

Modelo de Preservación Digital Sistémica: Cadena de Custodia Digital Archivística - CCDA

Daniel Flores

Universidade Federal Fluminense - RJ - Brasil

11ª edición del Seminario Internacional de Archivos de Tradición Ibérica, Transformación
Digital: Retos y oportunidades

Miércoles, 19 de febrero, Archivo General de Indias, Sevilla.

PROGRAMA

Sevilla, España - 19 de febrero de 2020

Entrada libre hasta completar aforo.

16:00 horas	Inauguración del Seminario Internacional de Archivos de Tradición Ibérica.	Severiano Hernández Vicente Subdirector General de los Archivos Estatales de España. Emma de Ramón Acevedo Presidenta interina de la ALA.
16:20 a 16:40 horas	Introducción sobre el panorama de la gestión de documentos electrónicos en Iberoamérica.	Ricard Pérez Alcázar Jefe de Área de Gestión Documental y Administración Electrónica de la Subdirección General de los Archivos Estatales de España.
16:45 a 17:25 horas	Modelo de preservación digital sistémica.	Daniel Flores Investigador de Productividad de la agencia brasileña CNPQ.
17:30 a 18:30 horas	Mesa de experiencias, avances y desafíos en la gestión de documentos electrónicos en Iberoamérica.	Neide Alves Dias De Sordi Directora general del Archivo Nacional de Brasil. Enrique Serrano Director del Archivo General de la Nación de Colombia Alexander Barquero Director del Archivo Nacional de Costa Rica. Emma de Ramón Directora del Archivo Nacional de Chile.
18:30 a 18:55 horas	Herramientas y plataformas tecnológicas para soportar archivos digitales.	Francisco Barbado Director de Serviços de Inovação e Administração Eletrónica da Direcção-Geral do Livro, Arquivos e Bibliotecas - Portugal.
19:00 a 19:30 horas	La aplicación de herramientas para la generación de paquetes de información OAIS en el contexto europeo. La experiencia de implementación de EARK2 en el Archivo Nacional de Hungría.	Elena Cortés Ruiz Jefa de Descripción y Conservación del Archivo General de la Administración de España y miembro del Comité Ejecutivo del DLM Forum. Zoltán Szatucsek Director Técnico del Archivo Nacional de Hungría y miembro del Comité Ejecutivo del DLM-Forum.
19:35 horas	Clausura del 11 SIATI.	

Sede: Archivo General de Indias
Calle Santo Tomas 5#
Edificio "La Cilla", CP. 41004
Sevilla, España.

Inscripciones y mayores informes:
www.alaarchivos.org
@ALAArchivos @ArchivosALA

pares.culturaydeporte.gob.es
@ArchivosEst
@PortalArchivosEspanolesPARES



Para referenciar este material del Grupo CNPq UFF Ged/A - Documentos Archivísticos Digitais:

Referencia:

FLORES, Daniel. **Modelo de Preservación Digital Sistémica: Cadena de Custodia Digital Archivística - CCDA**. Conferencia. Sevilla, ES. 50 slides, color, Slides Modelo Google Drive/Docs 4x3. Material producido para Conferencia en la 11ª edición del Seminario Internacional de Archivos de Tradición Ibérica, Transformación Digital: Retos y oportunidades. Sevilla, 19 de febrero de 2020. Disponible en: <<http://documentosdigitais.blogspot.com>>. Acceso en: 19 de febrero de 2020.

Citación con autor incluso en el texto:

Flores (2020)

Citación con autor no incluso en el texto:

(FLORES, 2020)



Antecedentes de nuestra Investigación



Antecedentes

Los productores

Los preservadores

Los productores y los sistemas de negocio:

- ❖ Sistemas digitales sin requisitos funcionales o no funcionales que garanticen la autenticidad y confiabilidad;
- ❖ Hoy por hoy, no archivamos más, sólo “tagueamos”;
- ❖ Hoy no se hacen más transferencias primarias o secundarias de Documentos digitales a los Archivos;
- ❖ Producimos documentos en sistemas de negocio y ni lo sabemos cuales.

ARCHIVAR:

un Documento Archivístico, denota un imperativo JURÍDICO y procedimientos ARCHIVÍSTICOS sistemáticos, no es sólo asignar un metadato al Documento, no es usar "TAGS", nada de eso, es un procedimiento jurídico y archivístico, de ARCHIVAMIENTO¹. Si estamos hablando de Documentos Digitales, el mismo tiene que pasar a tener "Forma Documental Diplomática Manifestada" (o almacenada, pero con su Manifestador de Dataset encapsulado), tiene que recibir sus Metadatos de Gestión (e-ARQ Brasil o Moreq-JUS) y Metadatos de Representación (Descripción Archivística), es decir, la equivalencia a los metadatos ISAD(G)/NOBRADE y ser transferido o recopilado (vía REST API) en un paquete OAIS SIP para que en el RDC-Arq (Conforme Res. 43/Conarq, ISO OAIS 14721 y 16363) sea transformado en un Paquete OAIS AIP de Preservación Permanente (en una Cadena de Custodia Digital Archivística Ininterrumpida, como forma de garantizar su Autenticidad) y sea dado acceso a través de Paquetes OAIS DIP en Plataformas Archivísticas de Descripción, Acceso, Difusión y Transparencia Activa (FLORES, 2016).

¹ Archivo (DIBRATE, 2005):

1. Secuencia de operaciones intelectuales y físicas que apuntan a la guardia ordenada de documentos. Ver también: arreglo, método de archivo y sistema de archivado.
2. La acción por la que una autoridad determina la custodia de un documento, cesada su tramitación.

Los preservadores

- ❖ No hay conexión digital prioritaria con los productores;
- ❖ Enfocamos en el analógico y poca inversión en el digital;
- ❖ No ofrecemos custodia ininterrumpida de documentos digitales;
- ❖ No ofrecemos Repositorios Archivísticos con Documentos en Datos para Big Data;
- ❖ No estamos con nuestros documentos digitales en PAQUETES OAIS AIP (No tenemos documentos digitales PERMANENTES PRESERVADOS según nuestros referenciales);
- ❖ Nuestros documentos están en soportes digitales, pero, fuera de un sistema digital con requisitos archivísticos;
- ❖ Modelo casi que exclusivamente analógico.

Una otra constatación

Vivimos en un mundo

La transformación digital
sistémica tiene 2 lugares

Innovación sostenida

Disrupción tecnológica

Para tal

Fuimos a buscar elementos, conceptos y principios para justificar la necesidad cada vez más urgente de la gestión archivística y de la preservación digital sistémica en los documentos digitales hoy producidos sin requisitos (buscamos Innovación Sostenida).

Ya que, estamos en una situación de INSEGURIDAD JURÍDICA La vida de las personas registradas en los documentos de archivo está en riesgo

...

Encontramos

- ⬡ Diplomática, InterPARES, una literatura consistente, etc.;
- ⬡ La complejidad y especificidad de los documentos digitales, Forma fija, contenido estable, la manifestación diplomática, los sistemas de negocio;
- ⬡ Requisitos para los sistemas de gestión;
- ⬡ Empaquetamiento OAIS (2 formatos en el mundo);
- ⬡ EDMS, SGDA, SIGAD, RDC-Arch;
- ⬡ ...

Pero

Algunos vacíos persistieron ...



CSI

Y la Cadena de Custodia
de los crímenes



Cadena de custodia

Documento o seguimiento que demuestre la **sucesión de personas jurídicas o personas** que hayan tenido posesión, custodia y control sobre los documentos.

Documento ou trilha que demonstra a **sucessão de entidades coletivas ou pessoas** que tiveram posse, custódia e controle sobre os documentos. (ICA Multilingual Archival Terminology)

← → ↺ ⓘ Não seguro | ciscra.org/mat/mat/term/95



[Home](#)

[Help](#)

[Login](#)

[Register](#)

[Select Language](#)

Multilingual Archival Terminology



chain of custody ([Edit Term](#))

[Add Definition\(s\)](#)

Definitions:

noun

1. Document or paper trail showing the succession of offices or persons having seizure, custody, control, transfer, analysis, and disposition of physical and electronic evidence.

Citation:

[Glossary of Records and Information Management Terms, 3rd ed. (ARMA International, 2007)]

CoC



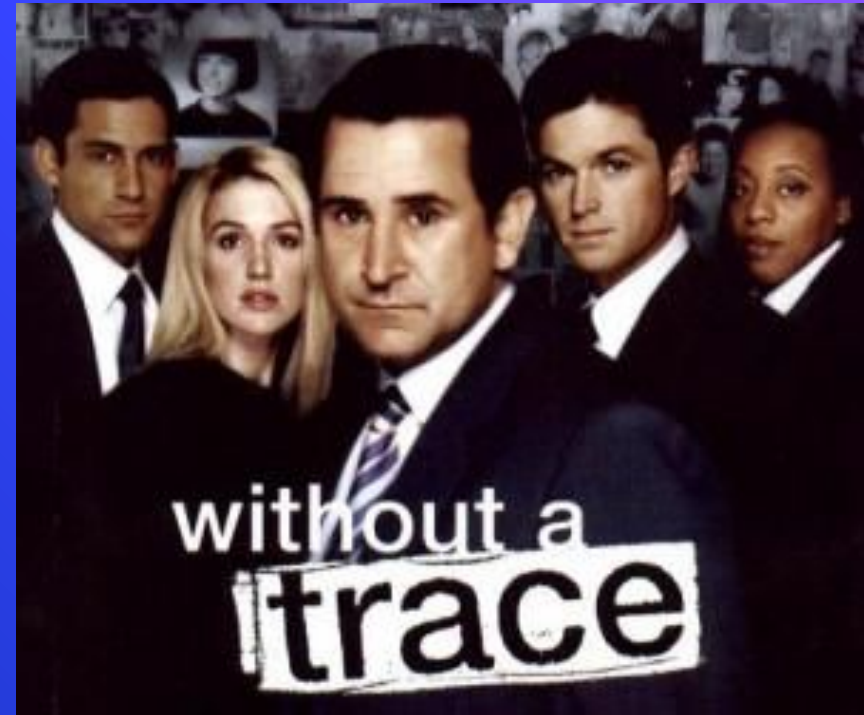
El concepto de la Cadena de Custodia ya no daba más cuenta de los documentos digitales.

En algunos casos un Archivo recibe o almacena en un Disco Duro, medios o soportes digitales sus documentos, en principio estando de acuerdo con la definición de la Cadena de Custodia pensada a un ambiente analógico, pero no para un ambiente digital ... sin rastros digitales ...

Bajo los principios de los DADS

Tiene complejidad

Tiene especificidad



Home > Governo

Funcionário do TCE-AM executa script errado no SQL e apaga 16,5 mil processos

Por Redação | 06 de Outubro de 2017 às 12h20

Pues, tenemos
BACKUP como
seguridad y
Preservación
Digital

Depois de ter 16,5 mil processos apagados do banco de dados PostgreSQL, o Tribunal de Contas do Estado do Amazonas (TCE-AM) anunciou que até a próxima semana todos os processos deverão ser recuperados. A garantia foi dada pelo conselheiro-presidente do TCE-AM, Ari Moutinho Júnior, que lembrou que os dados do TCE possuem **backup**.

Os processos eletrônicos foram apagados por uma pane nos sistemas e-Contas e Spede (Sistema de Processos e Documentos Eletrônicos) depois que um administrador de sistemas executou indevidamente um script sem fazer a devida checagem.

Segundo informações do TCE-AM, 80% dos processos de aposentadoria foram afetados, sendo que dos 16,5 mil processos excluídos, 62% já foram plenamente recuperados, enquanto que os outros 38% estão em fase de recuperação e deverão estar acessíveis nos próximos dias. "Os TCE têm backup, tanto que os dados estão sendo recuperados paulatinamente, mas o incidente havia tornado inacessível os arquivos, bloqueando o acesso", explicou o conselheiro-presidente.

Em coletiva à imprensa, Ari afirmou que os dois servidores concursados identificados como os responsáveis pela pane, seja de maneira direta ou indireta, terão de responder administrativamente pelo problema técnico que causaram na Corregedoria do TCE, tendo ainda que ressarcir os cofres públicos em R\$ 33 mil, que foram utilizados na contratação de empresas especializadas na recuperação e armazenamento de dados.

"Os servidores serão encaminhados à Corregedoria e serão obrigados a ressarcir os custos do Tribunal de Contas, porque nós não toleramos a imprudência e o excesso de confiança, que geraram preocupação momentânea na população do Estado do Amazonas", afirmou Ari. Com a ajuda das empresas contratadas para auxiliar na



Y las pistas
de auditoría

El Documento Archivístico Digital

Para que sirva de fuente de prueba, testimonio, memoria, patrimonio, garantía de derechos y la plena ciudadanía,

DEBE:

ser mantenido auténtico
(**transmisión**, **preservación** y **custodia**),

confiable (producción),

Sea este original o un representante digital.

Autenticidad

Autenticidad

Es la Calidad del documento
ser justo aquél que ha sido
producido



Autenticación

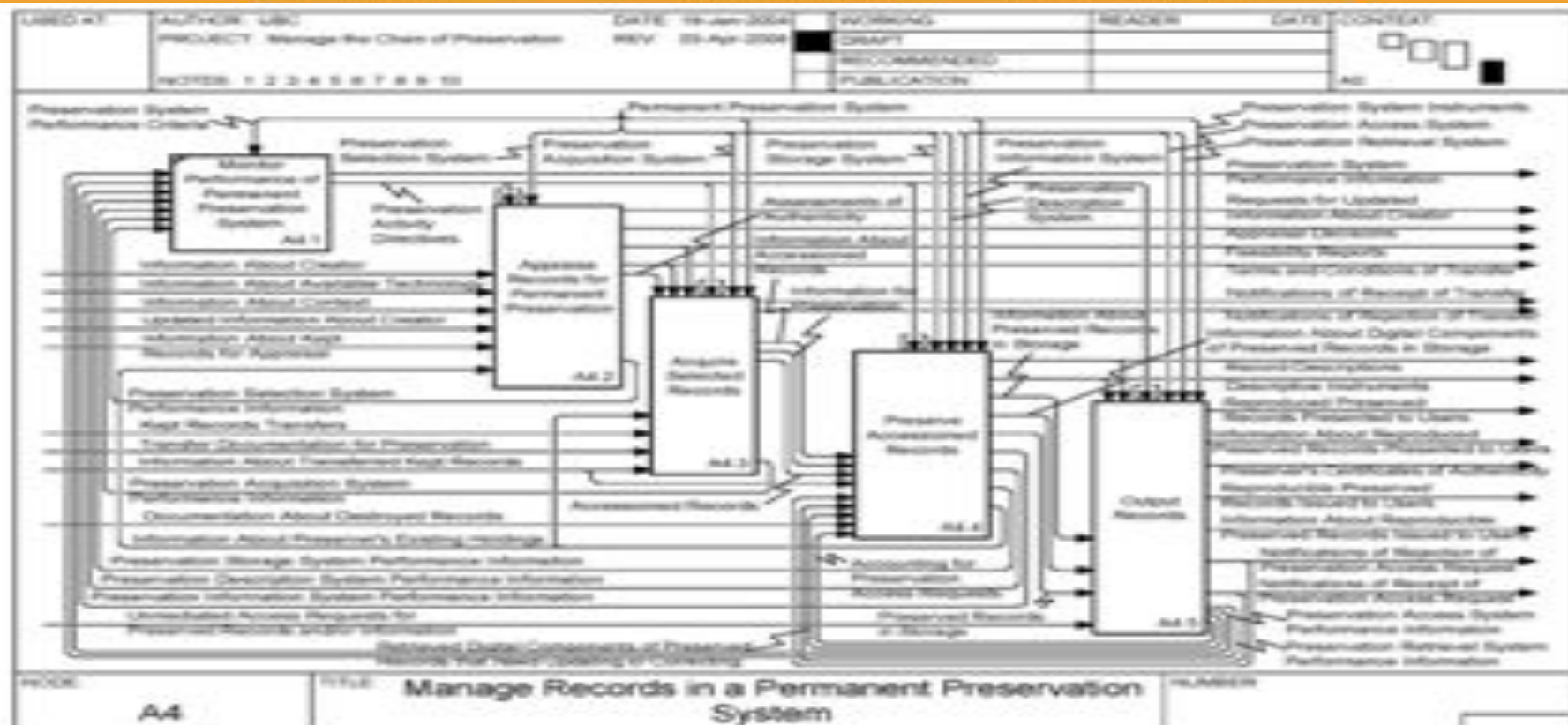
Declaración de autenticidade
hecha en un dado momento
por una persona autorizada
para tal

- La autenticação no garantiza la autenticidad del documento – así, se puede declarar como auténtico algo que no lo es.
- Un documento sin autenticación puede ser auténtico.
- Mientras la teoría archivística tradicional, siguiendo jurisprudencia, los documentos considerados confiables por sus productores en el curso normal de sus actividades son presumidos auténticos, con los documentos en sistemas electrónicos, la presumible autenticidad debe estar apoyada por la evidencia de que un documento no fue alterado o corrompido en sus aspectos esenciales durante su transmisión. [Duranti. Rumo a uma teoria arquivística de preservação digital.]

CoP

**Encontramos la Cadena de Preservación
presentada por InterPARES;**

InterPARES2 Chain of Preservation



Nosotros estudiamos la CoP

- ⬡ Al probar en laboratorio, se nos presentó más procedimental;
- ⬡ tecnológica;
- ⬡ técnica;
- ⬡ no conceptual;
- ⬡ es un modelo computacional,
- ⬡ Por supuesto, magnífico y complementar a una Cadena de Custodia.

Investigamos +

Y llegamos a una posible ruptura paradigmática

CCDA

Cadena de preservación

Sistema de controles que se estende por todo o ciclo de vida dos documentos, a fim de assegurar sua autenticidade ao longo do tempo.

(ICA Multilingual Archival Terminology)

O projeto Interpares 2 (2001) apresenta um modelo de Cadeia de Preservação (CoP) como uma sequência de passos para a produção, manutenção, avaliação e preservação digital de documentos autênticos.

[Capa](#) [Seções](#) [Colunistas](#) [Blogs](#) [Anuários](#) [Anuncie](#)

[Livraria](#) [Lançamentos](#) [Mais vendidos](#) [Boletim Jurídico](#) [Cursos](#) [Busca de livros](#)

SUPOORTE A LITÍGIOS

E-mails exigem cuidados específicos para que sirvam como prova

2 de setembro de 2015, 11h16

 [Imprimir](#)

 [Enviar por email](#)

 2493

 48

 4

[Por Marcelo Stopanovski](#)

Já é comum que processos jurídicos utilizem uma mensagem de correio eletrônico como meio de prova. Seja sobre um contrato trocado pelo e-mail e as manifestações expressas de vontade entre as partes nas mensagens que o discutem ou como elemento cabal da existência de uma fraude interna em uma empresa ou uma licitação, o e-mail é sem dúvida um instrumento de prova.

Então basta salvar o e-mail como PDF e dar *upload* no processo eletrônico e tudo certo? Com a devida ressalva aos especialistas por deixar de lado procedimentos mais aprofundados, algumas



Marcelo Stopanovski
Consultor e professor

Los elementos
Intrínsecos y
extrínsecos de
autenticidad están en
el Paquete OAIS AIP en
el RDC-Arch

- Confidencialidade. O emissor possui chave pessoal e registrada em uma cadeia de autenticação;
- Integridade. A alteração de um bit sequer na mensagem resulta em uma incompatibilidade com as chaves;
- Irretratabilidade. O emissor não pode negar que aplicou a assinatura à mensagem.

Ou seja, um e-mail é uma prova inerentemente considerável somente se for assinado eletronicamente, a exemplo da assinatura do magistrado em um processo eletrônico conferindo características de documento eletrônico para o despacho.

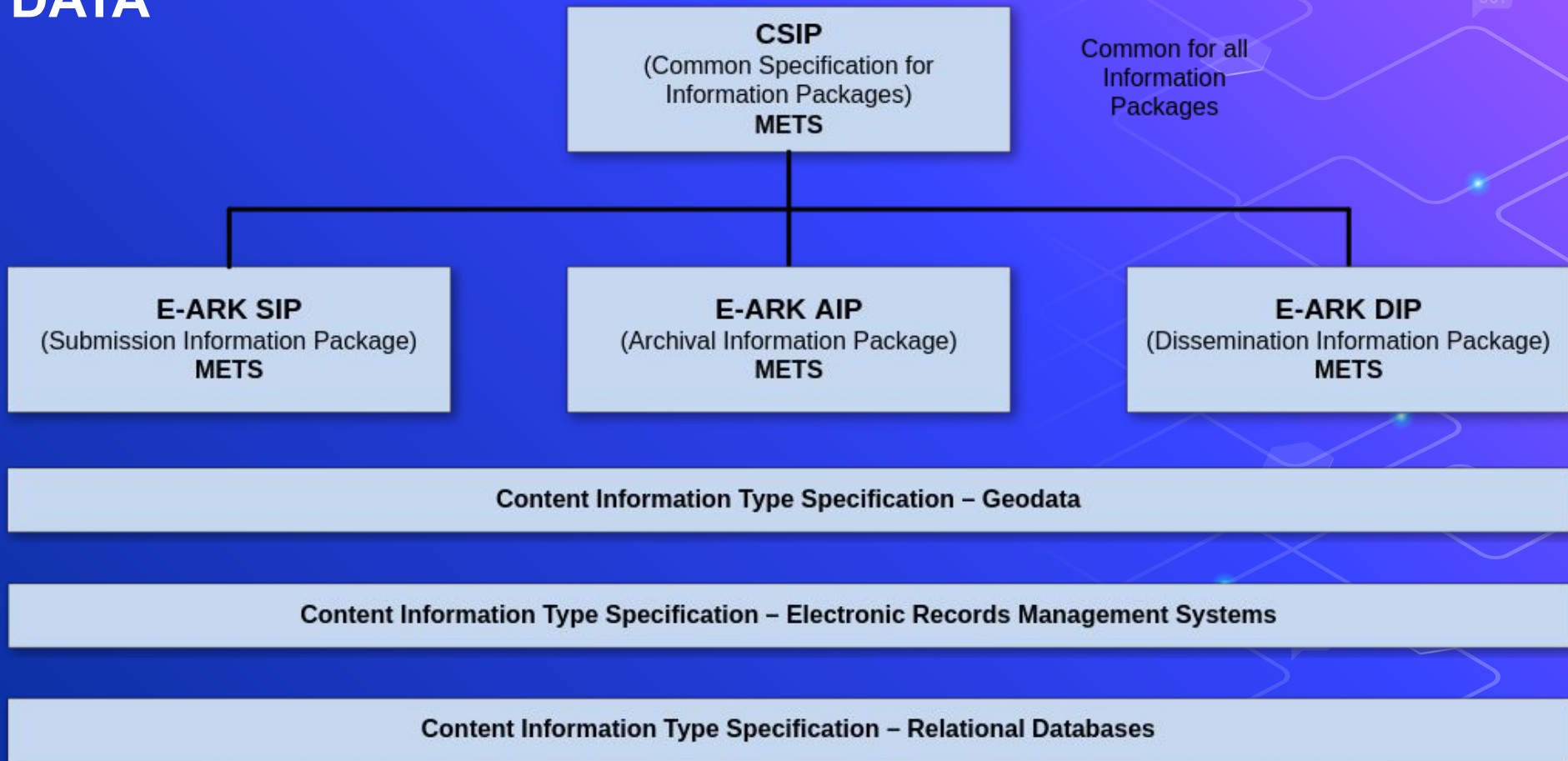
Quando este não for o caso, as mensagens devem ser periciadas para atestarem suas características de prova jurídica. Em princípio a perícia deve validar:

- O arquivo da mensagem em si, verificando origem, destino, data, hora e conteúdo;
- A **cadeia de custódia** da mensagem, validando a não contaminação do valor jurídico da prova, verificando especialmente autorizações e garantia de integridade das informações custodiadas.

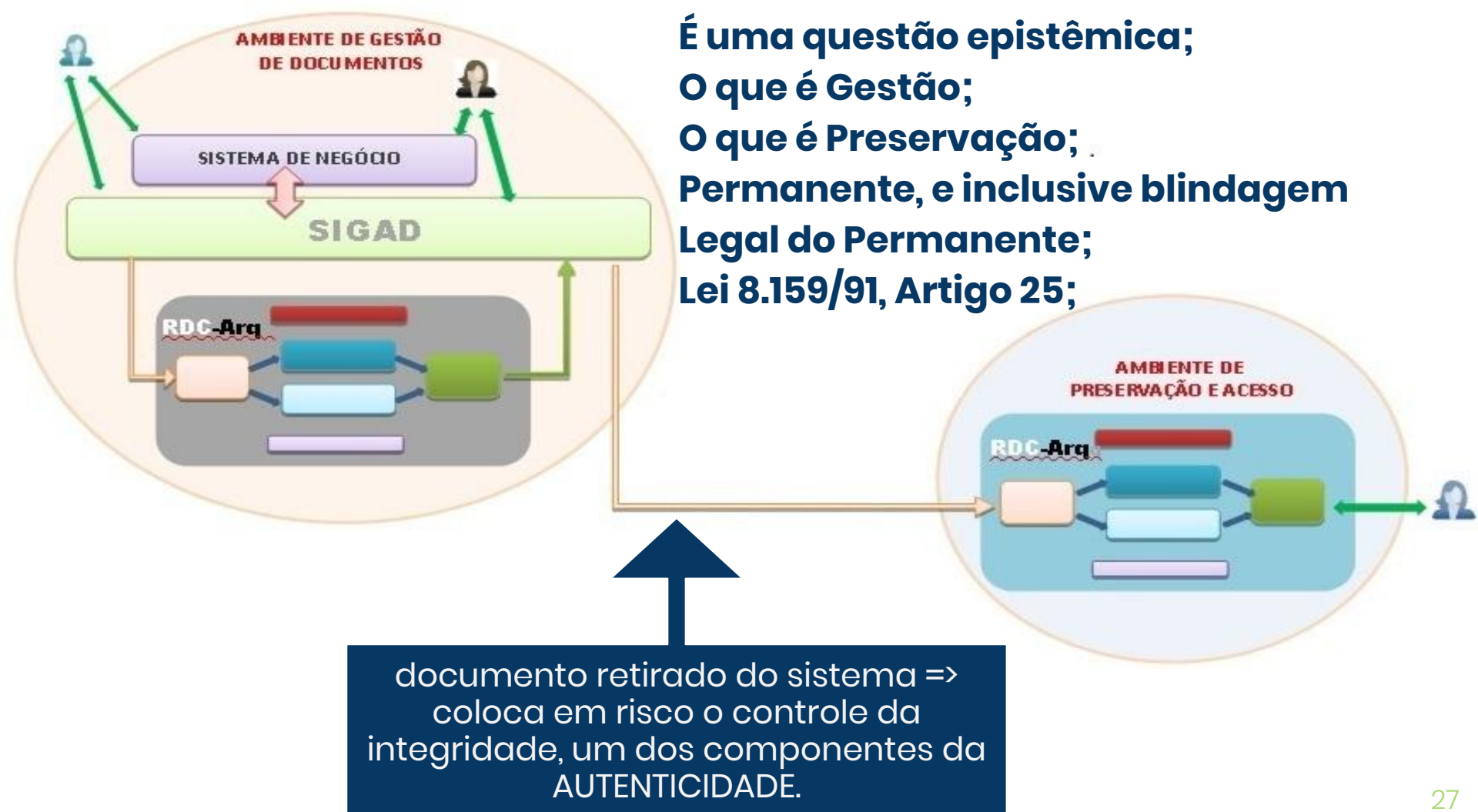
A **cadeia de custódia** é especialmente relevante para os casos de informações em meio digital, dada a facilidade de alteração dos conteúdos sem rastros aferíveis.

Somente será possível equacionar a validade da mensagem se, além do acesso ao arquivo da mensagem que foi impressa, for seguida a sequência de atos que levaram à aquisição da informação. Desde a coleta na máquina, no servidor ou no provedor até a posse do arquivo pela parte.

Los Paquetes Archivísticos para los RDC-Arch y el BIG DATA



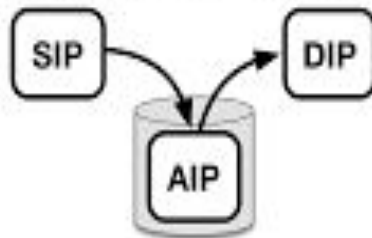
**É uma questão epistêmica;
O que é Gestão;
O que é Preservação;
Permanente, e inclusive blindagem
Legal do Permanente;
Lei 8.159/91, Artigo 25;**



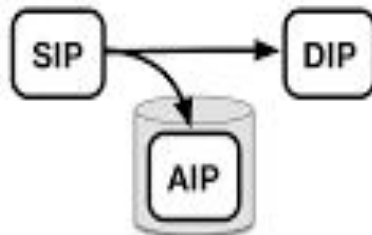
En el FUTURO:

**Las transferencias
serán por
Paquetes OAIS
SIP?**

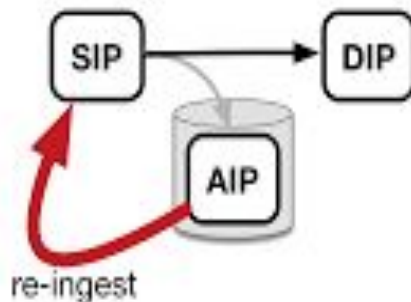
a) OAIS: ingest SIP->AIP, disseminate AIP->DIP



b) Archivemática: AIP & DIP created on ingest, no AIP->DIP process



c) Archivemática: DIP from AIP only via re-ingest

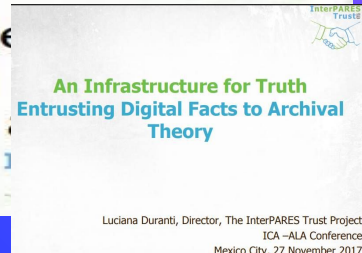


Archival authentication

A declaration of authenticity based on either on material proof, inference, or deduction

Let's move from theory to practice: what are the means for authenticating digital facts?

- **A chain of legitimate custody** remains ground for inferring authenticity and authenticate a record.
- **Digital chain of custody:** the information preserved about the record and its changes that shows specific data was in a particular state at a given date and time.
- A **declaration** made by an expert who bases it on the trustworthiness of the system hosting the record and procedures and processes controlling its preservation



Cadeia de Custódia Digital por Luciana Duranti:

"DIGITAL CHAIN OF CUSTODY: the information preserved about the record and its changes that shows specific data was in a particular state at a given date and time."

Fonte:

Conferência Magistral no Congresso do ICA - ALA na Cidade do México, 2017

Sistemas de información y preservación digital

An Infrastructure for Truth

Entrusting Digital Facts to Archival Theory

Cadeia de Custódia Digital Arquivística

Download em .PDF (pg. 10):

http://www.alaarchivos.org/wp-content/uploads/2017/12/Magistral-Luciana-Duranti.pdf?fbclid=IwAR11wLL_g14Beb6hivpwwUWd5dpRr6PMQm6yXqfxcJwST-E2LeWjDeqhV4

La información preservada sobre el documento y sus cambios que demuestran que un dato específico estaba en un determinado estado en una fecha y hora” [traducción nuestra].

chain of custody

Relationships

Related Term:

[custodial history](#)
[custody](#)

n. ~ 1. RECORDS · The succession of offices or persons who have held materials from the moment they were created. - 2. LAW · The succession of officers or individuals who have held real evidence from the moment it is obtained until presented in court.

Notes:

In both senses, the ability to demonstrate an unbroken chain of custody is an important test of the authenticity of records or evidence.

Citations:

[†]([Bastian 2001, p. 96](#)) Custody, both the legal and physical ownership of records, has long been recognized as a fundamental principle of archival management. . . . Hilary Jenkinson based the sanctity of evidence on the ability to prove continuous custody. T. R. Schellenberg, while rejecting 'continuous custody' as unworkable for the National Archives of the United States, still considered that having custody of the records that crossed the threshold of the Archives was essential to protecting their integrity.

Archival Authenticity in a Digital Age

Home / CLIR Publications / CLIR Reports / Authenticity in a Digital Environment / Archival Authenticity

by Peter B. Hirtle

Archival Authenticity: An Example

One way in which archivists working with analog records have sought to ensure the enduring value of archives as evidence is through the maintenance of an unbroken provenance for the records. Archivists need to be able to assert, often in court, that the records in their custody were actually created by the agency specified. Furthermore, the archivist must be able to assert that the records have been in the custody only of the agency or the archives. In an analog environment, the legal and physical transfer of the documents from the agency to the archives ensures an unbroken chain of custody.

Archives truly exist only when there is an unbroken chain of custody from the creating agency to the archives. For a government archives, the transfer of custody is best accomplished as a matter of law. As Margaret Cross Norton, a pioneer theorist of American archives, noted:

We must disabuse ourselves of the concept that the acquisition by the state historical society of a few historical records . . . automatically transforms the curator of manuscripts into an archivist . . . An archives department is the government agency charged with the duty of planning and supervising the preservation of all those records of the business transactions of its government required by law or other legal implication to be preserved indefinitely (Mitchell 1975).

In a nongovernmental agency, policy can take the place of law if the policy identifies what records of business transactions need to be preserved indefinitely. Either law or policy, however, should govern the transfer of records to an archives.

Why is the authorized transfer of a complete set of records to an archives with an unbroken chain of custody important? First, it helps maintain the evidentiary value of the records. An archivist can be called upon to testify in court about the nature of the records in his or her custody. That archivist would not be expected to testify as to the accuracy of the contents of the records. However, he or she should be able to assert that on the day when the records left the custody of the originating agency or organization, a particular document was included as part of the records.

Equally important as unbroken custody in establishing the integrity of records is the completeness of the documents. Only records that are complete can ensure accountability and protect personal rights. As soon as records become incomplete, their authority is called into question. For example, when information is

Electronic Records

Education-Training

SERP Framework

- Policy
- Strategy
- Governance
- Collaboration
- Technical Expertise
- Open Standards / Neutral Formats
- Designated Community
- Electronic Records Survey
- Ingest
- Storage
- Device / Media Renewal
- Integrity**
- Security
- Preservation Metadata
- Access

Related/Additional Framework Topics

Electronic Records Resources

Glossary

Integrity

DEFINITION: A key capability in ISO 14721 conforming digital repositories is ensuring the integrity of the records in its **custody**, which involves two related preservation actions. The first action generates a cryptographic hash algorithm that normalizes any digital object regardless of size or content type to a fixed length bit stream (e.g., 156 bits). This fixed length bit stream is called a hash digest and it serves as a digital fingerprint. Depending upon the "strength" of the hash digest algorithm used, it is "computationally infeasible" for two different digital objects to have the same hash digest or to reconstruct a data object from this hash digest.

The second action involves integrity fixity that supports an unbroken electronic chain of **custody** captured in Preservation Description Information (PDI) in AIPs. Hash digests cannot support this chain of **custody** because migration to newer file formats will introduce changes in the underlying bit streams. Affixing a digital signature to an AIP that authenticates it after any preservation action will mitigate this issue. Over time digital signatures support a strong, unbroken chain of electronic **custody**.

Level 0	The archival repository has no documented procedure for integrity protection of electronic records in its custody .
Level 1	The archival repository generates and preserves MD-5 hash digests before and after device/media renewal and other archival storage preservation actions.
Level 2	The archival repository generates and preserves SHA-1 hash digests before and after device/media renewal and other internal preservation actions for partially conforming ISO 14721 AIPs.
Level 3	The archival repository generates SHA-2 hash digests before and after device/media renewal and other internal preservation actions for all fully conforming ISO 14721 AIPs and stores them in the Preservation Description Information (PDI) of the AIPs.

Level 4

Level 4a: The archival repository encapsulates fully conforming ISO 14721 AIPs in XML and signs them with a digital signature.

Level 4b: Integrity protection procedures are continuously evaluated and updated as new tools and approaches become available.



InterPARES 1 Project

International Research on Permanent Authentic Records in Electronic Systems

preservation domain

Research Questions and Findings of the Preservation Task Force

The main products resulting from the work of the Preservation Task Force are a survey of current preservation practices in the area of electronic records, a white paper on storage media for digital information storage and a model of the activities involved in the preservation of authentic electronic records. The major activities represented in the preservation model are:

- managing the preservation process;
- bringing in electronic records;
- maintaining electronic records; and
- outputting electronic records.

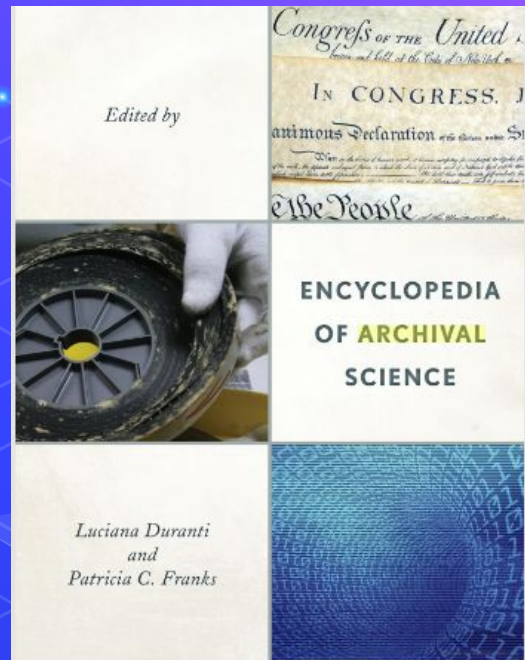
In addition, main findings of the Preservation Task Force include the following:

- Electronic records cannot be preserved as such; only the ability to reproduce them can be preserved.
- Considering that the processes of storage and retrieval imply transformations both physical and of presentation, the traditional concept of **unbroken chain of custody** must be extended to include the processes necessary to ensure the unaltered transmission of the record through time.
- Technology cannot determine the solution to the long-term preservation of electronic records.
- Archival needs define the problem and archival principles must establish the correctness and adequacy of each technical solution.
- Solutions to the preservation problem are inherently dynamic.

New Currents in Acquisition

The traditional waters of acquisition, which assumed the transfer of physical custody of the records, are being muddled by postcustodialism. Archivists are increasingly allowing for the possibility of distributed custody, where physical custody, particularly for *digital records*, remains with the creator after appraisal. For example, in the case of a complex database that remains on the servers of the creating agency, but that cannot be disposed of without **archival** authorization, the archives may be said to have acquired care and control of the record, but not custody. Postcustodialism perhaps shifts the meaning of acquisition from “custody and control” of the records to “care and control.”

Archivists are rethinking custodial approaches in other ways in an era of records abundance and resource scarcity. The growing volume of records and storage costs are making archivists increasingly willing to consider *deaccessioning* or systematic *reappraisal*. Deaccessioning to other archives has long been an option, but receptiveness is increasing to returning material to its original donors or even the destruction of records formerly appraised as **archival**. Archivists are more accepting of the potential impermanence of acquisition.



Conclusion

Acquisition is vital to the establishment and growth of an archives. From the development and implementation of an acquisition policy through to the legal transfer and accessioning of records, the acquisition process covers a broad sweep of core **archival** activity. Though continuing to evolve in concept and practice, it is difficult to imagine **archival** practice without acquisition.—Robert Fisher



How to ensure Chain of Custody for email and archive migrations

21 Oct 2015 by Michel Zehnder

Who has handled the evidence?

In the world of email and email archive migrations you'll often see reference to [Chain of Custody](#) (CoC) as a requirement. So what exactly do we mean by that?

CoC is about traceability and being able to demonstrate that the source hasn't been tampered with. It's evidence that the wood you buy from your timber merchant comes from certified forests, or that drug trial specimens [haven't been contaminated](#) and mixed up with others. Items in transit are locked down at every stage, with auditable records that will stand up to legal scrutiny.

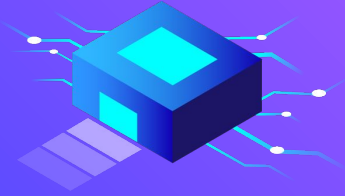
More specifically, in our field, CoC is a "process used to maintain and document the chronological history of the handling, including the transfer of ownership, of any arbitrary digital file from its creation to a final state version" (US [National Digital Stewardship Alliance](#)). CoC tracks the movement of evidence through its [collection, safeguarding, and analysis lifecycle](#) by documenting each person who handled it, the date/time it was collected or transferred, and the purpose for the transfer. With email migrations, CoC records are vital for legal defense once your old source has been decommissioned.

When you move email records, you need to be able to account for every single message that was stored in your source system and what's happened to each one at every step of migration. If the message is not contained in the target destination, you need to be able to explain why not, and what happened to that message. CoC records are most likely to be required retrospectively, so there's only one chance to get them right. That's a good reason to use specialist tools to manage your migration project, rather than relying on manual methods.

Y cuando empezaren a ocurrir los siniestros relacionados a los Documentos de Archivo Nativo Digitales:

Cómo será el análisis Forense Digital con base en la Diplomática Digital / Digital Forensics, que vamos a solicitar:

- Normas;
- Patrones;
- Modelos;
- Requisitos;
- Políticas; y
- Profesionales de sólida formación.



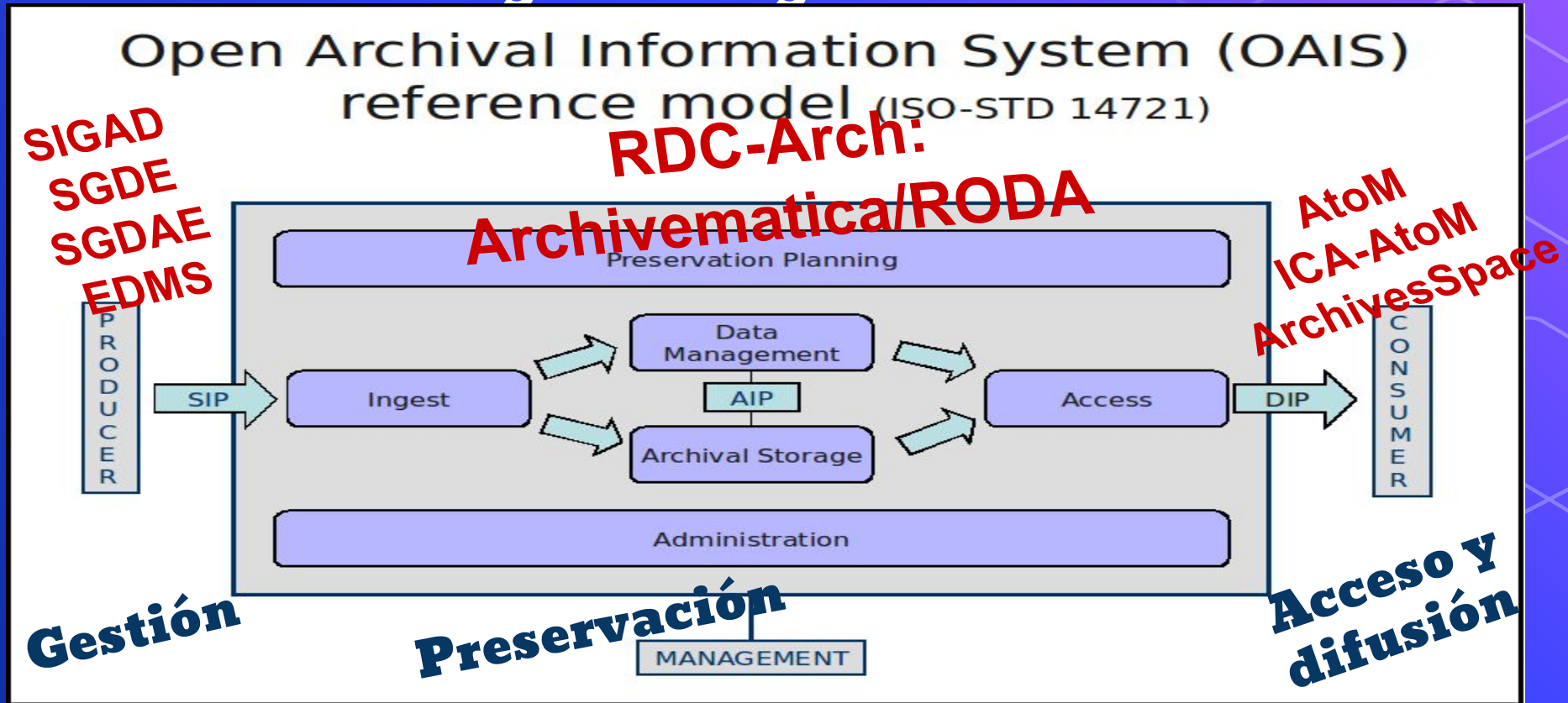


Preservación Digital Sistémica, orientada a Modelos (OAIS): Gestión, Preservación y Acceso

La Preservación Digital debe ser SISTÉMICA ...

- No se puede más pensar en preservar documentos en Bases de Datos, y sin en Paquetes;
- Hay que superar la barrera de la Preservación Digital enfocada en medios, y en la sistémica adoptar la camada del Administrador de Storage Service asignada al Administrador de TI;
- Hay que irse más allá de las Estrategias de Preservación Digital sin un abordaje Sistémico, donde se convertía formatos, se migraba, emulaba, SECANDO HIELO;

Cadena de Custodia y de Preservación de Documentos Digitales siguiendo el Modelo OAIS





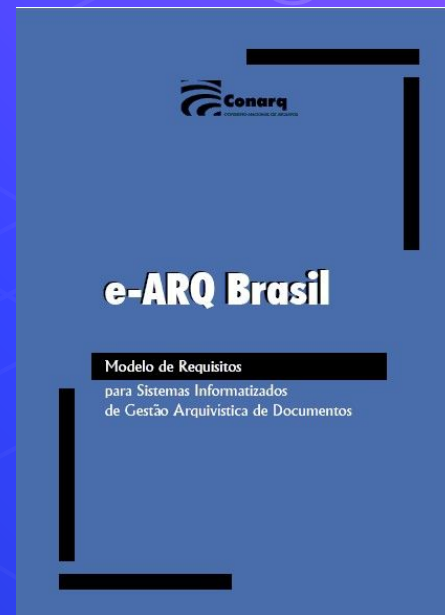
Guía de Implementación
de un Sistema de Gestión de
Documentos Electrónicos de
Archivo → **SGDEA**

● El e-ARQ

- Presenta los requisitos para un Sistema Informatizado de Gestión Archivística de Documentos (SIGAD);
- Gestión e Intermedio;

● El SIGAD

- Sistema desarrollado para realizar las operaciones técnicas de gestión archivística de documentos.



010

El

“Repositorio

Archivístico Digital

Confiable”

RDC-Arq o

RDC-Arch

es el Archivo

Histórico o

Permanente.

Repositório arquivístico digital confiável - RDC-Arq (Res. 43/CONARQ)

Um repositório digital de documentos arquivísticos é um repositório digital que armazena e gerencia esses documentos, seja nas fases corrente e intermediária, seja na fase permanente. Como tal, esse repositório deve:

- gerenciar os **documentos e metadados de acordo com as práticas e normas da Arquivologia**, especificamente relacionadas à **gestão documental, descrição arquivística multinível e preservação**;
- resguardar as características do documento arquivístico, em especial a **autenticidade (identidade e integridade) e a relação orgânica** entre os documentos.



A "Trusted Digital Archival Repository - TDAR or RDC-Arq (BR)" will be the "Historical Digital Archives" **in the future.**

Publication of the eArchiving Building Block technical specifications



©Pixabay

The European Commission is happy to publish updated technical specifications for the Connecting Europe Facility (CEF) eArchiving Building Block.

Karin Bredenberg, Activity 2 lead on behalf of the whole CEF eArchiving team from the National Archives of Sweden, noted:

"The DILCIS Board is proud to announce the official release of the next generation of E-ARK specifications! The new releases include a number of bug fixes and other updates which were only possible thanks to the huge amount of valuable feedback from the archival community in early 2019! We would like to thank you all and welcome everyone to both use and contribute to the specifications!"

<https://dilcis.eu/13-news/27-new-specification-releases-published>

"Common Specification for information Packages (CSIP)"

Textual document online: <https://earkcsip.dilcis.eu/>

Pdf: <https://earkcsip.dilcis.eu/pdf/eark-csip.pdf>

XML: <https://earkcsip.dilcis.eu/schema> and <https://earkcsip.dilcis.eu/>

"E-ARK SIP"

Textual document online: <https://earksip.dilcis.eu/>

Pdf: <https://earksip.dilcis.eu/pdf/eark-sip.pdf>

XML: <https://earksip.dilcis.eu/schema> and <https://earksip.dilcis.eu/>

"E-ARK AIP"

Textual document online: <https://earkaip.dilcis.eu/>

Pdf: <https://earkaip.dilcis.eu/pdf/aip-specification.pdf>

"E-ARK DIP"

Textual document online: <https://eardip.dilcis.eu/>

Pdf: <https://eardip.dilcis.eu/pdf/eark-dip.pdf>

XML: <https://eardip.dilcis.eu/profile>

"Common Specification for Geospatial data"

CS Geospatial data as pdf: https://github.com/DILCISBoard/E-ARK-Geodata/blob/master/Specification/CSGeo_v2.0.0.pdf

"Common Specification SIARD"

More work is going to occur with SIARD. Comments have been gathered during the review:

[https://github.com/DILCISBoard/SIARD/issues?](https://github.com/DILCISBoard/SIARD/issues?utf8=%E2%9C%93&q=is%3Aissue+label%3A%22Review+comment%22+)

<https://github.com/DILCISBoard/SIARD/issues?utf8=%E2%9C%93&q=is%3Aissue+label%3A%22Review+comment%22+>

SIARD format 2.1 (English):

https://github.com/DILCISBoard/SIARD/blob/master/specification/2018-12-04_SIARD_Format_Version-2_1-English.pdf

SIARD format 2.1 (German):

https://github.com/DILCISBoard/SIARD/blob/master/specification/2018-12-04_SIARD_Forumt_Version-2_1-German.pdf

SIARD format XML-schema:

<https://github.com/DILCISBoard/SIARD/blob/master/schema/metadata.xsd>

"Common Specification for Electronic Records Management Systems"

CS ERMS specification as pdf: https://github.com/DILCISBoard/E-ARK-ERMS/blob/master/Specification/CSERMS_v2.0.0.pdf

XML-schema: <https://github.com/DILCISBoard/E-ARK-ERMS/blob/master/Schema/ERMS.xsd>

XML-schema documentation pdf: https://github.com/DILCISBoard/E-ARK-ERMS/blob/master/Schema/ERMS_Schema_Documentation/pdf/ERMS.pdf

La Plataforma Archivística de Acceso y Difusión, tiene REQUISITOS ...



- Autenticación referenciada al “Repositorio Archivístico Digital Confiável” - RDC-Arq (Res.43/Conarq);
- Tener una navegación Multinivel;
- Mantener una relación de organicidad;
- Aceptar los más variados formatos de archivos para uso;
- Soportar Metadatos Archivísticos: ISAD(G)/NOBRADE, ISAAR, ISDIAH, ISDF, PREMIS, Taxonomia, etc...;
- Implementar el Modelo OAIS - SAAI (ISO 14.721/NBR 15.472), al trabajar con Paquetes OAIS: SIP, AIP e **DIP**;
- Importación/exportación en formatos patrones de interoperabilidad;
- Permitir la repoblación de sus Documentos Archivísticos y Metadatos (Objetos Digitales y Metadatos) al hecho de una invasión, monitoreado por el RDC-Arc;

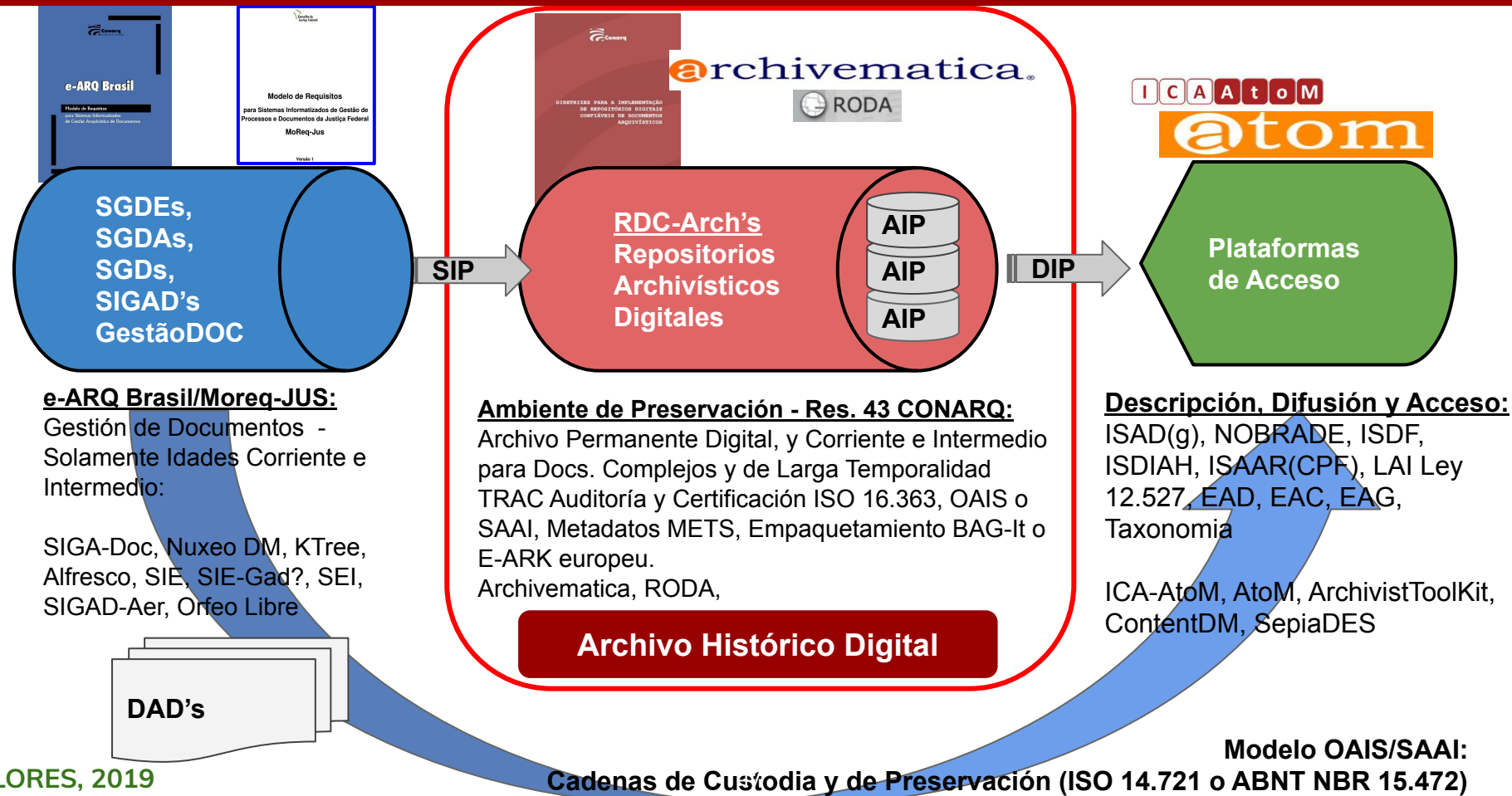
- Ser compatible con otros metadatos, mismo que no Archivístico, pero que sirvan de interoperabilidad para Modelos Conceptuales como Dublin Core, RAD, MODS, MADS, MARC, etc.;
- La producción automática de instrumentos de descripción archivística de multiniveles;

“No más deberíamos dar acceso de Documentos de Archivo en Websites sin estas funcionalidades, a los “medios externos USB u ópticos, HDs, CMS’s, Bases de Datos, sin una “Cadena de Preservación y de Custodia”, pero en Plataformas Archivísticas de Descripción, Acceso, Difusión y Transparência Activa de Informaciones y Documentos: como el AtoM (ICA-AtoM, etc.).”



EL NEGOCIO FAMILIAR ARCHIVÍSTICO SUPERNATURAL

Salvar personas, ofrecer seguridad jurídica a través de sus documentos seguros, confiables, preservables y auténticos ... Ofreciéndoles Custodia Digital Archivística - CCDA delante de las demandas de los documentos digitales y de la transformación digital



Consideraciones (1/2):

- Estábamos en búsqueda de un concepto más amplio, quizás un principio de no interrupción de una línea en dónde los documentos digitales deben de estar confinados en Sistemas Digitales con Requisitos Archivísticos e implementando la Política Archivística, bajo una CCDA;
- La Cadena de Custodia Digital Archivística se nos presenta como un importante concepto o principio archivístico ante la realidad digital;
- Aún no la hemos validado (CCDA) como un Modelo;

Consideraciones (2/2):

- Seguimos implementando la investigación junto a las instituciones, capturando Documentos Digitales de las entidades productoras o preservadoras para una CCDA;
- Los Archivos Nacionales o Generales de las Naciones necesitan ofrecer Custodia Digital Ininterrumpida bajo una CCDA, en un RDC-Arch en Paquetes AIP de Preservación;
- Necesitamos superar la ruptura paradigmática para hacernos una transición paradigmática basada en: Documentos de Archivo en Datos, en Repositorios Archivísticos Auditados y Certificados.



**¡Muchísimas
Gracias!**

Prof. Dr. Daniel Flores
Departamento de Ciência da Informação/UFF
Pesquisador CNPq
df@id.uff.br

Líder do Grupo de Pesquisa
CNPq UFF Ged/A

<http://documentosdigitais.blogspot.com>

<https://uff.academia.edu/DanielFlores>

<Facebook.com/DanielFloresBrasil>