas; procedimentos / documentação de processos de sincronização.

5.2 GESTÃO DE RISCO DE SEGURANÇA

5.2.1 O repositório deve manter uma análise sistemática dos fatores de risco de segurança associados aos dados, sistemas, pessoal e planta física.

O repositório emprega os códigos de prática encontrados na série ISO 27000 da lista de controle do sistema de padrões; análise de risco, ameaça ou controle.

5.2.2 O repositório deve ter controles implementados para tratar adequadamente cada um dos riscos de segurança definidos.

O repositório emprega os códigos de prática encontrados na série de padrões ISO 27000; lista de controle do sistema; análises de risco, ameaça ou controle; e adição de controles com base na detecção e avaliação contínua de riscos. Repositório mantém a certificação ISO 17799

5.2.3 A equipe do repositório deve ter funções, responsabilidades e autorizações delineadas relacionadas à implementação de mudanças no sistema.

O repositório emprega os códigos de prática encontrados na série de padrões ISO 27000; lista de controle do sistema; análises de risco, ameaça ou controle; e adição de controles com base na detecção e avaliação contínua de riscos. Repositório mantém a certificação ISO 17799

5.2 GESTÃO DE RISCO DE SEGURANÇA

5.2.4 O repositório deve ter plano(s) de preparação e recuperação para desastres por escrito, incluindo pelo menos um backup externo de todas as informações preservadas junto com uma cópia externa do(s) plano(s) de recuperação.

O repositório emprega os códigos de prática encontrados na série de padrões ISO 27000; planos de desastre e recuperação; informações sobre e prova de pelo menos uma cópia fora do local de informações preservadas; plano de continuidade do serviço; documentação ligando funções com atividades; dados geológicos, geográficos ou meteorológicos locais ou avaliações de ameaças. O repositório mantém a certificação ISO 17799.

Infraestrutura Organizacional

Requisitos Arquivísticos

Infraestrutura Tecnológica

Gerenciamento dos objetos

Garantir documentos digitais confiáveis e acessíveis para o futuro

Transparência

Relatório, manuais e processos publicizados. (site da instituição)

Base de conhecimento

Ter uma base de conhecimento que registre todas os padrões, regras, normas, definições, metodologias, configurações e todos os documentos e informações que descrevem o funcionamento do ecossistema

Planos de trabalho

Para cobrir as lacunas encontradas nos diagnósticos

Documentar

Manter um arquivo/dossiê sobre o ecossistema, documentação administrativa, tomada de decisões e etc.

Aderência a normas e boas práticas

Normas nacionais e internacionais, estudos de casos, boas práticas

Autoavaliação constante

Diagnóstico de todos os contextos do ecossistema

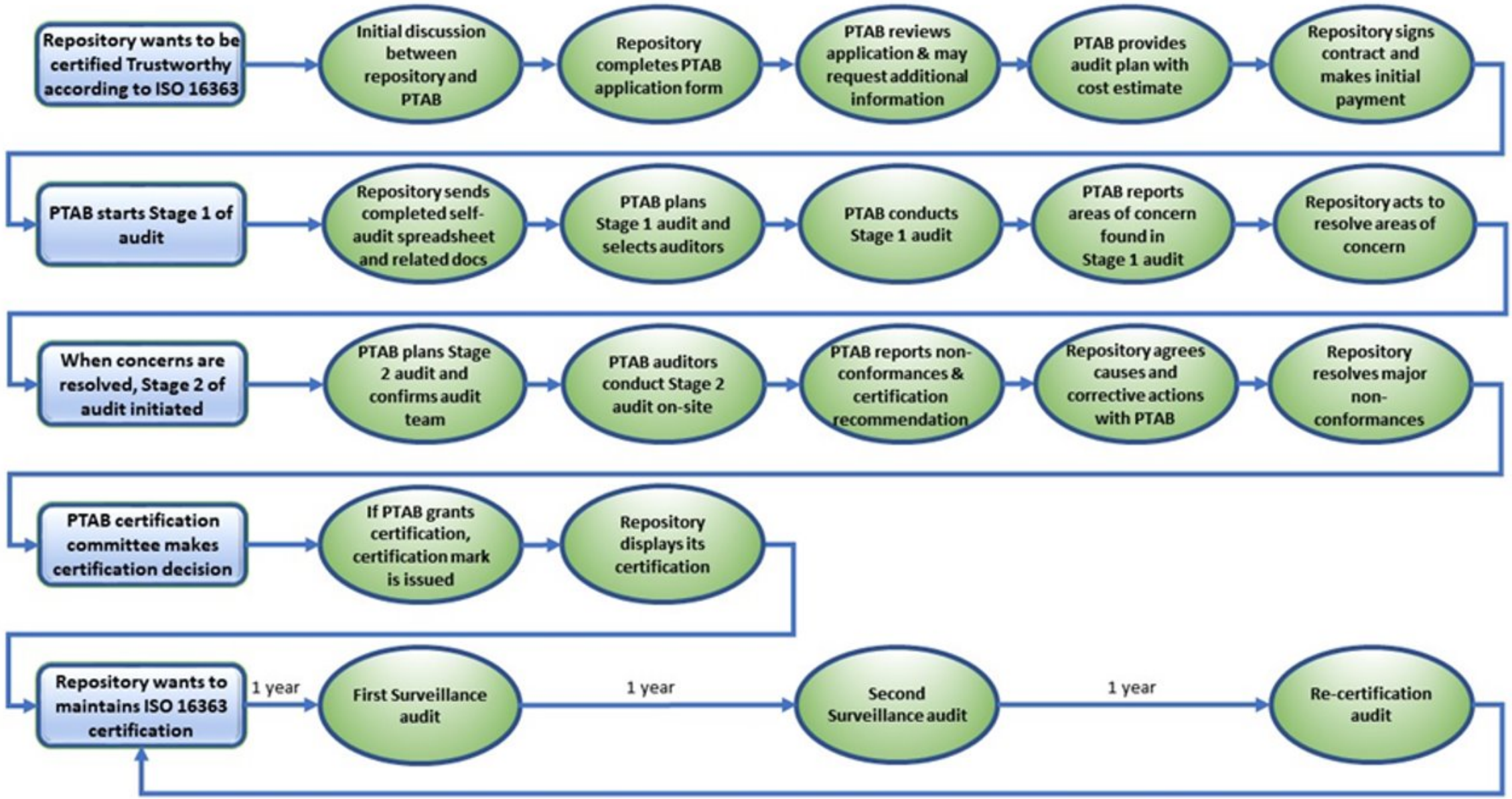
Manualizar procedimentos

Processos e procedimentos documentados e sempre atualizados

Instituir Política de Preservação

Competências do GT

1. Conhecimento sobre a ISO 16.363 e outras normas relevantes;
2. Conhecimento sobre preservação digital;
3. Conhecimento sobre avaliação e gestão de riscos de informações digitais;
4. Conhecimento técnico dos aspectos de preservação digital que se aplicam à atividade a ser auditada;
5. Conhecimento geral dos requisitos regulamentares relevantes para os TDRs;
6. Conhecimento de sistemas de gestão;
7. Compreensão dos princípios de auditoria com base na ISO 19011.


Repository wants to be certified Trustworthy according to ISO 16363
Initial discussion between repository and PTAB
Repository completes PTAB application form
PTAB reviews application & may request additional information
PTAB provides audit plan with cost estimate
Repository signs contract and makes initial payment
PTAB starts Stage 1 of audit
Repository sends completed self-audit spreadsheet and related docs
PTAB plans Stage 1 audit and selects auditors
PTAB conducts Stage 1 audit
PTAB reports areas of concern found in Stage 1 audit
Repository acts to resolve areas of concern
When concerns are resolved, Stage 2 of audit initiated
PTAB plans Stage 2 audit and confirms audit team
PTAB auditors conduct Stage 2 audit on-site
PTAB reports non-conformances & certification recommendation
Repository agrees causes and corrective actions with PTAB
Repository resolves major non-conformances
PTAB certification committee makes certification decision
If PTAB grants certification, certification mark is issued
Repository displays its certification
Repository wants to maintains ISO 16363 certification
1 year
First Surveillance audit
1 year
Second Surveillance audit
1 year
Re-certification audit

Referências

Thibodeau, Ken. (2002). Overview of Technological Approaches to Digital Preservation and Challenges in Coming Years. https://chnm.gmu.edu/digitalhistory/links/pdf/preserving/8_37e.pdf

M. Ferreira, Introdução à preservação digital – Conceitos, estratégias e actuais consensos. Guimarães, Portugal: Escola de Engenharia da Universidade do Minho, 2006. https://repositorium.sdum.uminho.pt/bitstream/1822/5820/1/livro.pdf

PINTO, Maria Manuela. PRESERVMAP : um roteiro da preservação na era digital. 2009

THOMAZ, Kátia P.Critical Factors for Digital Records Preservation http://jiito.informingscience.org/articles/JIITOv1p021-041Thomaz12.pdf

WATERS, Donald; GARRETT, John - Preserving digital information, report of the task force on archiving of digital information, p. III

LAVOIE, Brain - The Open Archival Information System reference model: introductory guide

CORNELL UNIVERSITY LIBRARY; ICPSR; MIT LIBRARIES – Attributes of a TDR. In Digital preservation management: http://dpworkshop.org/dpm-eng/foundation/tdr/index.html.

OBRIGADO

SUDESTE/RIAA
Rede Sudeste de Repositórios Institucionais

alex@an.gov.br

alex-holanda